ISSN No:-2456-2165

The Impact of Quantum Computing on Cybersecurity

Abhinandan Joshi
Computer Science & Engineering
National Institute of Technology Uttarakhand, India

Abstract:- In the computer based solutions of the problems in today's world; if the problem has a high complexity value, different requirements can be addressed such as necessity of simultaneous operation of many computers, the long processing times for the operatsion of algorithms, and computers with hardware features that can provide high performance. For this reason, it is inevitable to use a computer based on quantum physics in the near future in order to make today's crypto-systems unsafe, search the servers and other information storage centres on internet very quickly, solve optimisation problems in the NP-hard category with a very wide solution space and analyse information on large-scale data processing and to process high- resolution image for artificial intelligence applications. In this study, an examination of quantum approaches and quantum computers, which will be widely used in the near future, was carried out and the areas in which such innovation can be used was evaluated. Malicious or non-malicious use of quantum computers with this capacity, the advantages and disadvantages of the high performance which it provides were examined under the head of security, the effect of this recent technology on the existing security systems was investigated.

Keywords:- *Quantum Computer, Security, Cryptography, Threat.*

I. INTRODUCTION

Quantum computers; are designed to be based on quantum physics rules and can be expressed as computers that have the capacity to process more than the processing power and computation capabilities of conventional computers

- Quantum computers, which have a completely different structure from the functioning mechanism of a conventional computer, have the ability to make large-scale calculations conventional computers that can not be imagined by.
- In conventional computers, the numbers 0 and 1 are recorded as electrical currents on very small electronic circuits. If a circuit carries an electrical current it is expressed as 1, when the circuit does not carry an electrical current, it is expressed as 0.
- In quantum computers, there are 3 different combinations as working principle [a]. Contrary to conventional computers, quantum computers have more states: 1 state, 0 state, both 1 and 0 state. This format is called the superposition in the quantum physics, This triple combination in quantum computers is defined as "Quantum Bit" or "Qubit".
- Electrons have a natural spin formation. It is possible that this format can be changed by taking energy from outside. The quantum computers working according to this principle can transform information by changing the spin order of electrons during the processing of information.
- However, another physics principle comes into play in such situations: The Heisenberg Uncertainty Principle. It proposes that both position and velocity of an electron can not be determined at the same time because these two states can be transformed into each other. For this reason, when we examine an electron, it comes out of the state of superposition in which it is found.
- The logic of the operation triggered by the presence or absence of electrical current in conventional computers occurs at atomic size in quantum computers [a]. Qubits in quantum computers use the quantum circulant method to interact with each other.
- The principle of quantum circulation argues that when two electrons interact with each other, if one of the electrons is in a spin-down state, the other must be spin-up.
- Understanding how an ordinary process is performed on quantum computers is the basis for understanding the working mechanism of quantum computers.
- An electron can pass into the superposition state only if it is not detected by any observation tools or measuring instruments. In other words, the electron must not interact with any physical environment. If the electron is observed, spin state is fixed to that state. Since the observer cannot detect two different states of a material simultaneously, the mechanism of the changeable structure is disturbed.
- Observing the result obtained with a quantum computer actually requires understanding of the operating principle of this device fully. It is enough to obtain a constant result from the electrons in the superposition state and to observe these electrons to fix them.
- The observing process, performed to obtain the result, is called the collapse of the probability wave function in the quantum physics and all 2-bit qubits are collapsed and are interpreted as a single value by the observer. All qubits which are used depending on the first collapsed bit value, will be formed according to the shape of the first qubit and then the results will be obtained.
- The idea of using quantum computing on computers was first put forward by Richard Feynmann in 1959. But even
- the development of the conventional computers used was not completed at that time, therefore this idea was not found applicable in real world. The quantum working

principle use

Social media presence: A strong social media presence can help your brand reach more people and build relationships with your target audience. Consider creating accounts on platforms like Facebook, Instagram, Twitter, LinkedIn, and TikTok to promote your brand and engage with potential customers.

Search engine optimisation (SEO): Optimising your website for search engines can help improve your visibility in search engine results pages (SERPs). This involves researching and incorporating relevant keywords into your website con- tent, improving your website's loading speed, and creating high-quality backlinks to your website.

Email marketing: Email marketing is a cost-effective way to reach your target audience and promote your brand. Collect email addresses from your website visitors and use email marketing software to create and send personalised emails to your subscribers.

Content marketing: Content marketing involves creating and sharing valuable content that informs, educates, or entertains your target audience. This can include blog posts, videos, infographics, podcasts, and more. By consistently providing valuable content, you can build trust with your audience and establish your brand as an authority in your industry.

Influencer marketing: Collaborating with social media influencers can help your brand reach a wider audience and build credibility with your target market. Look for influencers who align with your brand values and have a strong following in your industry

Events and sponsorships: Participating in relevant events and sponsoring industry related organisations or causes can help your brand gain exposure and build relationships with your target audience. Consider attending trade shows, hosting webinars, or sponsoring community events to promote your brand.

Referral programs: Encouraging your satisfied customers to refer others to your brand can be a powerful way to grow your customer base. Offer incentives like discounts or free products/services to customers who refer others to your business.

In conclusion, there are many ways to promote your brand and attract new customers. By implementing a combination of the strategies above and continuously monitoring and adjusting your marketing efforts, you can effectively reach your target audience and grow your business.

REFERENCES

[1]. J. A. Silva, T. B. Ludermir, W. R. Oliveira. (2016). Quantum perceptron over a field and neural network architecture selection in a quantum computer, Neural Networks, pp. 55-64.
[2]. M. Gencer, ”Computer Book”, URL: http://www.mgencer.com/files/Bilgisayartabi.pdf, pp. 21-41.
[3]. G. Arun, V.Mishra. (2014). A review on quantum computing and communication, Emerging Technology Trends in Electronics, Communication and Networking, pp. 1-5.
[4]. I. Sndor, L. Gyongyosi. (2012). Advanced Quantum Communications: An Engineering Approach. John Wiley & Sons.
[5]. P. K. Amiri. (2003). ”Quantum computers”, IEEE Potentials, vol. 21 (5), pp.6-9.
[6]. S. Shamsolah Salemian, S. Mohammadnejad. (2010). ”An Error-Free Protocol for Quantum Entanglement Distribution in Long Distance Quantum Communication”, Communication Systems Networks and Digital Signal Processing (CSNDSP), pp. 626-630.
[7]. C. P. Williams, S. H. Clearwater. (1998) ”Explorations in Quantum Computing”, Springer-Verlag NewYork, Inc. TELOS.
[8]. P. W. Shor. (1994). ”Algorithms for quantum computation: discrete logarithms and factoring”, Proceedings of the 35th Symposium on Foundations of Computer Science, Los Alamitos, IEEE Computer Society Press, pp. 124-134.
[9]. N. Wiebe, A. Kapoor, K.M. Svore. (2014). ”Quantum deep learning”. Retrieved from URL: https://arxiv.org/abs/1412.3489
[10]. S. J. Devitt. (2016). ”Performing quantum computing experiments in the cloud”. Retrieved from URL: https://journals.aps.org/pra/abstract/10.1103/PhysRevA.94.032329
[11]. K. P. Kumar. (2013). ”PQ key-a novel key generation algorithm for processing big data using quantum computing”. Retrieved from URL: http://digital-library.theiet.org/content/conferences/10.1049/cp.2013.2481
[12]. F. S. Grodzinsky, M. J. Wolf, K. W. Miller. (2011). ”Quantum computing and cloud computing: humans trusting humans via machines”, Technology and Society (ISTAS), pp. 1-5.
[13]. H. Singh, A.Sachdev. (2014). ”The quantum way of cloud computing”, Optimisation, Reliability, and Information Technology (ICROIT) 2014 International Conference, pp. 397-400.
[14]. S. Caraiman,V.Manta. (2012). ”Image processing using quantum computing”, System Theory, Control and Computing (ICSTCC), 2012 16th International Conference, pp. 1-6.
[15]. V. Hahanov, V. Miz. (2013).” Quantum computing approach for shortest route finding”, East-West Design & Test Symposium, pp. 1-4.

[16]. O. Korchenko, Y. Vasiliu, S. Gnatyuk. (2010). ”Modern quantum technologies of information security”.
[17]. Shor, P. W. (1994). Algorithms for quantum computation: Discrete logarithms and factoring. Proceedings 35th Annual Symposium on Foundations of Computer Science.
[18]. M. N. Abdullah, M. T. Islam, M. M. Kabir, & M. R. Amin. (2018). Quantum computing: An overview with challenges and future prospects. International Journal of Computer Science and Network Security, 18(6), 94-101.
[19]. A. E. Rakhmanov, S. S. Knyazeva, D. A. Sidorov, & V. P. Shkodyrev. (2019). The future of quantum cryptography in the context of quantum computing. Journal of Physics: Conference Series, 1270(1), 012102.
[20]. A. R. Calderbank, P. W. Shor, & J. A. Smolin. (1998). Quantum error correction via codes over GF(4). IEEE Transactions on Information Theory, 44(4), 1369-1387.
[21]. S. Haroche & J-M. Raimond. (2006). Exploring the Quantum: Atoms, Cavities, and Photons. Oxford University Press.
[22]. A. O. Pittenger. (2000). An introduction to quantum computation algorithms. Progress of Theoretical Physics Supplement, 139, 77-108.
[23]. A. E. Siegman. (1986). Lasers. University Science Books.
[24]. R. P. Feynman. (1982). Simulating physics with computers. International Journal of Theoretical Physics, 21(6/7), 467-488.
[25]. C. Monroe & J. Kim. (2013). Scaling the ion trap quantum processor. Science, 339(6124), 1164-1169.
[26]. D. C. McKay, S. Sheldon, J. A. Smolin, & J. M. Chow. (2019). Efficient Z-measurement calibration for quantum devices with correlated noise. Physical Review A, 100(2), 022341.
[27]. Y. Su, W. Li, M. Li, & X. Li. (2019). Image recognition with quantum-enhanced feature extraction. IEEE Access, 7, 13846-
[28]. A. G. Fowler, M. Mariantoni, J. M. Martinis, & A. N. Cleland. (2012). Surface codes: Towards practical large-scale quantum computation. Physical Review A, 86(3), 032324.
[29]. D. V. Averin & C. Bruder. (2003). Capacitive coupling of charge qubits. Physical Review B, 67(16), 165322.
[30]. M. A. Nielsen. (2010). Quantum computation with cluster states. Quantum Information and Computation, 10(1&2), 5-48.