OUR Journal: ODU Undergraduate Research Journal

Volume 7 *Special Issue: Interdisciplinary Cybersecurity Research* Article 5

2020

Application of Quantum Cryptography to Cybersecurity and Critical Infrastructures in Space Communications

Rita Meraz
Old Dominion University

Linda Vahala
Old Dominion University

Application of Quantum Cryptography to Cybersecurity and Critical Infrastructures in Space Communications

Cover Page Footnote

This research is supported in part under NSF grant DGE-1723635.

APPLICATION OF QUANTUM CRYPTOGRAPHY TO CYBERSECURITY AND CRITICAL INFRASTRUCTURES IN SPACE COMMUNICATIONS

By Rita Meraz* and Linda Vahala

I. INTRODUCTION

Critical infrastructure can be defined, as stated by the French aerospace company Thale—which provides services to top markets and departments of the federal government globally—as everything that is needed to keep society working and the economy up and running (Renaud et al. 2017). This statement dictates that critical infrastructure involves every aspect that keeps the commonwealth stable and evolving; therefore, because of the vast aspects that involve these actions, critical infrastructure is divided into sectors, numerically 16, each with a specific objective that contributes to the well-being of a nation's society and economy (Homeland Security). Some of these sectors are:

- Chemical Sector
- Commercial Facilities Sector
- Communications Sector
- Defense Industrial Base Sector
- Communications Sector
- Critical Manufacturing Sector
- Food and Agriculture Sector
- Dams Sector
- Emergency Services Sector

*This research is supported in part under NSF grant DGE-1723635.

Security to these sectors is crucial, and a threat to their safety can potentially damage the services that the millions of residents in a nation currently depend on. As stated by the U.S. Department of Homeland Security, "Critical infrastructure describes the physical and cyber systems and assets vital to the United States that their incapacity or destruction would have a debilitating impact on our physical or economic security or public health or safety (Homeland Security)." Therefore, the protection and continuous updates of current security systems are necessary to prevent situations such as terrorism, cyber attacks, unauthorized interference of information, etc.

In today's digital world, cybersecurity plays a critical role in the protection of critical infrastructure. Each sector in critical infrastructure relies on the internet, making them vulnerable to cyber threats. Consequently, cybersecurity, which combines state-of-the-art security and technology, is crucial to provide protection and guarantee the safety and continuity of activity within each sector.

This paper focuses mainly on the implementation of cybersecurity to the communication sector, which encompasses the systems that provide interconnection services. These systems are satellites which are fundamental for communication. They play an essential role in science, government agencies, or businesses. Thus, the protection of the signal transmitted from such space systems is substantial.

The possibility to hack satellites used for the transmission of information by organizations such as the U.S. military or intelligence agencies can be attainable, and the consequences of this happening could be alarming. In other words, if an eavesdropper were able to intrude these satellite communication systems, the information obtained could be used against the administration controlling such communication networks, making a threat to the wellbeing of the system, and therefore of the critical infrastructure of the society.

This paper provides a review of laser communication satellites. It also introduces quantum space communication systems to demonstrate that advancement in technology is necessary due to quantum systems possessing features that current systems do not.

II. LASER COMMUNICATION SPACE SYSTEMS OVERVIEW

Laser communications systems have their beginning since 1990, but it was not until 2012 that ARTEMIS, European Space Agency's (ESA) first GEO data communication satellite became the first to establish a laser link with a ground station at Kyiv (Kramer, 2002). Its success represented a breakthrough in communication satellites, and throughout the years, more and more countries started implementing such systems. The need for more reliable and technological communication systems brought these systems into operation since some of their main characteristics are that they can transmit a lot of data faster, error-free, and with less power-required than radio frequency satellites. Furthermore, the beam produced by these systems has small diffraction which provides better precision and thus can improve interstellar navigation.

In 2013, NASA displayed its first laser communication system into space, the Lunar Laser Communications Demonstration (LLCD) mission which was able to operate error-free and decrease ten times the link loss of data from previous experiments (Cornwell, 2016). Even though the mission proved that laser links were able to provide exceptional precision, high-definition video link, and high data rates, every system has its downside. These laser operational satellites can communicate tens of terabytes of information in just seconds, but the data transmitted has to overcome atmospheric turbulence, cloud cover, and other impediments to achieve its destination. Most important, the current encryption implemented in these systems can be breakable, which makes the information sent vulnerable to cyber threats. As mentioned before, communication is a sector of critical infrastructure; its security is crucial to guarantee safety to the nation. Not only because the government and specialized agencies make use of it, but also because it provides the means to which people live in the present time.

Encryption is defined as the process of encoding information to ensure its confidentiality from unauthorized users (Aumasson, 2018). The data transmitted between desired parties can be protected through cryptosystems, which are mathematical algorithms that provide security through keys. These can be symmetric which work with secret-keys or asymmetric which work with public-keys (Papoutsis et al. 2007). A more descriptive definition, for symmetric ciphers, is that security lies entirely in the key itself,

and so the safety of the system is compromised by the security of the key. For instance, assume an analyst wants to send a document with important information about the company she works for, so she sends the document encrypted with a key (i.e. password). Thus, for the receiver to access the document, the analyst must also send the key. Sharing the key makes it possible for an unauthorized user to decode the password and consequently get access to the document with valuable information. For asymmetric ciphers, different keys are used for encryption and decryption. Following the example previously mentioned, in the asymmetric encryption, both users, the analyst, and the receiver would create a public and a private key that would be uniquely interconnected. The receiver would first share his public key; then the analyst would encrypt the document with the public key from the receiver, and then return it to him. The receiver is the only one able to open his public key with his private key. In other words, the public key would encrypt the document, but only the corresponding private key will be able to decrypt it. This behavior makes it difficult for an intruder who does not have the matching private key to decrypt the public key and intercept the document.

Current encryption techniques are based on these symmetric-asymmetric encryption categories. Some examples are the Data Encryption Standard (DES), the advanced encryption standard (AES), and the Rivest-Shamir-Adleman Algorithm (RSA). A brief evaluation of each one is given subsequently. First, the DES is a block encryption algorithm meaning it operates on a group of bits, where the signal is divided into blocks of fixed length and subsequently encrypted using a single key (Coppersmith, 1997). Second, the AES is another symmetric block cipher and a modified version of the DES created by the U.S. government to protect classified information. It alternates independent key round transformations and has a simple algebraic structure (Dobbertin, 2005). One more example is the Rivest-Shamir-Adleman Algorithm (RSA), which is based on factoring large numbers, products of two prime numbers, to generate the encryption keys (Azad, 2015). It has the advantage that private keys do not need to be transmitted.

The following table presents a summary of these common encryption algorithms:

Data Encryption Standard (DES)	Advanced Encryption Standard (AES)	Rivest-Shamir-Adleman Algorithm (RSA)
● Block encryption algorithm ● Signal is divided into fixed-length blocks ● Enciphered using a single key ● Key size: 56 bits ● High complexity level	● Symmetric block cipher ● Modified version of DES created by the U.S. government to protect classified information ● Key works for both encrypting and decrypting ● Its algebraic structure is simple ● Key size: 128, 192, and 256 bits	● Uses very large prime numbers to generate the public key and the private key ● Private keys do not need to be transmitted ● Widely use ● Slow and computationally complex ● Key size:1,024 to 4,096 bits

Like these examples, there are other encryption algorithms used for the protection of data, but each one, including the ones mentioned, has its disadvantage that makes its implementation on satellites unfeasible (Mitali, 2014). For instance, the key size of the DES algorithm, which is 56 bits, is too small to manage inter-satellite communication. Furthermore, its structure has a high complexity level. The AES algorithm is capable of using cryptographic keys of 128, 192, and 256 bits to encrypt and decrypt data, but it is a symmetric block cipher meaning it requires key sharing which compromises the security of the system. Finally, the widely used RSA algorithm is slow and computationally complex, which is impractical for the encryption of large data sets (Papoutsis et al., 2007). It can be concluded that the need for a more powerful cryptosystem that can guarantee cyber protection to such space systems is evident.

III. QUANTUM CRYPTOGRAPHY

While this paper will not provide a comprehensive review of Quantum computing, it is essential to mention some of its characteristics to understand quantum cryptography. Quantum computing can be complicated to discern. Sometimes, it can even be seen as science fiction since the way it behaves is different from what people are used to in the classical world ruled by Newton's Laws. Many scientists have tried to understand

the laws that govern quantum physics, but as the well-known physicist Richard Feynman said: “If you think you understand quantum mechanics, you don’t understand quantum mechanics.”

Quantum computing is based on the laws of quantum physics. Every computing system relies on the ability to manipulate and store bits (IBM). In contrast to classical computing, where a bit can only be in one state at a time, 0 or 1, in quantum computing, quantum bits called qubits can also be in both states at once, a term called superposition. Mathematically, the linear combination of both states can be expressed as $|\phi\rangle=\alpha|0\rangle+\beta|1\rangle$ where α and β are complex numbers (Wang et al. 2015). An analogy for this term would be to consider a coin spinning. As the classical world would predict, the coin has a 50 percent chance to land either tails or heads, but that is not the case in the quantum world. In the quantum level, the probability of the coin to fall head over tail can be any percentage, for instance, 40-60, 30-70, meaning that its probability identity is a spectrum and not a single defined one. Quantum computing characteristics surpass classical computing ones in many ways. For instance, quantum computing can store considerably larger amounts of information and be faster at database searching than traditional computing. Furthermore, because of the superposition characteristic that quantum possesses, quantum computing allows multiple computations to happen simultaneously. It can be seen that many aspects of quantum computing can be used to improve current classical systems, and space communication systems are not an exception. The data transmitted by such devices can be further protected through quantum cryptography, which overcomes existing traditional classical cryptography schemes (Kester et al. 2013).

Quantum cryptography uses the laws of quantum physics to secure the data that is transmitted by desired parties (Padamvathi, 2016). Quantum Key Distribution (QKD) protocol provides a way of sharing and distributing keys encoded in single photons (Quantum Flagship), in other words the data is transmitted with single-photon transmissions. The way QKD works is that the sender, who in quantum cryptography is called Alice, sends each bit. The receiver, which is called Bob, tries to extract the information from the signal that Alice has sent. To obtain the information from Alice’s signal, Bob needs to perform some measurement on this signal. As mentioned before in no quantum encryption techniques, if the intruder called Eve has access

to the corresponding communication channel, she can measure each bit that Alice sent to Bob and thus, get access to the message but in quantum physics, Eve has to do some measurements to reveal the message, but that process changes the signal. That is to say that if Eve does not know in which orientation each bit was sent, she can select the wrong orientation for her measurement, giving notice to Bob and Alice that an intruder attempted to intercept the information (Nielsen, 2010). It can be seen that the quantum cryptosystem can provide significant aspects in satellite cybersecurity since it can secure data transmission by applying the laws of quantum physics. Furthermore, QKD encryption cannot be broken. It is ideally challenging to be intercepted by unwanted users, and if this were to happen, the unauthorized user would not be able to evade detection.

A representation of quantum cryptography is shown in the following figure:

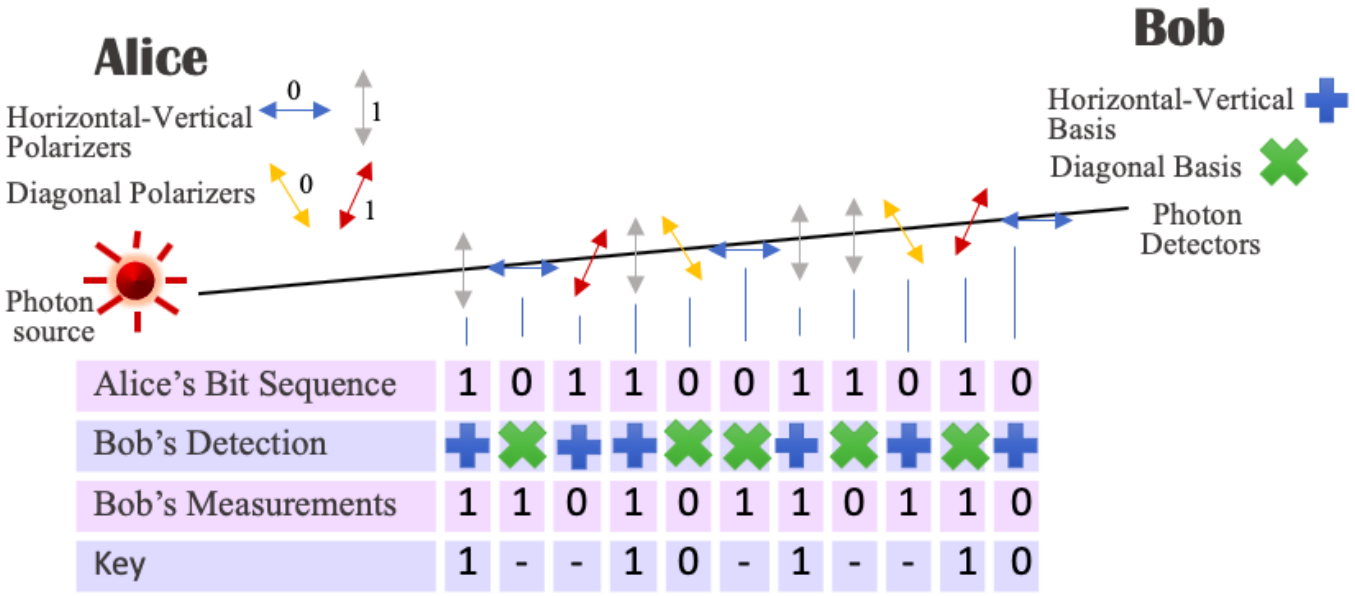

Figure 1: Quantum Cryptography representation example

Most of the current encryption algorithms are governed by the previously mentioned RSA scheme. But this algorithm can be easily breakable by quantum cryptography (Galindo et al., 2018). Thus, the change to a more robust encryption scheme to secure communications is needed, and quantum cryptography provides such protection. An example of the impact that quantum cryptography could have is on the European Data Relay System developed by the European Space Agency (ESA). Due to the protection of data that it provides,

this system—which is designed to reduce the delay and increase the amount of transmission of data between satellites and the Earth—might need to improve its current cryptography to protect the information, and that can meet new changes of the system. Quantum cryptography can provide such aspects (ESA, 2015).

All the great qualities mentioned about quantum computing have triggered universities, the government and research centers to direct their attention into quantum. More and more countries are investing in research and starting with experiments using principles of such area of study. In 2016, China launched the first quantum communications satellite named Micius, which was able to successfully implement quantum cryptography by teleporting photons using single photons between the ground stations in China and Austria (MIT, 2018). With this milestone, China was set at the lead in having the utmost advances on the field. Japan is next in the field, even though it hasn't been able to launch a quantum communication satellite. The National Institute of Information and Communications Technology (NICT), Japan's primary research institution for communications, was able to establish a small and light quantum communication transmitter onboard of the satellite SOCRATES microsatellite (2017). It was once more proven that quantum is feasible in communications apace systems. Furthermore, this mission also shows that the cost of quantum communication can be reduced by being implemented in small, low-cost satellites.

This paper could mention countless features about quantum computing that keep proving its efficacy and the great protection it provides to the data transmitted by space systems. But the many features could make the paper deviate from its main point and become very extensive. The key in this paper is that quantum cryptography guarantees secure communication through the randomness aspect of the superposition behavior generated using quantum optics.

IV. CONCLUSION

Critical infrastructure can be Strengthening the resilience and security of cyberspace has become a fundamental mission of every nation's homeland security. Currently, most encryption schemes are based on algorithms that can be breakable. This is one of the main reasons that governments throughout the world invest in the design of quantum computers. Quantum cryptography provides unique protection which guarantees secure communication through the randomness aspect of the superposition behavior generated using quantum optics. Even though this paper presents the advantages of implementing quantum cryptography in space systems such as satellites which are part of the communications sector, quantum can also be utilized to enhance the security of the different sectors in the critical infrastructure of a nation. The characteristics mentioned show that quantum cryptography can provide a more reliable, more accessible, faster and safer encryption scheme. Therefore, continuing research in quantum cryptography is necessary to take humans critical infrastructure to the next step in security and technology.

Appendix

The following equations and plots are an aside project that describes the Steady-State Scalar Berloff Asymptotics. The Berloff asymptotics are a set of equations that are related to quantum fields.

The Gross-Pitaevskii (GP) model illustrates the mean-field theory in the quantum field (Berloff, 2004). We use the Pade summation method to obtain an estimate of the simple vortex structure

$$\psi = R(r)\, e^{in\Phi}$$

The following equation is a GP model of the form

$$0 = \nabla^2\psi + [\mu - g|\psi|^2]\psi$$

the boundary conditions to obtain an approximation to the simple vortex solution are

$$\psi \to \sqrt{\mu/g}\ as\ r \to \infty\ ,$$

$$\psi \to 0\ as\ r \to 0,$$

The attempted solution for the simple vortex is obtained through the modified form of the steady GP equation

$$R''(r) + \frac{1}{r}R'(r) - \frac{\pi^2}{r^2}R(r) + [\mu - gR^2(r)]R(r) = 0$$

Pade approximation of the simple vortex

$$R(r) = r\sqrt{\frac{(a_1 + \mu\, b_2 r^2)}{1 + b_1 r^2 + g b_2 r^4}}$$

where a_1, b_1, b_2 are unknown coefficients.

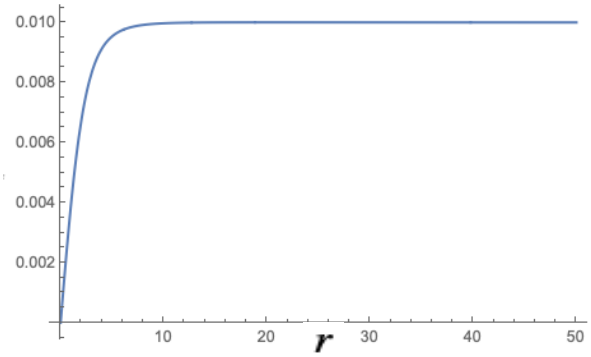

Figure 2: Plot of various approximations of the simple vortex solution as a function of distance from the pivot of the vortex

The residues plot meaning the deviation of the Pade solution from the exact solution to the ODE is:

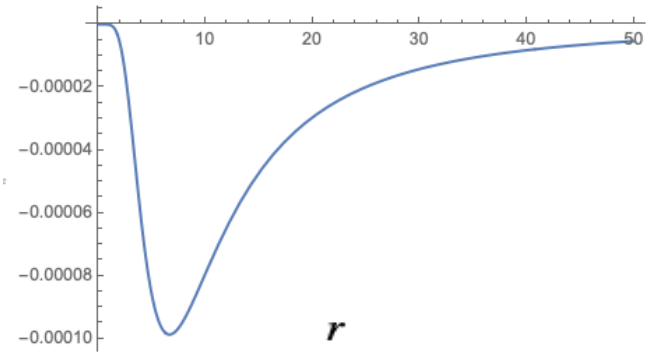

Figure 3: Residues Plot

Acknowledgement

This Research Experience for Undergraduates (REU) was sponsored by the National Science Foundation.

Special thanks to Dr. Vahala who mentored and guided me through the research despite the challenges

presented. I extend my gratitude to Old Dominion University and the Electrical Engineering faculty for allowing me access to the college resources.

REFERENCES

1. J. C. Renaud, Q. Rétinas, C. Fleury, C. Viseux, R. Olivier. “Thales,” *Thales Corporate Communications*, 2017. Available: https://www.thalesgroup.com/sites/default/files/database/document/2019-04/Web%20file%20-%20English%20-%20Thales%20-%20brochure%20-%20EN%20-%20V7.pdf. [Accessed June 18, 2019]
2. Homeland Security. “Critical Infrastructure Sectors.” Available: https://www.dhs.gov/cisa/critical-infrastructure-sectors. [Accessed June 12, 2019]
3. Homeland Security. “Infrastructure Security.” Available: https://www.dhs.gov/topic/critical-infrastructure-security. [Accessed June 15, 2019]
4. Homeland Security. “Cybersecurity.” Available: https://www.dhs.gov/cisa/cybersecurity. [Accessed June 15, 2019]
5. Aumasson, "Serious cryptography a practical introduction to modern encryption," M. D. Green, Ed., ed: San Francisco: No Starch Press, 2018.
6. D. Coppersmith, C. Holloway, S. M. Matyas, and N. Zunic, "The data encryption standard," *Information Security Technical Report,* vol. 2, no. 2, pp. 22-24, 1997, doi: 10.1016/s1363-4127(97)81325-8.
7. H. J. Kramer, “ARTEMIS,” *eoPortal Directory*. 2002. [Online]. Available: https://earth.esa.int/web/eoportal/satellite-missions/a/artemis. [Accessed May 17, 2019]
8. D. Cornwell, "Space-Based Laser Communications Break Threshold," *Opt. Photon. News,* vol. 27, no. 5, pp. 24-31, 2016.
9. E. Papoutsis, G. Howells, A. Hopkins and K. McDonald-Maier, "Key Generation for Secure Inter-satellite Communication," *Second NASA/ESA Conference on Adaptive Hardware and Systems (AHS 2007)*, Edinburgh, 2007, pp. 671-681.

10. “What is Quantum Computing,” IBM. Available: https://www.research.ibm.com/ibm-q/learn/what-is-quantum-computing/. [Accessed June 15, 2019]
11. P. Wang, X. Zhang and G. Chen, "Efficient quantum-error correction for QoS provisioning over QKD-based satellite networks," *2015 IEEE Wireless Communications and Networking Conference (WCNC)*, New Orleans, LA, 2015, pp. 2262-2267.
12. Q. Kester, L. Nana and A. C. Pascu, "A novel cryptographic encryption technique of video images using quantum cryptography for satellite communications," *2013 International Conference on Adaptive Science and Technology*, Pretoria, 2013, pp. 1-6.
13. M. A. Nielsen, I. L. Chuang, “Quantum Computation and Quantum Information,” *Cambridge University Press,* 2010
14. O. Galindo, V. Kreinovich and O. Kosheleva, "Current Quantum Cryptography Algorithm Is Optimal: A Proof," *2018 IEEE Symposium Series on Computational Intelligence (SSCI)*, Bangalore, India, 2018, pp. 295-300.
15. “The European Data Relay System,” *ESA Communications*, 2015. Available: https://esamultimedia.esa.int/multimedia/publications/BR-322/. [Accessed May 30, 2019]
16. Emerging Technology from the arXiv, “Chinese satellite uses quantum cryptography for secure videoconference between continents,” *MIT Technology Review*. Jan 2018. [Online]. Available: https://www.technologyreview.com/s/610106/chinese-satellite-uses-quantum-cryptography-for-secure-video-conference-between-continents/. [Accessed July 1st, 2019]
17. “World's First Demonstration of Space Quantum Communication Using a Microsatellite,” National Institute of Information and Communications Technology, July 2017. [Online]. Available: https://www.nict.go.jp/en/press/2017/07/11-1.html#Glossary2. [Accessed July 3, 2019]
18. N. G. Berloff, "Padé approximations of solitary wave solutions of the Gross–Pitaevskii equation," *Journal of Physics A: Mathematical and General,* vol. 37, no. 5, pp. 1617-1632, 2004/01/19 2004, doi: 10.1088/0305-4470/37/5/011.

19. H. Dobbertin, V. Rijmen, and A. Sowa, "Advanced Encryption Standard - AES [electronic resource] 4th International Conference, AES 2004, Bonn, Germany, May 10-12, 2004, Revised Selected and Invited Papers," 1st ed. 2005.. ed, 2005.
20. S. Azad and A.-S. K. Pathan, "Practical cryptography algorithms and implementations using C++," in *Algorithms and implementations using C++*, ed: Boca Raton: Taylor & Francis, 2015.
21. V. K. Mitali and A. Sharma, "A survey on various cryptography techniques," *International Journal of Emerging Trends & Technology in Computer Science (IJETTCS)*, vol. 3, no. 4, pp. 307-312, 2014.
22. V. Padamvathi, B. V. Vardhan, and A. V. N. Krishna, "Quantum Cryptography and Quantum Key Distribution Protocols: A Survey," in *2016 IEEE 6th International Conference on Advanced Computing (IACC)*, 27-28 Feb. 2016 2016, pp. 556-562, doi: 10.1109/IACC.2016.109.
23. Quantum Flagship. "Quantum Key Distribution." https://qt.eu/understand/underlying-principles/quantum-key-distribution-qkd/ (accessed April 15, 2020).