Industrial application for Global Quantum Communication

A Mirza[1] **and F. Petruccione**[1,2]
[1] *University of KwaZulu-Natal, Westville Campus, Durban, South Africa*
[2]*National Institute for Theoretical Physics, South Africa*

E-mail: mirzaa@ukzn.ac.za

Abstract. In the last decade the quantum communication community has witnessed great advances in photonic quantum cryptography technology with the research, development and commercialization of automated Quantum Key Distribution (QKD) devices. These first generation devices are however bottlenecked by the achievable spatial coverage. This is due to the intrinsic absorption of the quantum particle into the communication medium. As QKD is of paramount importance in the future ICT landscape, various innovative solutions have been developed and tested to expand the spatial coverage of these networks such as the QuantumCity initiative in Durban, South Africa. To expand this further into a global QKD-secured network, recent efforts have focussed on high-altitude free-space techniques through the use of satellites. This couples the QKD-secured Metropolitan Area Networks (MANs) with secured ground-to-satellite links as access points to a global network. Such a solution, however, has critical limitations that reduce its commercial feasibility. As parallel step to the development of satellite-based global QKD networks, we investigate the use of the commercial aircrafts' network as secure transport mechanisms in a global QKD network. This QKD-secured global network will provide a robust infrastructure to create, distribute and manage encryption keys between the MANs of the participating cities.

1. Introduction

Quantum Information Processing and Communication (QIPC) is a field of research and application that fuses the laws of quantum physics into the current ICT framework. This expands the limits of conventional ICT solutions to a point where the technological manipulation of information is limited only by the laws of physics [1]. Information can therefore be characterized, quantified and processed using the basic rules of quantum mechanics. Exploiting some of the fundamental features of the quantum world, such as Heisenberg's uncertainty principle, superposition and entanglement [1], QIPC is an enabling resource for future ICT solutions.

Quantum communication is the most mature QIPC technology at present. The field is spearheaded by quantum encryption or, more correctly named, Quantum Key Distribution (QKD). This is a secure method of transferring encryption keys between two distant parties. An encryption algorithm is a construct that scrambles data in a unique manner for a given input parameter, known as the key. Thus the security of the encryption process, and in turn the communication, is directly dependent on the security of the encryption key.

Conventional key distribution routines, such as the Deffie-Hellman method [2], use mathematical algorithms to encapsulate the key bits during its distribution process. Due to the mathematical nature of the scheme, it is susceptible through advances in computing power and future mathematical

discoveries. This compromises the future integrity and security of information encrypted in such a manner.

QKD, however, encodes the key bits using a physical parameter of a quantum two-level system (qubit). In this case, the qubit is the data carrier and hence any form of data retrieval requires a measurement of a physical property of the qubit. As the qubit evolves within a quantum regime, it obeys the respective laws and therefore provides an intrinsic level of security against eavesdropping. The measurements of certain parameters of a quantum system create perturbations in the various other characteristics of system. An eavesdropper will therefore necessarily need to defy the established laws of quantum mechanics in order to retrieve intelligible data while remaining unnoticed. Due to the fundamental quantum nature of the encoding, the QKD process has been shown to be resistant against any computational capacity of an adversary [3].

2. Quantum networks

QKD has traditionally been implemented within a point-to-point environment. This is due to the stringent requirements of the qubit. The intrinsic absorption within the communication channel, together with the current lack to regeneration abilities for an optical qubit, has limited the key distribution distance of a photon to a distance of 120 km [4] prior to being absorbed. Thus one of the major bottlenecks in the commercialization of QKD is the limited spatial coverage that QKD offers. Recent efforts have been made in developing QKD networks such as the Durban-QuantumCity project [5], SECOQC [6], SwissQuantum [7] and Tokyo QKD network [8]. The QuantumCity initiative was launched in 2009 and is still currently operational. It is a star-topology network comprising of four nodes and running along the eThekwini municipality's optical infrastructure.

Most of these networks use a secure key management layer to manage keys between network users. As mentioned, current technology permits the distribution of qubits to a distance of up to 120 km in fibre per link. Such link lengths are typical of a Municipal Area Network (MAN) and the examples have been mentioned above. A QKD solution spanning a global network will however require further investigation.

3. Satellite-based global QKD network

The use of satellite technology in achieving a global quantum secured communication network has been of interest in the past few years. Many feasibility tests have been conducted [9, 10, 11] however various challenges still prevent the realization of a ground to satellite QKD link. These challenges are mainly associated with spatial and temporal synchronization of the stations. The time available for QKD synchronization is in the order of minutes per session. This requires high-speed synchronization and an efficient and stable communication link. An advanced tracking system is therefore critical to such an implementation [11]. Due to the relatively high speeds of the satellite the Doppler effect and time variations due to relativity must also be compensated. Together with these additional challenges, the basic free space challenges of atmospheric parameters (temperature, visibility, weather and background noise) may further limited and degrade the contact time for the quantum key exchange.

In this technique the satellites are considered to be trusted nodes. The nodes travel between various MANs creating a global backbone encryption key resource. The satellite network therefore requires an access point at each participating MAN network. The access point will require, further to a robust QKD link, the communication infrastructure to provide gateway functionality to the Metropolitan area. Unfortunately, most sites that are good for ground-to-satellite links are in relatively remote and isolated in their surroundings. Although this ensures better visibility, it lacks the infrastructure to support a commercial global access point.

4. Global QKD network based on commercial airliner network

As parallel step to the development of satellite-based global QKD networks, we are investigating the use of the commercial aircrafts' network as secure transport mechanism to support the global QKD network. Commercial airliners create an ideal alternate global network for key distribution in terms of

coverage, reliability and contact time. Further the airports at each connected city have the appropriate supporting infrastructure to serve as an access point for the MANs to the global network.

4.1. Implementation

The QKD process, implemented in the proposed scheme, will occur whilst the aircraft is docked at the airport. This allows a simple fibre-based QKD system is to be used for the key distribution process. Due to the use of a fibre channel, the solution bypasses the additional synchronization techniques required when using a satellite-based network. The frequency and reliability of the link, further enhances the opportunities that this option has to offer.

The initial systems that are to be used will require the aircraft to be a trusted zone although certified tamper-proofing techniques will be used. The long-term objective is to upgrade these initial systems to contain a quantum memory and an entangled photon source for QKD. As with the satellite solution, this would provide the idea untrusted network scenario.

The commercial airliners are to serve as a global link between the MANs of connected cities, as such the airports serve as gateways. Each aircraft will be fitted with a tamper-proof QKD unit in the communications hub in the hull of the aircraft. This is a highly restricted zone and can therefore be assumed a secure location. This unit will be responsible for the quantum-secured key distribution between itself and the sister unit stationed in the respective airport. The secure key management layer, from within the airport building, will then manage the keys. This, in total will provide the access point to the MAN. Information can be encrypted on site and safely propagated through conventional communication networks or the keys sold onwards to the respective clients.

4.2. QKD Protocol

The QKD procedure for the aircraft network will be as follows:

- The qubit source will be installed into the carrier aircraft and the detectors into the participating airports.
- The carrier aircraft will dock at a gate for disembarkment, preparation for the next flight and boarding of passengers. During this time the diagnostics cable will be connected to the aircraft. This will also contain the dark fibre for the QKD process.
- QKD will be conducted between the aircraft and the departing airport while docked at the Airport A.
- This initial key, k_A, will then be stored in a secured memory within the QKD station in the aircraft.
- After docking at the arriving airport, Airport B, a second key is generated between the aircraft and Airport B, k_B.
- An XOR function is then employed to encrypt k_A with k_B using a One Time Pad. This securely transfers k_A to the Airport B.
- The two airports then have a secure key ready to be used. The secure key management layer will control the flow and distribution of these keys.
- The local MAN is then used to distribute the keys further to end users within the network using local QKD links.

The use of airports development of a global QKD network is ideal for a robust global network with ample redundancy and frequency to provide the required quality of service for current encryption key demands. Together with a vast global coverage, the airports' ICT infrastructure in general contain the resources for connections to the respective host city. This makes such a solution of great interest when looking at commercial options for global QKD networks.

Currently the Centre for Quantum Technology is negotiating with the Airports Company of South Africa (ACSA) in order to implement the first aircraft-based QKD system.

5. Conclusion

QKD is gaining a focal interest in the commercial world at present. The technological challenges that face this technology in integrating and absorbing QKD as a transparent operation within the hardware layer of the OSI model will ultimately define the market share awarded to this technology.

6. Acknowledgements

This work is based on research supported by the South African Research Chair Initiative of the Department of Science and Technology and National Research Foundation.

7. References

[1] Nielsen M A and Chuang I L 2000 *Quantum Computation and Quantum Information* (Cambridge University Press)
[2] Gollmann D 2006 *Computer Security* (John Wiley & Sons)
[3] Renner R, Gisin N, and Kraus B 2005 *Phys Rev A* **72** 012332
[4] Zhen-Qiang Y, Zheng-Fu H, Wei C, Fang-Xing X, Qing-Lin W and Guang-Can G 2008 *Chinese Phys. Lett.* **25** 3547
[5] Mirza A and Petruccione F 2010 *JOSA B* **27** A185
[6] Peev M etal 2009 *New J of Phys* **11** 075001
[7] [online] http://swissquantum.idquantique.com/
[8] Sasaki M etal 2011 *Optics Express* **19** 10387
[9] Bonato C, Tomaello A, Da Deppo V, Naletto G and Villoresi P 2009 *New J. Phys.* **11** 045017
[10] Rarity J G 2000 *IEE Seminar Nanotechnology and Quantum Computing* 11
[11] Toyoshima M, Takenaka H, Shoji Y, Takayama Y, Takeoka M, Fujiwara M and Sasaki M 2011 *Intl J. of Optics.* **2011** 254154