PROFESSIONAL PAPER

Annals of Disaster Risk Sciences

Vol 3, No 2 (2020)

Quantum Computers - An Emerging Cybersecurity Threat

Dajana Jelčić Dubček, University of Applied Sciences Velika Gorica, Croatia

Address for correspondence: Dajana Jelčić Dubček, University of Applied Sciences Velika Gorica, Croatia, e-mail: dajana.jelcic-dubcek@vvg.hr

Abstract

Quantum computational supremacy may potentially endanger the current cryptographic protection methods. Although quantum computers are still far from a practical implementation in information processing and storage, they should not be overlooked in the context of cybersecurity. Quantum computers operate with qubits - units of information that are governed by the fundamental principles of quantum physics, such as quantum superposition of states and quantum coherence. In order to address the new challenge that quantum computers pose to cybersecurity, the very principles of their operation have to be understood and are overviewed in this contribution.

Keywords

qubits, quantum computing, quantum-safe cryptography, cybersecurity

1. Introduction

In October 2019. an article by Google scientists in the reputable journal Nature announced the experimental realization of a quantum processor Sycamore, a network of 53 programmable superconducting qubits (transmons) (Arute, 2019). The authors claimed that a problem which would have taken 10 000 years to be solved on a state-of-the-art classical processor had been processed in less than 200 seconds on the quantum one. The quantum supremacy of Sycamore with respect to the classical computers was questioned the very same day by the IBM scientists (Pednault, 2019). Nevertheless, it prompted again the old arguments about quantum computers and their ability to threat the global trade and cybersecurity.

It is the widely used RSA (Rivest et al., 1978) public-key cryptography that is considered particularly vulnerable to quantum attacks. The RSA secret keys are generated as a product of two N-digit prime factors. Their security relies on the general assumption that the opposite process of prime factorization, for which the computational time increases exponentially with N, is practically impossible in any finite time for a large enough N. The largest number factorized at present, even with the most powerful classical supercomputers and the most advanced algorithms, is the 829-bit RSA-250 number (250 decimal digits) (Boudot, 2020). And the next one is always a challenge - there is still no universal classical algorithm for the prime factorization. However, quantum computers and quantum algorithms promise to change this fact. The Shor's quantum algorithm (Shor, 1997) is shown to reduce the exponential computational time to the polynomial one and therefore potentially endanger the public-key cryptosystem.

In this work, the very principles of quantum computers and their relation to cybersecurity are presented. Sec.2. introduces qubits, units of quantum information, whose functioning is based on the quantum-mechanical concepts of superposition of states and quantum coherence. The subject of Sec.3. are the experimental and theoretical challenges encountered in the actual realization of quantum processors and their scaling to the real-world working machines. The advances in quantum computing in the context of present and future cybersecurity protocols and standardization are discussed in Sec.4. The concluding remarks are given in Sec.5.

2. Qubits – basic units of quantum information and computing

In classical (electronic) computing, the basic units of information are bits, logical states which can assume only two values, usually denoted by digits 0 and 1. The digits correspond to two physically distinguishable states of an electronic device, usually the current or voltage levels of tiny semiconducting circuits. The binary information is encoded in a series of bytes and sequentially processed through logic gates (electronic switches). Regardless of their physical realization, the output of this process is deterministic, i.e., uniquely defined by the input information and the applied gates.

These paradigmatic characteristics of the classical computing process – being *sequential* and *deterministic* – are to be replaced by the terms *simultaneous* and *probabilistic* for quantum computers. The units of information in quantum computing are *qubits* – the quantum bits. In analogy with classical bits, there are only two computational states of qubits, denoted by 0 and 1, which present two different classical values of some physical observable. The usual example of the qubit computational states 0 and 1 are the upward and downward pointing electron spins, the two opposite projections of the electron internal angular momentum.

What makes the qubits fundamentally different from classical bits is that they obey the laws of quantum physics that have no analogy in the classical world and often seem counter intuitive. In the quantum realm, the electron spin does not point up *or* down. Neither is its orientation somewhere between up and down. Instead, the spin points simultaneously up *and* down, i.e., it is in a *quantum superposition* of both states. It is only in the process of measurement that the spin/qubit assumes only one of the two possible states. It is a fundamentally random process, giving an ambiguous result 0 or 1 with certain probability for each of them.

It becomes even more intricated in a system of N mutually interacting qubits. There are 2^N possible multi-qubit states (different sets of single-electron spins) represented by the bit strings of type 0100…01110101. In a quantum system, however, it is impossible, even in principle, to know in which of the states the qubits actually are. Instead, the qubits are in a macroscopic *coherent* state – a linear superposition of 2^N classical states with the complex amplitudes allowing for their interference. While classical gates operate on each of the 2^N states in a succession, quantum gates are operators that act simultaneously on the quantum superposition of states and translate them, all at once, into a new set of states (quantum parallelism). The quantum coherence of the N-qubits wave function is destroyed only in the process of measurement, when the quantum state collapses into one of the possible classical outcomes with probability determined by its (complex) amplitude.

We are dealing with a "probabilistic computer, not any more with a Touring deterministic sequential machine" (Feynman, 1982). The result of a single quantum measurement is not a unique function of the input, but just one among the fundamentally random outputs. In order to find the final result, one needs to repeat the quantum calculus, and then consider the obtained results by classical methods. A good quantum algorithm is the one for which the exact answer corresponds to the most probable output superposition of states, while the others are mostly suppressed. The time-price for checking of the possible results does not depend significantly on N and the overall quantum computational time may still be considerably shorter than the time needed by the most advanced classical algorithms. Moreover, there is a big advantage with respect to the classical computing methods: in order to simultaneously examine 2^N states of the system a quantum computer needs only N qubits.

Quantum computers are not universal machines. The classical computational methods are deterministic and thus more appropriate in cases where one needs to know the exact result of some calculation. Quantum supremacy refers primarily to a complexity class of computational problems for which the computational time/power cost increases exponentially with an increasing number of bits (components). For example, the time needed to run the optimization analyses on a set of possible states described by N binary digits, with regard to some criterion, grows as 2^N. It explodes for large N's and it may be hard or even impossible to carry out the optimization in any reasonable time even on the best classical computers. However, the quantum algorithm for a database search, proposed by Grover, reduces this computational time quadratically with respect to its classical counterpart (Grover, 1996). The already mentioned prime factorization is an even more notable example. Using the quantum version of the fast Fourier transform, the Shor's algorithm reduces the prime-factorization computational time from an exponential to a polynomial dependence on N, retaining at the same time a small error probability (Shor, 1997).

3. Implementation

It has been almost 40 years since Feynman suggested quantum computers as a powerful tool for simulating quantum many-body systems (Feynman, 1982). Meanwhile, many computational codes and distinct mathematical apparatus based on the quantum mechanical principles have been developed (Coles, 2018) and a myriad of different physical realizations and architectures of quantum processors proposed by physicists and informational scientists (Nielsen, 2010). The quantum IBM Q-Experience processors with 5 and 16 qubits were launched in a Cloud for the general public (QExperience, 2016). It has been estimated, however, that at least 10 000 qubits are necessary for a useful quantum computer that can be implemented into existing computational systems. Scaling from the actual experimental systems of at most 100 qubits to the large-scale quantum computers, remains one of the main obstacles in their realization. It is not just a technological problem. Rather, it is related to the fundamental quantum-mechanical process of decoherence. No quantum system is completely isolated - due to the unintentional interactions of the quantum system with its surroundings, it becomes rapidly and strongly entangled with the environmental degrees of freedom. They provoke a gradual transition of the coherent quantum state into a single classical state (Schlosshauer, 2019). Quantum decoherence, analogous to the quantum to classical transition in the measurement process, becomes even more pronounced as the number of interacting qubits (quantum width) and/or gate cycles (quantum depth) increases. The thermal effects point into the same direction. Actual quantum computers require very low operating temperatures. Even temperatures as low as a few millikelvins may compete with the comparatively small transition energies between the many-qubit-states and suffice to break its coherent quantum state and translate it into a classical state. The interest of researchers is therefore directed towards fault-tolerant quantum computing, which protects qubits from errors generated from environmental interactions as well as from imprecise gate control (Lidar, 2013; Paler, 2015). The goal is to preserve the quantum coherence long enough and with a small enough error, such to enable a successful quantum calculation. One of the promising possibilities in this regard are transmons, the solid-state superconducting qubits used also in the Sycamore and the Q-Experience processors, which are designed specifically to reduce their sensitivity to noise (Schreier, 2008). Due to the many above discussed challenges, quantum computers are still in their early stage. The numbers factorized on quantum computers so far are not bigger than 15. Even the 53-qubit Sycamore, for which quantum supremacy was first announced (Arute, 2019), is far from being capable of decoding the actual RSA cryptographic keys. It is estimated that it will take at least 10 to 20 years of scientific work for quantum computers to become real-world functioning devices. However, it seems inevitable that, at some point in the relatively near future, quantum computers will become reality, at least in some extent. Collaborative efforts have been set up between academia, government and business, and oriented towards the first commercial applications of quantum computers (HSD Report, 2019). Meanwhile, the advances in quantum computing, based on the concepts of quantum parallelism and interference, have been implemented into the hybrid quantum-classical algorithms that can be run on digital computers, enhancing their possibilities (Ajagekar, 2019). Applicable for example, in complex combinatorial problems in molecular and biological engineering, weather forecasting or market scheduling, the quantum-inspired systems are welcomed also by the industry as powerful tools for optimization analyses (Fujitsu, 2020).

4. Quantum-safe cryptography

By performing tasks that classical computers cannot do in any feasible amount of time, quantum computers could completely change and revolutionize our science and world in general. There is, however, a trade-off: violation of data privacy and a security of the global information infrastructure. The presumed supremacy of quantum computers over the classical ones, opens up the possibility of an unauthorized access to the data stored on various devices. Personal data and documents or credit cards and business information, can all become the subject of quantum attacks. Confidential state information or patient health-care records, meant to remain secret for years, are particularly sensitive. Even if protected by the current encryption protocols, they could be collected and stored until the operable, sufficiently strong quantum computers become a reality. While believed to be resilient even to the most powerful classical supercomputers, the so called "hard" mathematical problems may become vulnerable to quantum attacks. This is especially true for the widely used public key (asymmetric) cryptography, which is based on the integer factoring (RSA) or discrete logarithm problems (EEC), shown already to be easily broken by means of Shor's algorithm. Various symmetric encryption codes, based on lattice theory, coding theory or the study of multivariate quadratic polynomials are, on contrary, believed to be quantum - safe (Stebila, 2015). For example, the Grover's square-root speedup of the AES (Advanced Encryption Standard) symmetric-key decryption can be annulled simply by doubling the size of a key. However, the shared secret key is still to be exchanged through the untrusted public-key channels and is therefore prone to deciphering and eye-dropping. It is hard to predict the development of quantum-safe cryptography (also called post-quantum cryptography). The present computational protocols may become unreliable in future due to the unprecedented advances in mathematical techniques. Meanwhile, however, a new and qualitatively different approach has been evolving – quantum cryptography. The quantum cryptography is to be distinguished from the math-based quantum-safe cryptography. The quantum-key-distribution (QKD) protocol exploits the fundamental principles of quantum mechanics (beyond the scope of this article), namely quantum entanglement (Horodecki, 2009) and the no-cloning theorem (Wootters, 1982). Being based on quantum mechanics itself, QKD prevents eavesdropping during the cryptographic key exchange and accomplishes an in principle unconditional security even in the future, independently of the advances in computational resources. The implementation of quantum-safe and quantum cryptography into the present security protocols and regulatory requirements is a slow process. The aim of the Open Quantum Safe (OQS) project is developing and prototyping quantum-resistant cryptography and integrating it in an open-source library appointed to all computational scientists and security practitioners (OQS, 2016). The efforts of European Union Agency for Network and Information Security (ENISA) are focused on protocols which can interoperate with existing communication networks and are secure against both quantum and classical attacks (Di Franco, 2018; ENISA, 2021). The Quantum-safe cryptography project by European Telecommunications Standards Institute (ETSI) is directed to the security of government and military communications, financial and banking transactions, the storage of personal and confidential corporate data in the cloud. It evaluates the proposed quantum-resistant public key algorithms, and considers their security properties, standardization and implementation for specific practical applications (ETSI, 2020). In the recent years, particular attention is paid to the modular systems, whose data is connected and exchanged through the Internet. The digital ledger systems (block-chains), in which the information is shared over a whole network of computers, are considered at present almost impossible to hack. However, the linking of the blocks of the chain, or the communication between the block-chains themselves, is based on hash functions and classical public key protocols which are potentially prone to quantum attacks. To ensure the authenticity, confidentiality and integrity of the transmitted messages, many encryption architectures and hybrid quantum-classical modifications of the public key cryptography have been suggested (Petrarche, 2020; Djordjevic, 2021). There are special concerns about the unauthorised access to the data transmitted and stored within the network Internet of Things (IoT), for which the low-energy and resources-requirements are hardly met with the expensive and complex quantum cryptographic systems (Fernández-Caramés, 2020). To build a blockchain framework for secure data transmission among IoT devices, the new lightweight quantum-inspired authentication and encryption protocols based on quantum random walks, have recently been proposed (El-Latif, 2021).

5. Conclusion

Quantum computers operate with quantum units of information (qubits), whose functioning is based on the fundamental quantum-mechanical principles of superposition of states and quantum coherence. Although not expected to be universal machines, quantum computers could potentially solve "hard" mathematical problems, not solvable by classical computers, which are the basis of actual cybersecurity protocols. Quantum computers are still an emerging technology and there are many experimental and theoretical obstacles and challenges to their scaling to real-world devices and their implementation into the present computational systems. Nevertheless, it is becoming obvious that it is essential for companies relying on information security and the ICT practitioners in general to keep up with their development. Numerous projects are launched worldwide, aiming to raise awareness of the potential impacts of quantum computing on information security. The main concern is directed to the sensitive data that needs to stay secure even far into the future. Governments all over the world are investing in quantum-safe cryptography and its adoption in the actual security schemes and standards. Once the technology of quantum computers matures, an unpredictable "quantum" jump into a quantum era of cybersecurity may happen all of a sudden, and only the collective international preparedness will ensure the stability in the cyberspace.

6. References

Ajagekar, A., Humble, T., You, F. (2019). Quantum Computing based Hybrid Solution Strategies for Large-scale Discrete-Continuous Optimization Problems. Computers and Chemical Engineering 32. 106630.

Arute, F. et al. (2019). Quantum supremacy using a programmable superconducting processor. Nature 574, 505–510.

Boudot, F. et al. (2020). https://listserv.nodak.edu/cgi-bin/wa.exe?A2=NMBRTHRY;dc42ccd1.2002

Coles,P.J. et al. (2018). Quantum Algorithm Implementations for Beginners. arXiv:1804.03719.

Di Franco, F. (2018). Analysis of the European R&D priorities in cybersecurity. European Union Agency for Network and Information Security (ENISA). ISBN: 978-92-9204-278-3. Retrieved from https://www.enisa.europa.eu/publications/analysis-of-the-european-r-d-priorities-in-cybersecurity

Djordjevic, I. B. (2021). QKD-enhanced Cybersecurity Protocols. IEEE Photonics Journal, doi: 10.1109/JPHOT.2021.3069510.

El-Latif, A. A. et al. (2021) Quantum-Inspired Blockchain-Based Cybersecurity: Securing Smart Edge Utilities in IoT-Based Smart Cities. Information Processing & Management 58, 4. 102549.

ENISA (2021). Post Quantum Cryptography: Current state and quantum mitigation. European Union Agency for Cybersecurity (ENISA), ed. Smart, N. and Lange, T.

ETSI. (2020) ETSI. Technologies. Quantum-safe cryptography. Retrieved from https://www.etsi.org/technologies/quantum-safe-cryptography

Fernández-Caramés, T.M. (2020). From Pre-Quantum to Post-Quantum IoT Security: A Survey on Quantum-Resistant Cryptosystems for the Internet of Things. IEEE Internet of Things 7, 7. 6457-6480.

Feynman, R.P. (1982). Simulating physics with computers. International Journal of Theoretical Physics, 21, 6/7, 467 – 488.

Fujitsu (2021). Quantum-inspired Digital Annealer (white paper). Retrieved from http://marketing.us.fujitsu.com/rs/407-MTR-501/images/quantum-inspired-computing.pdf

Grover, L.K. (1996). A fast quantum mechanical algorithm for database search. Proceedings 28th Annual ACM Symposium on the Theory of Computing. 212-219.

Horodecki R. et al. (2009). Quantum entanglement. Rev. Mod. Phys. 81 (2). 865–942.

HSD Report. (2019). Understanding the Strategic and Technical Significance of Technology for Security. Implications of Quantum Computing within the Cybersecurity Domain. The Hague Security Delta (HSD). Retrieved from https://www.thehaguesecuritydelta.com/media/com_hsd/report/257/document/HSD-Rapport-Quantum.pdf

Lidar, D.A., Brun, T.A.(Eds.). (2013). Quantum Error Correction. Cambridge University. Press.

Nielsen, M.A., Chuang, I.L. (2010). Quantum Computation and Quantum Information. 10th Anniversary Edition. Cambridge University Press. ISBN 978-1-107-00217-3.

OQS. (2016). Open Quantum Safe - software for prototyping quantum-resistant cryptography. Retrieved from https://openquantumsafe.org/

Paler, A., Devitt, S.J. (2015). An introduction to Fault-tolerant Quantum Computing. Cornell University. arXiv:1508.03695 [quant-ph]

Pednault, E. et al. (2019). Preprint at https://arxiv.org/abs/1910.09534

Petrarche, A. L., Suciu, G. (2020). Security in Quantum Computing. Annals of Disaster Risk Sciences 3, No 1. Special issue on cyber-security of critical infrastructure.

QExperience. (2016). Retrieved from https://www.ibm.com/quantum-computing/technology/experience/

Rivest, R.; Shamir, A.; Adleman, L. (1978). A Method for Obtaining Digital Signatures and Public-Key Cryptosystems. Communications of the ACM. 21 (2). 120–126.

Schlosshauer, M. (2019). Quantum decoherence. Physics Reports, 831. 1- 57.

Schreier, J.A. et al. (2008). Suppressing charge noise decoherence in superconducting charge qubits. Phys. Rev. B 77. 180502

Shor, P.W. (1997). Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer. SIAM J. Comput., 26 (5). 1484–1509.

Stebila, D. (2015). Quantum safe cryptography and security: An introduction, benefits, enablers and challengers. ETSI White Paper No 8. Retrieved from https://www.douglas.stebila.ca/research/papers/ETSI-Whitepaper15/

Wootters, W. and Zurek, W. (1982). A Single Quantum Cannot be Cloned. *Nature*. **299** (5886): 802–803. Bibcode:1982Natur.299..802W