Game Changer in Cybersecurity: Quantum Cryptography

Amitabh VERMA
MIS, Sohar University, Sohar, Oman
vermainfo123@gmail.com

Abstract

With digital technology and increasingly linked economies comes a new set of risks from a slew of cyber-attacks. To improve cyber resilience, a cybersecurity capability system comprised of People, Process, and Technology is required to control the ongoing advancement of science and technology, particularly the quantum computer. As a result, attempts have been undertaken to lay new groundwork for cryptography research in computer communication networks. One of these attempts resulted in the creation of quantum cryptography technology, the security of which is based on quantum mechanics rules. Cyberspace security has emerged as the most important problem for the Internet in the foreseeable future. The objective of this research paper is to discuss the flaws and security problems in contemporary encryption, quantum cryptography essential concepts, real-world application use of this technology, and lastly the future direction of quantum cryptography.

Index terms: Cyberspace, Security, Cryptography, Quantum, Internet, Photon

References

[1]. Al-Ghamdi Ameenah Al-Sulami Asia Othman Aljahdali, A.-B., Asia Othman Aljahdali, C., & Security, C. (2020). On the security and confidentiality of quantum key distribution. https://doi.org/10.1002/spy2.111.

[2]. Alléaume, R., Branciard, C., Bouda, J., Debuisschert, T., Dianati, M., Gisin, N., Godfrey, M., Grangier, P., Länger, T., Lütkenhaus, N., Monyk, C., Painchault, P., Peev, M., Poppe, A., Pornin, T., Rarity, J., Renner, R., Ribordy, G., Riguidel, M., Salvail L., Shields, A., Weinfurter, H., Zeilinger, A. (2014). Using quantum key distribution for cryptographic purposes: A survey. Theoretical Computer Science, 560, 62–81. https://doi.org/10.1016/j.tcs.2014.09.018.

[3]. Bhatt, A. P., & Sharma, A. (2019). Quantum Cryptography for Internet of Things Security. Journal of Electronic Science and Technology, 17(3), 213–220. https://doi.org/10.11989/JEST.1674-862X.90523016.

[4]. Broadbent, A., Schaffner, C., (2016). Quantum cryptography beyond quantum key distribution. Designs, Codes and Cryptography, 78, 351–382. https://doi.org/10.1007/s10623-015-0157-4.

[5]. Cavaliere, F., Mattsson, J., & Smeets, B. (2020). The security implications of quantum cryptography and quantum computing. Network Security, 2020(9), 9–15. https://doi.org/10.1016/S1353-4858(20)30105-7.

[6]. Kumar, A., & Garhwal, S. (2021). State-of-the-Art Survey of Quantum Cryptography. Archives of Computational Methods in Engineering, 28(5), 3831–3868. https://doi.org/10.1007/s11831-021-09561-2.

[7]. Kwiat, P. G. (2002). Focus on Quantum Cryptography. New Journal of Physics, 4. https://doi.org/10.1088/1367-2630/4/1/002.

[8]. Mosca, M. (2018). Cybersecurity in an Era with Quantum Computers: Will We Be Ready? IEEE Security & Privacy, 16, 38–41. https://doi.org/10.1109/MSP.2018.3761723.

[9]. Phoenix, S. J. D., & Townsend, P. D. (1997). Quantum cryptography: Protecting our future networks with quantum mechanics. Information Security Technical Report, 2(2), 88–97. https://doi.org/10.1016/S1363-4127(97)81332-5.

[10]. Pirandola, S., Andersen, U. L., Banchi, L., Berta, M., Bunandar, D., Colbeck, R., Englund, D., Gehring, T., Lupo, C., Ottaviani, C., Pereira, J. L., Razavi, M., Shaari, J. S., Tomamichel, M., Usenko, V. C., Vallone, G., Villoresi, P., & Wallden, P. (2020). Advances in quantum cryptography. Adv. Opt. Photon., 12(4), 1012–1236. https://doi.org/10.1364/AOP.361502.

[11]. Price, A. B., Rarity, J. G., & Erven, C. (2020). A quantum key distribution protocol for rapid denial of service detection. EPJ Quantum Technology, 7(1), 8. https://doi.org/10.1140/epjqt/s40507-020-00084-6.

[12]. Qi, B., Qian, L., & Lo, H.-K. (2010). A brief introduction of quantum cryptography for engineers.

[13]. Raban, Y., & Hauptman, A. (2018). Foresight of cyber security threat drivers and affecting technologies. Foresight, 20(4), 353–363. https://doi.org/10.1108/FS-02-2018-0020.

[14]. Zhao, B., & Pan, J.-W. (2013). Chapter 14 - Generation and Storage of Single Photons in Collectively Excited Atomic Ensembles. In A. Migdall, S. V Polyakov, J. Fan, & J. C. Bienfang (Eds.), Single-Photon Generation and Detection (Vol. 45, pp. 541–562). Academic Press. https://doi.org/https://doi.org/10.1016/B978-0-12-387695-9.00014-7.

[15]. Zhou, T., Shen, J., Li, X., Wang, C., & Shen, J. (2018a). Quantum Cryptography for the Future Internet and the Security Analysis. Security and Communication Networks, 2018, 8214619. https://doi.org/10.1155/2018/8214619.

[16]. Zhou, T., Shen, J., Li, X., Wang, C., & Shen, J. (2018b). Quantum Cryptography for the Future Internet and the Security Analysis. Security and Communication Networks. https://doi.org/10.1155/2018/8214619.