entropy

MDPI

Article

Satellite Quantum Communications When Man-in-the-Middle Attacks Are Excluded

Tom Vergoossen [1], Robert Bedington [1], James A. Grieve [1] and Alexander Ling [1,2,*]

[1] Centre for Quantum Technologies, National University of Singapore, Singapore 117543, Singapore; cqttv@nus.edu.sg (T.V.); r.bedington@nus.edu.sg (R.B.); james.grieve@nus.edu.sg (J.A.G.)
[2] Department of Physics, National University of Singapore, Singapore 117543, Singapore
* Correspondence: cqtalej@nus.edu.sg; Tel.: +65-65162985

Received: 15 March 2019; Accepted: 9 April 2019; Published: 10 April 2019

Abstract: An application of quantum communications is the transmission of qubits to create shared symmetric encryption keys in a process called quantum key distribution (QKD). Contrary to public-private key encryption, symmetric encryption is considered safe from (quantum) computing attacks, i.e. it provides forward security and is thus attractive for secure communications. In this paper we argue that for free-space quantum communications, especially with satellites, if one assumes that man-in-the-middle attacks can be detected by classical channel monitoring techniques, simplified quantum communications protocols and hardware systems can be implemented that offer improved key rates. We term these protocols photon key distribution (PKD) to differentiate them from the standard QKD protocols. We identify three types of photon sources and calculate asymptotic secret key rates for PKD protocols and compare them to their QKD counterparts. PKD protocols use only one measurement basis which we show roughly doubles the key rates. Furthermore, with the relaxed security assumptions one can establish keys at very high losses, in contrast to QKD where at the same losses privacy amplification would make key generation impossible.

Keywords: quantum communication; quantum cryptography; quantum key distribution; satellite QKD; access control; threat model; photon key distribution; PKD

1. Introduction

Cryptographic key distribution is a major application of quantum communication. Such schemes typically use measurements of quantum states of photons shared between two remote parties to allow both sides to derive shared entropy that can be quantitatively assessed to be private. This shared entropy may be used as keying material for use as one time pads [1] or as seed keys for symmetric encryption [2]. Quantum key distribution relies on the transmission of single photons so many photons must be distributed to generate a key over lossy channels. For shorter distances and metropolitan regions photons can be distributed between parties using optical fibres, but for global distances satellite-based nodes become more practical [3]. For quantum communication from satellites, and other moving platforms, photons are distributed using free space optics (FSO).

Quantum key distribution schemes [4,5] have extremely strong security guarantees due to minimal assumptions on the capabilities of the technology available to potential eavesdroppers—essentially any attack permitted by the laws of physics is deemed possible. Although typically the two communicating parties must trust the quantum key distribution (QKD) hardware within their control, they need not trust the optical channel between them because they can detect any attempt at eavesdropping and any man-in-the-middle attacks on the channel using statistical tests that are inherent to the QKD process. These tests require a fraction of the received photons to be discarded such that they cannot be used in the final keying material. This discarding arises in processes such as basis reconciliation, parameter estimation and privacy amplification. In many situations these discarded photons and slower key rates are a necessity for security e.g., in a metropolitan environment where QKD is performed over optical fibres which pass through many ducts and underground passages where, in principle, eavesdropping can take place.

For the case of satellite QKD (and other FSO delivery methods), where there is a direct line of sight, these measures seem to be harder to justify. To compromise the security of the link, other than disrupting it through denial-of-service attacks, an adversary would have to act as a man-in-the-middle. We argue that performing this attack for an optical link between a low earth orbit (LEO) satellite and ground station would be physically possible, but technically not feasible for most adversaries. It requires intercepting and re-sending a beam that is only a few metres across and rapidly tracking across the sky without being detected. Practical satellite-ground links employ dual tracking beacons to establish the required high accuracy pointing link, effectively providing a channel monitoring system. Additional hardware may be deployed to monitor the channel in other wavelengths, e.g., radar systems or thermal imaging cameras. Furthermore, space-situational awareness has led to publicly accessible catalogues that provide ephemeris data of orbiting space objects which are frequently updated, making it possible to assess if any (publicly known) satellites can threaten the link in space. If users fear that their adversaries could have technologies which can covertly intercept the link they could of course use QKD; other users can relax their threat assumptions. In light of the above we thus focus only on passive eavesdroppers, attackers which cannot be detected by channel monitoring techniques. As we will show, using this updated threat model simplifies the key delivery protocol.

In this paper we term the simplified quantum communication schemes that address this scenario as 'photon key distribution' (PKD) so as to separate them from conventional QKD protocols. Some more recent QKD schemes, where the security proofs may not yet be completely agreed, may also prove to be somewhere on the PKD to QKD spectrum depending on the security assumptions they require. While most QKD schemes use two bases for encoding, in our PKD schemes only a single encoding basis is used since mixed bases are primarily a mechanism to detect man-in-the-middle attacks. This avoids the basis reconciliation sifting stage and so is more efficient in its use of photons.

Sasaki et al. have previously discussed the opportunity for simplified cryptography schemes that fall between QKD and laser communications [6]. As they explain QKD (and PKD) fit within the wider field of physical layer security methods. These encompass such techniques as wiretap channels [7] and radio frequency equivalents [8], to laser-based methods that actively quantify the amount of information an eavesdropper can receive [9]. Our exploration of PKD here builds on the ideas put forward by Sasaki et al.

In this paper we look at the asymptotic secret key rates at high losses (i.e., long distance free space links) for three QKD schemes using three different kinds of transmitter hardware, and compare this to three simplified PKD schemes that use similar hardware. The simplified schemes are primarily targeted at satellite applications and all assume that a covert man-in-the-middle attack has been assessed to be non-existent. As expected, they are all found to remain effective at higher losses than their QKD counterparts.

2. Results

Table 1 shows a summary of the hardware types and corresponding QKD and PKD methods considered. Figure 1 shows a comparison of the quantum bit error rate (QBER) and bits per pulse achieved with these methods at increasing distances (losses). In this way the results can be presented independently of the pulse rate of any particular hardware setup. Although we use the term 'pulse' here for straightforwardness of comparison, the spontaneous parametric down conversion (SPDC) sources we consider are operated by a continuous-wave pump, i.e., not pulsed, and produce photon pairs on a stochastic basis, so 'detection events' would be the more appropriate term. Figure 1a,b show that for QKD protocols (BB84, BBM92) there is a sharp drop off in key rate as losses increase. At high losses more key has to be discarded in privacy amplification than is available so the secure key rate drops to zero. This does not happen in the PKD equivalents as it is assumed that there are no active man-in-the-middle attacks, and so privacy amplification is only required for multi-photon pulses.

Table 1. Quantum key distribution (QKD) and photon key distribution (PKD) methods modelled for different hardware implementations.

Photon Source	QKD Protocol	PKD Encoding (Example)
Weak coherent pulse (WCP)	Decoy state BB84	Pulse position modulation (PPM)
Spontaneous parametric down conversion (SPDC) pairs	BBM92 (entanglement-based BB84)	Heralded Left or Right-handed polarized photons
Ideal single photon source (SPS)	Single photon BB84	Left or Right-handed polarized photons

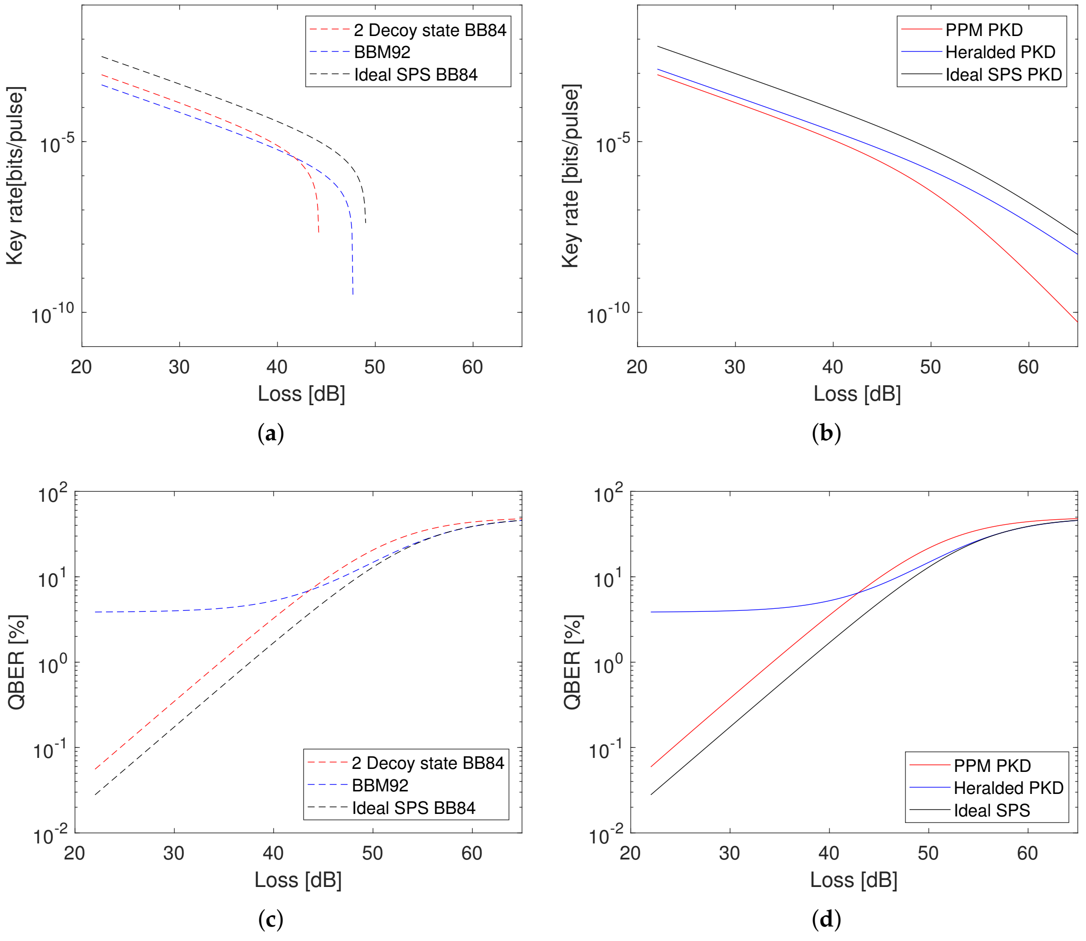

Figure 1. Modelling results for schemes described in Table 1. Assumptions are discussed in Section 3. (**a**) Key generation rate for quantum key distribution (QKD) protocols: decoy state BB84, BBM92, and BB84 using an ideal single photon source (SPS); (**b**) Key generation rate for photon key distribution (PKD) schemes: pulse-position modulated (PPM) photon key distribution (PKD), PKD with a heralded photon source, and PKD using an ideal SPS; (**c**) Quantum bit error rate (QBER) for QKD protocols; (**d**) QBER for simplified PKD schemes.

3. Discussion

The results are discussed in the sections below based on the different hardware types. General assumptions were that space-based detectors have 15,000 dark counts per second while ground-based detectors have 2500 dark counts per second. This was based on pessimistic cases for single photon detectors before and after radiation damage [10]. Furthermore, ground-based detectors were assumed to have an additional 1000 background counts per second due to scattered light entering the receiver. This was slightly more conservative than noise counts estimated in recent literature [11]. All sources were assumed to have perfect visibility, e.g., for a SPDC source this means it was assumed to produce perfectly entangled states.

3.1. Weak Coherent Pulse (WCP) Source

Satellite-to-ground decoy state QKD using a weak coherent pulse (WCP) source has conclusively been demonstrated on the Micius satellite in 2016 [12] and the QUBE mission aims to demonstrate a WCP QKD system on a nanosatellite [13]. WCP sources are highly attenuated lasers which approximate a single photon state although multi-photon emissions are possible. We used the Micius source parameters as a realistic assumption in our model; on average our source emitted 0.8 photons per pulse. For QKD it performed the decoy state BB84 protocol [14] where it also emitted decoy states of mean photon number 0.1, and operated at a ratio of 0.5:0.25:0.25 for signal, decoy and vacuum states.

For WCP PKD, no decoy states were transmitted, only signal states with an optimized mean photon number of between 0.4701 and 0.4583 for losses of 20–70 dB. These were assumed to be coupled to a modulator that enables pulse position modulation (PPM) to encode bits as early (bit 0) or late pulses (bit 1). Compared to polarization encoding this also removes the requirement to synchronize polarization reference frames which is especially convenient for then communicating to satellites.

3.2. Spontaneous Parametric Down Conversion (SPDC) Photon Pair Source

For the QKD protocols considered here the SPDC photon pair source was assumed to be an entangled photon pair source performing the BBM92 protocol [15,16]. The Micius satellite demonstrated an entangled photon pair source in orbit [17,18] and the SpooQy-1 nanosatellite will demonstrate a miniaturized device in orbit in 2019 [19]. The PKD protocols with this setup can use the same hardware or a simpler correlated (heralded) photon pair source, with unit visibility, such as the miniaturized device flown on the Galassia nanosatellite [20]. To avoid synchronising reference frames the two-state encoding could be in left and right hand circular polarization.

Protocols using pair sources require two detections i.e., one of the pair must be detected at the source and the other of the pair detected at the receiver. The total detection efficiency at the source was assumed to be 25% (i.e., there was a system loss of -6 dB). The main effect of this approach is that the quantum bit error rate (QBER) partly becomes a function of the accidental rate of coincident detection between the two detectors. This accidentals rate is given by $S_1 \times S_2 \times \tau$ [21,22], where S_1 and S_2 are the singles rates observed at the detectors, and τ the timing coincidence window.

In this study, we assume that the source was capable of producing photon pairs at a raw rate of 1×10^8 per second into a single spatial mode, and that the timing resolution was 1 ns, which are readily accessible [23]. This leads to a QBER that is between 3% and 4%; this QBER has a linear relationship with the timing window—faster electronics will lead to smaller QBER. An advantage of using photon pairs is that the probability of multi-photon emission is insignificant (similar to single photon sources), leading to a smaller percentage of the raw key being discarded in privacy amplification.

3.3. Single Photon Source (SPS)

The SPS was assumed to be a perfect device that produces single photons on demand and never multi-photon pulses. For QKD this means it can perform the BB84 [24] protocol without any requirement for decoy states. For PKD it can even be encoded in wavelength giving a broad scope for multiplexing. In both cases the SPS has the highest rates. It should be noted that compared to the other technologies SPS devices are currently at low ‘technology readiness levels’ [25] or only work at cryogenic temperatures which means they are not a practical choice for deployment in space.

3.4. Summary

The PKD protocols have higher rates than the QKD protocols because eavesdroppers have no access to the channel and only 'collective attacks' are allowed. That means if there are no multi-photon emissions (i.e., not using the WCP source) no privacy amplification is required. PPM PKD suffers from multi-photon emissions so requires privacy amplification. In general the relaxed security assumptions increase key rates and allow for key generation at larger distances. Comparing between different hardware methods of PKD (or between different hardware methods of QKD) is less conclusive, since the 'pulse' rates of different implementations of the hardware will vary.

4. Materials and Methods

The decoy state BB84 equations used are those published in reference [14], and the BBM92 equations are those from reference [26].

The equation for PPM PKD is derived from the Devetak–Winter bound for collective attack for a simplified coherent one way (COW) PPM scheme with decoys from Appendix B of reference [27]. All parts due to decoy are set to neutral, and an error correction term is added to the equation. The final key rate is thus

$$R(\mu_{opt}) = g(\zeta) \times \frac{t}{(1-t)} \times \eta \times (1 - H_2(QBER) \times f_E) \times f_{source} \tag{1}$$

where $g(\zeta)$ is a privacy amplification term corresponding to the optimized mean photon number $\mu_{opt} = \frac{\zeta}{1-t}$. η is the detection efficiency, f_{source} is the source frequency and t is the transmissivity.

5. Conclusions

The approach presented in this paper can be applied to key distribution, not only when using satellites, but also in other types of FSO-based systems. For example, in ad-hoc networks where the transmitter and receiver can visually identify each other, it may be straightforward to assess the absence of a man-in-the-middle and use PKD type protocols to establish a secret key. If the possibility of man-in-the-middle attacks can be excluded or monitored by conventional means, then PKD protocols can allow for secure key distribution using quantum communication methods at increased losses using similar or simplified hardware. In a practical key distribution scenario, it is worthwhile to have a better specification of the threat model and to devote efforts in closing physical side-channels, rather than attempting to defeat a hypothetical quantum adversary. Finally, we remark that using QKD hardware it may be possible to switch to a PKD protocol when the channel is assessed to be free of active attacks, and thus increase key distribution rates.

6. Patents

A patent has been filed for the heralded source key distribution method.

Author Contributions: Conceptualization: R.B., J.A.G. and A.L.; Data curation: T.V.; formal analysis: T.V.; funding acquisition: A.L.; Investigation: T.V.; methodology: T.V.; project administration: R.B. and A.L.; resources: A.L.; software: T.V.; supervision: R.B. and A.L.; validation: T.V.; visualization: T.V.; writing—original draft: T.V. and R.B.; writing—review and editing: T.V., R.B., J.A.G. and A.L.

Funding: This work 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).

Acknowledgments: We thank Charles Lim and Ignatius William Primaatmaja for their valuable feedback and suggestions.

Conflicts of Interest: The authors declare no conflict of interest. The funders had no role in the design of the study; in the collection, analyses, or interpretation of data; in the writing of the manuscript, or in the decision to publish the results.

Abbreviations

The following abbreviations are used in this manuscript:

QKD	Quantum key distrbution
FSO	Free space optics
PKD	Photon key distribution
SPS	Single photon source
WCP	Weak coherent pulse
PPM	Pulse position modulation
BB84	Bennett Brassard 1984 (QKD protocol [24])
BBM92	Bennett Brassard Mermin 1992 (QKD protocol [15])
QBER	Quantum bit error rate
COW	Coherent one way (QKD protocol [27])
SPDC	Spontaneous parametric down conversion

References

1. Vernam, G.S. Cipher Printing Telegraph Systems For Secret Wire and Radio Telegraphic Communications. *Trans. Am. Inst. Electr. Eng.* **1926**, *XLV*, 295–301. [CrossRef]
2. Roback, E. *Advanced Encryption Standard (AES)*; Technical Report 141; National Institute of Standards and Technology: Gaithersburg, MD, USA, 2001; doi:10.6028/NIST.FIPS.197.
3. Bedington, R.; Arrazola, J.M.; Ling, A. Progress in satellite quantum key distribution. *NPJ Quantum Inf.* **2017**, *3*, 30. [CrossRef]
4. Gisin, N.; Ribordy, G.; Tittel, W.; Zbinden, H. Quantum cryptography. *Rev. Mod. Phys.* **2002**, *74*, 145–195. [CrossRef]
5. Diamanti, E.; Lo, H.K.; Qi, B.; Yuan, Z. Practical challenges in quantum key distribution. *NPJ Quantum Inf.* **2016**, *2*, 16025. [CrossRef]
6. Sasaki, M. Quantum networks: Where should we be heading? *Quantum Sci. Technol.* **2017**, *2*. [CrossRef]
7. Wyner, A.D. The Wire-Tap Channel. *Bell Syst. Tech. J.* **1975**, *54*, 1355–1387. [CrossRef]
8. Poor, H.V.; Schaefer, R.F. Wireless physical layer security. *Proc. Natl. Acad. Sci. USA* **2017**, *114*, 19–26. [CrossRef] [PubMed]
9. Fujiwara, M.; Ito, T.; Kitamura, M.; Endo, H.; Tsuzuki, O.; Toyoshima, M.; Takenaka, H.; Takayama, Y.; Shimizu, R.; Takeoka, M.; et al. Free-space optical wiretap channel and experimental secret key agreement in 7.8 km terrestrial link. *Opt. Express* **2018**, *26*, 19513–19523. [CrossRef]
10. Tan, Y.C.; Chandrasekara, R.; Cheng, C.; Ling, A. Silicon avalanche photodiode operation and lifetime analysis for small satellites. *Opt. Express* **2013**, *21*, 16946–16954. [CrossRef]
11. Bourgoin, J.P.; Meyer-Scott, E.; Higgins, B.L.; Helou, B.; Erven, C.; Hübel, H.; Kumar, B.; Hudson, D.; D'Souza, I.; Girard, R.; et al. A comprehensive design and performance analysis of low Earth orbit satellite quantum communication. *New J. Phys.* **2013**, *15*, 023006. [CrossRef]
12. 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.; et al. Satellite-to-ground quantum key distribution. *Nature* **2017**, *549*, 43–47. [CrossRef]
13. Haber, R.; Garbe, D.; Schilling, K.; Rosenfeld, W. QUBE—A CubeSat for Quantum Key Distribution Experiments. *Proc. AIAA/USU Conf. Small Satell.* **2018**, *49*. [CrossRef]
14. Ma, X.; Qi, B.; Zhao, Y.; Lo, H.K. Practical decoy state for quantum key distribution. *Phys. Rev. A* **2005**, *72*, 012326. [CrossRef]
15. Bennett, C.H.; Brassard, G.; Mermin, N.D. Quantum cryptography without Bell's theorem. *Phys. Rev. Lett.* **1992**, *68*, 557–559. [CrossRef]
16. Naughton, D.; Bedington, R.; Barraclough, S.; Islam, T.; Griffin, D.; Smith, B. Design considerations for an optical link supporting intersatellite quantum key distribution. *Opt. Eng.* **2019**, *58*, 016106. [CrossRef]
17. Yin, J.; Cao, Y.; Li, Y.H.; Liao, S.K.; Zhang, L.; Ren, J.G.; Cai, W.Q.; Liu, W.Y.; Li, B.; Dai, H.; et al. Satellite-based entanglement distribution over 1200 kilometers. *Science* **2017**, *356*, 1140–1144. [CrossRef]
18. Yin, J.; Cao, Y.; Li, Y.H.; Ren, J.G.; Liao, S.K.; Zhang, L.; Cai, W.Q.; Liu, W.Y.; Li, B.; Dai, H.; et al. Satellite-to-Ground Entanglement-Based Quantum Key Distribution. *Phys. Rev. Lett.* **2017**, *119*, 200501. [CrossRef]

19. Grieve, J.A.; Bedington, R.; Tang, Z.; Chandrasekara, R.C.; Ling, A. SpooQySats: CubeSats to demonstrate quantum key distribution technologies. *Acta Astronaut.* **2018**, *151*, 103–106. [CrossRef]
20. Tang, Z.; Chandrasekara, R.; Tan, Y.C.; Cheng, C.; Sha, L.; Hiang, G.C.; Oi, D.K.L.; Ling, A. Generation and Analysis of Correlated Pairs of Photons aboard a Nanosatellite. *Phys. Rev. Appl.* **2016**, *5*, 054022. [CrossRef]
21. Janossy, L. Rate of n-fold Accidental Coincidences. *Nature* **1944**, *153*, 165. [CrossRef]
22. Grieve, J.A.; Chandrasekara, R.; Tang, Z.; Cheng, C.; Ling, A. Correcting for accidental correlations in saturated avalanche photodiodes. *Opt. Express* **2016**, *24*, 3592. [CrossRef] [PubMed]
23. Cao, Y.; Li, Y.H.; Zou, W.J.; Li, Z.P.; Shen, Q.; Liao, S.K.; Ren, J.G.; Yin, J.; Chen, Y.A.; Peng, C.Z.; et al. Bell Test over Extremely High-Loss Channels: Towards Distributing Entangled Photon Pairs between Earth and the Moon. *Phys. Rev. Lett.* **2018**, *120*, 140405. [CrossRef]
24. Bennett, C.H.; Brassard, G. Quantum cryptography: Public key distribution and coin tossing. *Theor. Comput. Sci.* **2014**, *560*, 7–11. [CrossRef]
25. Vogl, T.; Lecamwasam, R.; Buchler, B.C.; Lu, Y.; Lam, P.K. Space-compatible cavity-enhanced single-photon generation with hexagonal boron nitride. *arXiv* **2019**, arXiv:1902.03019.
26. Ma, X.; Fung, C.H.F.; Lo, H.K. Quantum key distribution with entangled photon sources. *Phys. Rev.* **2007**, *76*, 012307. [CrossRef]
27. Branciard, C.; Gisin, N.; Lutkenhaus, N.; Scarani, V. Zero-Error Attacks and Detection Statistics in the Coherent One-Way Protocol for Quantum Cryptography. *Quant. Inf. Comput.* **2007**, *7*, 639–664. [CrossRef]