SSC18-WKVI-08

Global quantum key distribution using CubeSat-based photon sources

David Mitlyng
S-fifteen Space Systems
1550 Larimer Street, Suite 293, Denver, CO 80202; +1-650-704-5650
david@s15.space

Robert Bedington
S-fifteen Space Systems
S15-02-10, 3 Science Drive 2, Singapore 117543; +65 8371 0458
rob@s15.space

ABSTRACT

The future of secure communication networks relies on the secure distribution of symmetric encryption keys. Current methods of distributing keys are either vulnerable (public key encryption has the capability of being cracked with quantum computers) or are expensive (couriers physically delivering keys to remote locations). The most secure method is to distribute keys from small satellites using Quantum Key Distribution (QKD). S15 Space Systems is a spin-off company that is developing space-based, quantum-safe communications built on research performed at the Centre for Quantum Technologies (CQT) at the National University of Singapore. The team is developing technologies such as QKD which harness unique properties of quantum physics to enable highly secured encryption services. QKD can generate encryption keys that are secure against computational hacks and that can be distributed to remote parties with solid guarantees that they have not been intercepted by man-in-the-middle eavesdroppers. Quantum light source hardware is being developed that fits on a 3U CubeSat, and a small constellation of these satellites can effectively service thousands of users.

INTRODUCTION

Currently, most encryption keys derive their security from complex mathematical functions that require unfeasibly large classical computers to crack, but quantum computers are coming online soon that will compromise many of these keys. Since QKD derives its security from symmetric keys that are fundamentally random and fundamentally private it is provably secure against future computational developments. QKD requires that information be transmitted optically, typically with bits encoded in individual photons that must be uniquely distinguished and timestamped at the transmitter and receiver. Accordingly the signals are very weak and susceptible to loss compared with classical laser communications. Within optical fibers they are restricted to distances of 50-100km before physically secured, trusted repeater stations are required. Using free-space optics the losses are lower and by delivering QKD from space the entire world can be connected securely.

With today's existing network, communications between two distant parties (called Alice and Bob in typical cryptography parlance) can be easily intercepted by an unwanted third party (also known as Eve, short for eavesdropper). To thwart Eve, Alice and Bob encrypt their sensitive message with a symmetric encryption key that only they know (symmetric because the same key is used to encrypt and decrypt the message). Eve can intercept the encrypted message, but can't decrypt it – not yet, anyway.

Because Alice and Bob need a new key for each message, they rely on public key encryption (PKE) for the efficient distribution of keys. PKE uses public-private key pairs consisting of a public key that is available to everybody, and a private key that is buried in the public key. The public key is designed as a trap-door function: it is easily created from the private key, but the private key cannot be easily found from the public key. An example of a trap-door function commonly used for PKE is multiplication of two large prime numbers to create a third, larger, non-prime number. Once you know this large number, it is incredibly hard to factor out the two prime numbers.

Eve can intercept Alice and Bob's public key but cannot extract their private key. But quantum computers, new algorithms and sudden unexpected advances in classical computing capabilities could give Eve the capability to crack PKE.[1]

But a new system is necessary that utilizes secure channels that cannot be intercepted for key delivery. It should be noted that keys are not actually delivered in

QKD – they are created as part of the QKD process. This is more secure than existing systems where keys are delivered across the open network, making them susceptible to interception.

These encryption keys can then safely encrypt and decrypt messages that are sent over normal communications channels.

TYPES OF QKD

There are different types QKD that mainly stem from two principles: Prepare-and-Measure, and Entanglement. The former exploits quantum indeterminacy to prevent an eavesdropper from measuring the quantum state of the photon (which encodes the bit of information) without changing it. In the latter, two photons are linked (entangled) such that measuring the state of one photon affects the state of the other.

Prepare-and-Measure Protocols

The foundational Prepare-and-Measure protocol is known as BB84, after the paper written by Charles Bennett and Gilles Brassard in 1984.[2] It relies on the uncertainty principle, where the act of measuring a photon's polarization is an integral part of quantum mechanics, not just a passive, external process, as in classical physics. In this scheme, the transmitting party, Alice, encodes the bits of the encryption key through the polarization of individual photons. Alice sends these photons to the receiver, Bob, through a weak coherent pulse that is generated with specially modified lasers. Bob receives these photons, measures the polarization states, and, after protocol checks with Alice, verifies they both have the same unique, random, encryption key. These checks (parameter estimation, error correction, and privacy amplification) are performed over a normal (but authenticated) communications channel.

Eve may be sitting outside of Bob's compound and receive the same photons but has to guess at the polarization to measure (either linear or diagonal). Only Alice and Bob know the correct polarization to measure and the measurement results and will quickly discover and discard any key that has been compromised by Eve.

Prepare-and-Measure QKD has been demonstrated with laser hardware that emits pulses at such a low power that very small numbers of photons (ideally, one) are sent per pulse. Because of this, Prepare-and-Measure QKD is also known as weak coherent pulse QKD.

Entanglement-based Protocol

The first Entanglement-based protocol, known as E91 after the 1991 Artur Ekert paper, takes advantage of entanglement.[3] Pairs of entangled photons are created and sent to Alice and Bob, who measure their correlated polarizations. If Eve intercepts one of the pairs, the entanglement is broken, introducing errors and making Eve's presence detectable.

In contrast to Prepare-and-Measure schemes, there is no active choice required when encoding states into the photons. Instead, both parties are recipients who share a source of maximally entangled photon pairs, the generation of which is a truly random process. Typical implementations utilize photon pairs entangled in the polarization degree of freedom, and the photon pair is split such that one photon is transmitted to Alice, while its twin is transmitted to Bob. Both parties make independent measurement choices on the photons and decide to measure them in either the diagonal or horizontal basis. Alice and Bob still need to perform clear channel checks in the same manner as in the Prepare-and-Measure protocol. However, no random number generators are required to prepare the source, and the measurement devices for Alice and Bob are identical.

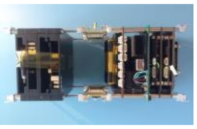
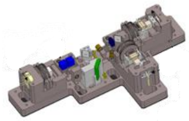
QKD FROM A CUBESAT

QKD Hardware

S15 Space's primary QKD system uses an entangled-photon quantum light source based on the flight-proven small photon entangling system (SPEQS) developed at CQT. SPEQS was designed as a compact and rugged package to generate and analyze photon-pairs produced using Spontaneous Parametric Down Conversion (SPDC). The SPEQS package contains a laser and crystals, which produce the photon pairs, as well as single photon detectors with polarization analyzers to detect them.[4]

This SPEQS design has heritage from the on-orbit demonstration on the Galassia mission in 2016, high-altitude demonstrations in 2012 and 2014, and lab and long-distance terrestrial demonstrations over a decade ago. A summary of this heritage is shown in Table 1.

Table 1: Quantum light source heritage from CQT

Year	Mission	
2012	Basic miniature spontaneous parametric down-conversion (SPDC) source demonstrated by high-altitude balloon.[5]	
2013	Correlated SPDC pair source demonstrated by high-altitude balloon.[6]	
2014	Space-qualified, correlated, SPDC source launched on GomX-2, survived launch failure.[7]	
2016	Space-qualified, correlated, SPDC source demonstrated on Galassia CubeSat.[8]	
2019 (planned)	Demonstration of entangled photon pair source in space on SpooQySat CubeSat.[10]	

Each successive mission gradually raises the technology readiness level of the photon pair sources. Initial iterations developed the miniaturized electronics and ruggedized optics. These led onto on-orbit tests of a correlate photon pair source, producing photons that are not entangled in polarization but may have entanglement in other degrees of freedom (e.g. time-frequency).Error! Reference source not found.

The most advanced SPEQS design is slated for launch on the SpooQySat CubeSat in late 2018.[9] This polarization entangled version of SPEQS features a custom isostatic and thermally isolating mounting system to try and reduce the performance variation of the device. The engineering model of SpooQy-1 with a structural model SPEQS payload is shown in Figure 1.

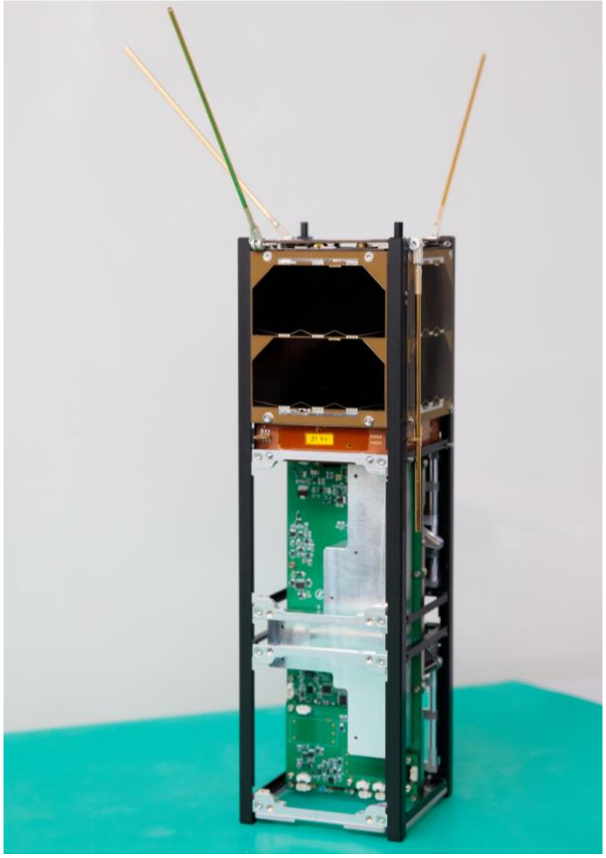


Figure 1. Engineering model of SpooQySat with structural model SPEQS Payload (panels removed for display purposes)

Follow-on CubeSats will further establish the space worthiness of the source and beam photons out of the satellite to perform QKD. The next mission is planned for a launch on a CubeSat in 2020 and should demonstrate satellite-to-ground entanglement distribution and QKD.

Concept of Operations

QKD is most useful to ensure secure communications between two distant ground stations. A CubeSat operating in a LEO orbit doesn’t typically have a simultaneous view of two distant ground stations at the same time. So the trusted node QKD method is used. The CubeSat first distributes keys between the satellite and each ground station in turn. Then by using a mathematical operator within the satellite (which knows both keys), both ground stations will get symmetric keys. This protocol requires that the satellite knows both keys, which means the satellite must be trusted to be secure by ground stations; this is termed a trusted node.

The concept of operations for LEO trusted node QKD is shown in Figure 2.

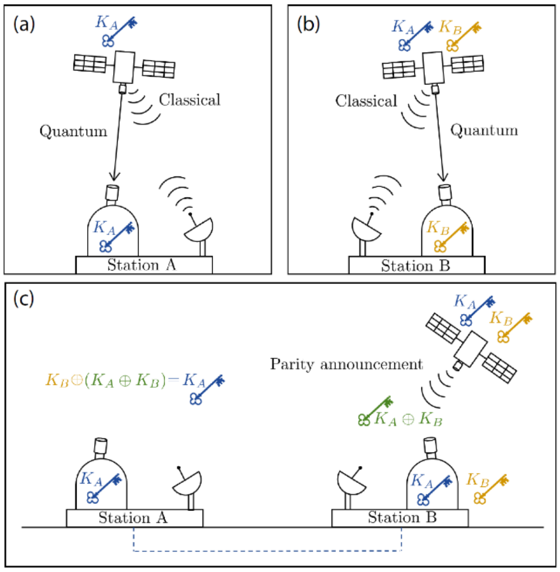


Figure 2. Trusted Node QKD ConOps (originally published in reference 11)

Panel (a): Satellite passes over the first ground station (Station A) and establishes a shared secret key K_A running the QKD protocol.

Panel (b): Satellite passes over the second ground station (Station B) and establishes a shared secret key K_B with running the QKD protocol.

Panel (c): Satellite holds both keys (K_A and K_B), while Stations A and B knows only their own. Satellite publicly announces the parity of both keys $K_A \oplus K_B$, which allows Station B to determine key K_A

Both Station A and Station B now have the shared symmetric encryption key K_A, which can then be used to encrypt private communications between A and B. Keys generated through QKD are unique and random each time so there is no way to send K_A directly to station by using QKD alone

In principal, a single LEO satellite of this kind, in a polar orbit, can service the entire world, with revisit times and throughputs increased by launching additional satellites. This provides an economical way to roll out a QKD service, particularly for early adopters to this system. Even though the number of passes is irregular (maybe once a week, accounting for statistical cloud cover at both stations), many keys can be delivered per pass (depending on the size of the satellite and receivers).

CONCLUSIONS

A QKD satellite network deployed through CubeSats or other small satellites provides an important part of the future of secure communications. This technology is at sufficient technology readiness to ensure that a basic network can be deployed in the next five years, just in time to head off the vulnerabilities of existing key distribution systems.

Acknowledgments

This work is supported by the Centre for Quantum Technologies (CQT) and the National University of Singapore. The SpooQy-1 mission is partially supported by the National Research Foundation, Prime Minister's Office, Singapore (under the Research Centres of Excellence programme and through Award No. NRF-CRP12-2013-02) and by the Singapore Ministry of Education (partly through the Academic Research Fund Tier 3 MOE2012-T3-1-009).

References

1. P.W. Shor, Algorithms for quantum computation: discrete logarithms and factoring, In: Proceedings 35th Annual Symposium on Foundations of Computer Science, IEEE, 1994, pp. 124–134.
2. C.H. Bennett, G. Brassard, Quantum Cryptography: public key distribution and coin tossing, In: International Conference on Computers, Systems & Signal Processing, 1984, pp. 175–179.
3. A.K. Ekert, Quantum cryptography based on Bell's theorem, Phys. Rev. Lett. 67 (1991) 661–663.
4. K. Durak, et al., The next iteration of the small photon entangling quantum system (SPEQS-2.0), In: Advances in Photonics of Quantum Computing, Memory, and Communication IX, SPIE, 2016.
5. W. Morong, A. Ling, D. Oi, Quantum optics for space platforms, Optic Photon. News 23 (10) (2012) 42.
6. Z. Tang, R. Chandrasekara, Y.Y. Sean, C. Cheng, C. Wildfeuer, A. Ling, Near-space flight of a correlated photon system, Sci. Rep. 4 (6366) (2014).
7. Z. Tang, et al., The photon pair source that survived a rocket explosion, Sci. Rep. 6 (1) (2016) 25603.
8. Z. Tang, et al., Generation and analysis of correlated pairs of photons onboard a nanosatellite, Phys. Rev.Appl 5 (054022) (2016).
9. R. Bedington, X. Bai, E. Truong-Cao, Y.C. Tan, K. Durak, A. Villar Zafra, A. Ling, Nanosatellite experiments to enable future space-based QKD missions, EPJ Quant.Technol. 3 (1) (2016).

10. R. Chandrasekara, et al., Generation and Analysis of Correlated Pairs of Photons on Board a Nanoscatellite, 9996, Quantum Information Science and Technology II, Proceedings of SPIE, 2016.

11. R. Bedington, J.M Arrazola, A. Ling, Progress in Quantum Key Distribution, NPJ Quantum Information, 2017.