Quantum Key Distribution: A Solution to Space Security Limitations

Steven P. Harmon

Department of Accountancy, Finance, and Information Systems

ISIN 380: Space and Satellite Cybersecurity

Dr. Molly M. Cooper

April 26, 2024

Quantum Key Distribution: A Solution to Space Security Limitations

Unique vulnerabilities in traditional cryptography have brought space systems security to the forefront of government and private industry policy as aging space systems present significant risks to global communications and data security. To address these increasing risks, quantum key distribution (QKD) represents a significant advancement, particularly with regard to space systems' long-term security challenges. Several entities have already demonstrated the practical application of QKD in both space-based and terrestrial systems.

This technology provides resistance to interception and tampering without alerting the participants to the presence of an eavesdropper. In addition, QKD offers inherent resilience to threats posed by emerging quantum computing technologies to traditional cryptographic technologies. However, the deployment of QKD faces several challenges, including integration complexities and the prohibitive costs associated with deployment. This analysis will explore how stakeholders can overcome these challenges to leverage QKD's full potential and ensure that its deployment in space systems is as effective in practice as it is in theory.

The Evolution of Quantum Key Distribution

Quantum cryptography is not a new concept. According to Bennett and Brassard (1989), Stephen Wiesner introduced the initial concepts of quantum cryptography in the late 1960s through his work "Conjugate Coding." They state that, in this unpublished work, Wiesner explained how governments could utilize quantum physics to produce bank notes that would be impossible to counterfeit. In the September 1989 experiment discussed by Bennett and Brassard, a sender and receiver exchanged a quantum key where 20% of the bits were different than expected in the exchange. This presented a recognized proof of concept, but the error rate was unacceptable. They explain that in October of 1989, a similar experiment resulted in a more convincing success with a crossover frequency of only 6.6%.

Bennett and Brassard (1989) also note that, due to a reconciliation protocol introduced by themselves and Jean-Marc Robert in 1985, the two endpoints successfully extracted 443 perfectly shared bits from the originally sent one thousand bits. Bennett and Brassard state that after an additional equality confirmation protocol reconciled 403 bits, the two endpoints determined with high confidence the secure nature of those bits, with a chance of an error being undetected being less than 10^{-12}. They affirm a 403-bit value shared between the two endpoints was completely unknown to a third entity, presenting a public discussion between the two participants that did not leak any information about the resulting string to someone who was unaware of the original 1000-bit value. Importantly, Bennett and Brassard (1989) show how such a quantum cryptographic key can be resistant by design to eavesdropping and interception. In their experiment, they showed how the third party is unable to intercept more than 200 bits of information about the 403-bit accepted bits without alerting the original participants to tampering. This provides a theoretically impossible task to overcome for anyone intent on listening in on the encrypted communications and represents early experimental successes of putting theoretical QKD into practice.

Quantum Key Distribution Compared to Traditional Cryptography

As Lindsay (2020) explains, traditional cryptography depends on the computational difficulty of mathematical problems, often with a pre-shared key pair. The task of compromising these advanced mathematical problems with current computational methods is an unrealistic goal because experimental machines are not powerful enough to break current encryption standards. However, adversaries can theoretically compromise these cryptographic mechanisms if such an adversary discovers an efficient algorithm or if they exploit sufficiently powerful computers to break the encryption. As newer traditional cryptographic methods secure the digital landscape, industry stakeholders have long considered older cryptographic algorithms flawed. Harmon (2023) notes that older space system deployments often used encryption mechanisms that are now outdated and considered less secure, presenting a challenge for space systems with traditional cryptography. As technology evolves, cryptography must evolve to continue providing secure communications. Furthermore, Lindsay (2020) states that quantum computing offers advanced computational abilities with the prospect of being able to break current encryption standards more easily, presenting another challenge to classic cryptography.

Quantum Key Distribution relies on the principles of quantum mechanics rather than mathematical complexity. According to Mafu and Senekane (2018), it is impossible for an adversary to eavesdrop on secure communication without alerting the participants. They state that it is impossible to perform a measurement on the unknown quantum state without introducing disturbances, and that a single measurement of an observable quantum creates uncertainty in other properties, prohibiting the measurement of simultaneous states. In each case, the quantum state has changed, and detection of the measurement is automatic for the sender and receiver. This confirms the assertion by Bennett and Brassard (1989) that a third party cannot meaningfully compromise the quantum key without alerting the authorized parties. In addition, Mafu and Senekane (2018) reinforce the fact that a third party cannot clone a quantum key and pass it on in an undisturbed state, as the mere act of detection, measurement, and cloning irreparably alters the quantum state of the key, making both the copy and the passed key imperfect.

Historical Challenges to QKD

As with any new innovation, challenges to the practicality and security of QKD presented themselves early on. According to Zhang et al. (2018), the lack of perfect single-photon sources and detectors in practice resulted in several security vulnerabilities in QKD. Zhang et al. notes that, as with other technologies, designing protocols with security in focus can be a significant defense against such vulnerabilities. They state that researchers have proposed many such protocols that can secure against some known vulnerabilities. Many of these protocols are already possible with current technology.

In addition, Zhang et al. (2018) discuss how large-scale deployment has been challenging thanks to high channel loss and decoherence, with the distance record sitting at only 404 kilometers. One solution they propose is a quantum repeater, however, questions remain about the real-world applicability of such repeaters as a result of the limitations to performance of quantum memory. Zhang et al. notably explain that due to the significantly less channel loss and negligible decoherence in empty space, satellite-based quantum communication is a more promising solution for practical implementations.

Quantum Key Distribution in Space Systems

The empty space surrounding space systems presents a unique opportunity to utilize QKD. Lu et al. (2022) state that one of the advantages of satellite-based quantum communications is that the loss of photons induced by atmospheric absorption and scattering only occurs in the lower ~10km of the atmosphere. This presents a solution to one of the more restrictive aspects of QKD. According to Zhang et al. (2018), providing efficient QKD across a distance greater than even several hundred kilometers terrestrially becomes exponentially difficult. However, according to Lu et al. (2022), such effects of absorption and decoherence become proportional to the square of the distance rather than the exponent of the distance.

While satellites can communicate with extremely limited absorption and decoherence in the vacuum of space, atmospheric and other limitations cause interference when communicating between a satellite and a ground station. As Lu et al. (2022) note, atmospheric absorption and optical and detection efficiencies all contribute to losses in efficiency. They explain that the diffraction of an optical beam is primarily related to its spatial mode, wavelength, and the telescope aperture in free-space quantum communication. Lu et al. conclude that choosing shorter photon wavelengths and a larger waist radius can mitigate the diffraction losses. However, they point out that due to beam truncation, having a beam waist larger than the telescope radius will cause significant losses. Lu et al. suggest that setting the full width at half maximum beam waist to be half of the transmitting telescope diameter is optimal for reducing losses. Furthermore, they suggest that it is essential to develop a high-precision, high-bandwidth acquiring, pointing, and tracking (APT) system to mitigate pointing errors and reduce losses related to optical inefficiencies.

Micius

Lu et al. (2022) analyze the effectiveness and success of the Micius satellite. They state that the Micius satellite is a practical application of QKD, managed by the Chinese Academy of Science (CAS) Strategic Priority Research Program on space science. Micius's goals include satellite-to-ground QKD, quantum entanglement distribution from satellite to two ground stations, and ground-to-satellite quantum teleportation. Lu et al. explain that, thus far, three key milestones have been achieved: satellite-to-ground decoy-state QKD with a reliable distance of up to 1200 km and satellite-replayed intercontinental key exchange, satellite-based entanglement distribution to two locations on the Earth separated by 1205 km, and ground-to-satellite quantum teleportation of photons. These milestones represent the feasibility of QKD as a means to overcome existing security concerns with space systems.

Lu et al. (2022) state that the first goal after launching Micius was to establish a space to ground quantum link and perform QKD from the satellite to the ground station. Micius successfully established a quantum link between the satellite and the Xinglong ground station with a diffraction loss of approximately 22 dB at 1200 kilometers. Liao et al. (2017) affirm this, achieving a rate of approximately one kHz over a distance of up to 1200 kilometers. However, Lu et al. (2022) state that this success came with the confirmation that such a challenge requires a fast and precise APT to overcome to beam divergence and other challenges. Furthermore, determining the space to ground clock drift is essential, as it allowed them to filter the background noise and achieve more reliable results.

In addition to the success of the space to ground quantum linking goal, Lu et al. (2022) state that the second mission was to achieve satellite-based entanglement distribution. They state that current challenges limited entanglement distribution over terrestrial distances to about 300 kilometers. Initial experimental results were insufficient to achieve entanglement-based quantum cryptography due to a low-key rate and a high quantum bit error rate of 8.1%. However, Lu et al. notes that after significant upgrades to the ground station's telescopes, additional experimentation produced much better results with a significantly increased key rate and a quantum bit error rate reduced from 8.1% to 4.5%, well within expected limits. Liao et al. (2017) confirm that since September 2016, Micius has reliably performed successful QKD. They state that even at 1200 kilometers, they were successful in achieving a key rate of approximately 1 kbit per second.

Importantly, Lu et al. (2022) indicate that the Micius satellite also served as a trustful relay to connect multiple points on Earth in a high-security QKD exchange network. In the experiment, they explored distribution between Xinglong and Graz ground station near Vienna. By performing a bitwise exclusive OR operation on the random keys shared between Micius and the two ground stations, Micius yields and sends a new string through traditional communications channels, enabling the decoding of other original keys using another exclusive OR operation. Lu et al. note that after Micius distributed a key with both Graz and Xinglong, performing the bitwise exclusive OR between each key and sending the combined key to Xinglong enabled them to combine the keys and end up with an identical key provided to Graz.

As these keys are known only to the communicating parties and the satellite, the satellite acts as a secure and trusted relay to communicate over great distances while appreciating the benefits of QKD. To demonstrate this, Lu et al. explained that the experiment established a 100 kB secure key between Xinglong and Graz. Xinglong and Graz used 10kB of the key to transmit a picture with a size of 5.34 kB to Vienna, and another picture with a size of 4.9 kB to Beijing, with the other 70 kB combined with AES-128 protocol and used in a video conference between Beijing and Vienna. This experiment represented a relative success in ultra-secure communications using a combination of traditional cryptography and QKD. Liao et al. (2017) indicate that future plans include launching higher orbit satellite constellations to improve distance and coverage area, requiring larger telescopes, better APT systems, and more efficient optics. They also state the inclusion of international partners in sharing quantum keys for secure communications and experimentation.

Overcoming Challenges in Deploying Quantum Key Distribution in Space

As legacy space systems in use continue to age, security must be at the forefront of policy and development in space endeavors. Utilizing QKD in space is shown to be highly secure and feasible but comes with a substantial cost. These costs include development and research, manufacturing, building, and staffing of space systems. Furthermore, a represented need for ultra-secure communications is necessary to qualify the prohibitive costs of deployment. As quantum computing advances past the theoretical and into the experimental realms of science, this need is ever present. Traditional cryptography will soon be obsolete, leaving communications to require quantum-resistant cryptography such as QKD.

While the Micius satellite required a significant amount of space to achieve its stated missions, Li et al. (2022) state that by utilizing CubeSats in a satellite constellation similar to a Starlink constellation, size, weight, and cost of each satellite can be significantly reduced. CubeSats promise to be a much more appealing approach to QKD deployment. This presents the benefit of expanding the reach of QKD while significantly reducing the total cost of deployment. Shorter distances between each satellite in the constellation can theoretically improve the efficiency of each individual node. Li et al. note that the performance of these theoretical constellations remains unknown due to the lack of experimental verification. However, they show during experimentation that such a CubeSat can be an efficient means of performing QKD, with relative successes appreciated between four ground stations using a payload with a size of only 0.190m^3. With this in mind, stakeholders should establish additional experiments to study the feasibility of QKD in CubeSat constellations to achieve secure global communications.

International cooperation is necessary to overcome the scaling challenges to QKD. Liao et al. (2017) exhibits the benefits of their partnerships with international ground stations in establishing efficient QKD and experimentation of the practical applications of QKD across great distances. Satellite communications often include diplomatic, military, and industrial strategic considerations. Ensuring that international partners are participating in the development of ultra-secure technologies presents a united front to adversaries who may seek to disrupt these activities. In doing so, stakeholders can ensure that the international community as a whole appreciates the benefits of QKD and help share the costs of deployment amongst all parties.

One significant challenge that remains problematic for any solution is the integration of older space systems into a newer cryptographic scheme. Researchers can overcome this challenge by developing a dedicated bridge satellite that is both integrated into the QKD network and carries backwards compatibility with older satellite encryption technologies. By exploiting QKD, the bridge satellite can calculate a unique checksum by utilizing the inherent error rate in QKD, ensuring that each new quantum key provides a new checksum without needing input from ground station controllers. The network can then utilize the unique checksum to enhance the confidentiality of traditional cryptographic systems between the bridge satellite and the legacy satellite, considering any communications that do not include the dedicated checksum insecure. Due to the one-way generation of the checksum, even if an adversary compromises the communication channel or the checksum between the bridge satellite and the legacy satellite, the quantum key is not at risk.

Conclusion

Despite decades of experimentation and research, Quantum Key Distribution remains enigmatic in modern cryptography. Though researchers have made great strides, stakeholders must conduct additional research and experimentation to overcome the proposed challenges in this analysis. Preparation, dedication, and international collaboration with key private sector stakeholders, who can drive technology development and provide critical funding, are crucial.

Overcoming these challenges can pave the way for secure technologies resilient to the inherent vulnerabilities in traditional cryptography. In doing so, satellite technologies can be secured against traditional cryptographic drawbacks and emerging tech in quantum computing. Utilizing QKD can assure ultra-secure communications, theoretically eliminating the possibility of eavesdropping and interference. Bridging the gap between QKD and traditional cryptography enhances the security of both older and newer space technologies. By ensuring the security of space communications, reducing costs through collaboration and innovation, and providing backwards compatibility with legacy systems, the future is set for global communications that are not only secure, but universally trusted.

References

Bennett, C.H. & Brassard, G. (1989, October 29). The dawn of a new era for quantum cryptography: The experimental prototype is working! *ACM SIGACT News, 20*(4), 78-80. https://doi.org/10.1145/74074.74087

Harmon, S. (2023). *Implications of a cyber attack on satellite infrastructure* [Unpublished manuscript]. Department of Accountancy, Finance, and Information Systems, Ferris State University.

Li, Y., Liao, S.-K., Cao, Y., Ren, J.-G., Liu, W.-Y., Yin, J., Shen, Q., Qiang, J., Zhang, L., Yong, H.-L., Lin, J., Li, F.-Z., Xi, T., Li, L., Shu, R., Zhang, Q., Chen, Y.-A., Lu, C.-Y., Liu, N.-L., … & Pan, J.-W. (2022, August 18). Space-ground QKD network based on a compact payload and medium-inclination orbit. *Optica, 9*(8), 933-938. https://doi.org/10.1364/OPTICA.458330

Liao, S.-K., Cai, W.-Q., Liu, W.-Y., Zhang, L., Li, Y., Ren, J.-G., Yin, J., Shen, Q., Cao, Y., Li, Z.-P., Li, F.-Z., Chen, X.-W., Sun, L.-H., Jia, J.-J., Wu, J.-C., Jiang, X.-J., Wang, J.-F., Huang, Y.-M., Wang, Q., … & Pan. J.-W. (2017, August 9). Satellite-to-ground quantum key distribution. *Nature*, *549*, 43-47. https://doi.org/10.1038/nature23655

Lindsay, J.R. (2020, Summer). Surviving the quantum cryptocalypse. *Strategic Studies Quarterly, 14*(2), 49-73. https://www.jstor.org/stable/26915277

Lu, C.-Y., Cao, Y., Peng, C.-Z., Pan, J.-W. (2022, July 6). Micius quantum experiments in space. *Reviews of Modern Physics*, *94*(3). https://doi.org/10.1103/RevModPhys.94.035001

Mafu, M. & Senekane, M. (2018, May 30). Security of quantum key distribution protocols. In S. Gnatyuk (Ed.), *Advanced technologies of quantum key distribution* (pp. 3-15). IntechOpen. https://doi.org/10.5772/intechopen.74234

Zhang, Q., Xu, F., Chen, Y.-A., Peng, C.-Z., Pan, J.-W. (2018, August 31). Large scale quantum key distribution: Challenges and solutions. *Optics Express*, *26*(18), 24260-24273. https://doi.org/10.1364/OE.26.024260