An investigation of synchronisation techniques for a handheld QKD device

S Pillay[1], M Mariola[1], F Petruccione[1,2]

[1] Quantum Research Group, School of Chemistry and Physics, University of KwaZulu-Natal, Private Bag X54001, Durban 4000, South Africa
[2]National Institute for Theoretical Physics (NITheP), KwaZulu-Natal, South Africa
Email: 206507614@stu.ukzn.ac.za

Abstract. The importance of cryptography has become more prevalent in contemporary communication and the commercial use of Quantum Key Distribution (QKD) is now a realistic option for fibre networks. Long-range, free-space QKD and miniaturised, personal QKD devices are emerging fields of research aiming towards future commercial use. Previously, a handheld QKD device was developed using the Coherent One-Way (COW) protocol to exchange the encryption key between the transmitter and receiver. An optical synchronisation system was developed for the handheld device establishing real time synchronisation between the transmitter and receiver. This paper will investigate the viability of other synchronisation techniques appropriate for a handheld QKD device. The first technique will use asynchronous communication to establish communication between the transmitter and receiver. The second technique will use a radio channel to establish synchronisation, based on Binary Phase-Shift Keying. The radio channel also serves as the public channel for the QKD system.

1. Introduction

Quantum Key Distribution (QKD) provides an unconditionally secure method to share an encryption key between two authenticated parties [1]. QKD does not rely on the complexity of mathematical algorithms in order to protect sensitive data. Instead, quantum 2-level systems are used to distribute binary data from the transmitter to the receiver [2]. The use of QKD facilitates the long-term security of sensitive data, since QKD is not vulnerable to increasing computing power in decryption technology. Quantum particles necessarily follow the laws of quantum physics which govern their behavior. The No Cloning theorem [3] and Heisenberg's Uncertainty principle [4] ensure that any eavesdropping attempts on the transmission are detected. The most commonly used quantum 2-level system is a single photon of light, encoded using its polarisation state or phase. This method of encoding is used in most prepare-and-measure schemes, such as the BB84 protocol [5] and the SARG04 protocol [6].

Commercial applications of QKD have been well developed for metropolitan fibre networks [7]. Free-space QKD is a technology that is still undergoing research but is rapidly gaining commercial relevance [8]. Another emerging QKD technology are handheld, portable QKD devices which are designed to be used by individual users over a short range [9]. Handheld devices can be implemented with either a free-space or a fibre link and allow a user to share and store a set of secret keys with a central node for personal use at a later time. An application of this technology is the sharing of a secret One-Time Pin between a bank and a customer. The keys can also be used as authentication tools for workplace security or other applications. The handheld device must be integrated into a network using shared nodes to connect users with a central mainframe. The user can top up on One-Time Pins at

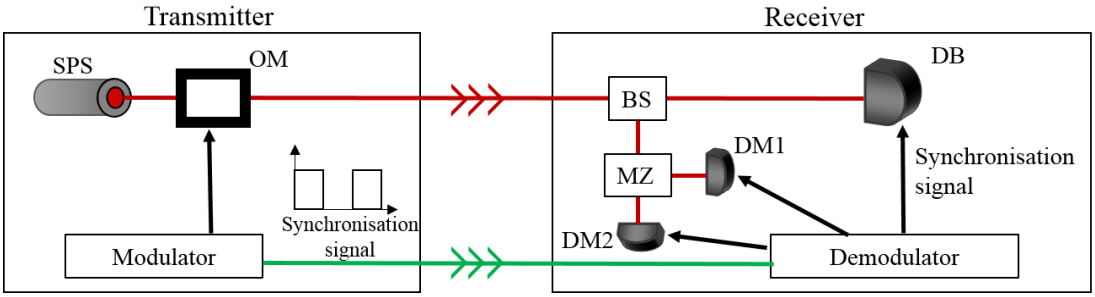

Figure 1. A schematic of the COW protocol detailing the transmitter and receiver modules. The transmitter includes a faint, coherent laser source, SPS, coupled with an external optical modulator, OM, used to create the bit encoding. The transmitter also includes a synchronisation modulator and additional electronics and on-board memory required for post-processing. The receiver module requires a beam splitter, BS, to create two separate optical paths from the incoming bit stream. The first path serves as the detection line and requires a single photon detector, DB, which measures incoming photons to create the raw key. The second path of the beam splitter serves as the monitoring line. This path consists of a Mach-Zehnder interferometer, MZ, and single photon detectors at each output of the interferometer, DM1 and DM2. The purpose of the interferometer is to confirm the coherence between two consecutive decoy pulses. A break in coherence infers the presence of an eavesdropper. The demodulator receives the synchronisation signal and commands the gates of the single photon detectors DB, DM1 and DM2.

a node, such as an ATM machine. The ATM, in turn, distributes this key with a central mainframe using a long-range fibre or free-space QKD channel. The user can then use the stored pins for secure communication with the central mainframe. This paper will discuss the application of the COW protocol in handheld devices in Section 2. Section 3 will detail the existing optical synchronisation system that was built for the device. Section 4 and 5 will discuss other potential methods of synchronisation, including asynchronous transmission and radio synchronisation.

2. Coherent One-Way Protocol

Current implementations of handheld devices use the BB84 protocol with polarisation encoding but a four-state protocol such as BB84 requires more components and post-processing algorithms after the key distribution. The Coherent One-Way (COW) protocol [10] provides a simpler alternative for smaller QKD devices. The COW protocol is suitable for use in fibre networks since coherence between laser pulses will deteriorate in a turbulent, free-space channel. Since a handheld device transmits over a short range, free-space channel, the pulses will not be affected by turbulence, allowing for a COW protocol implementation. The bit encoding implemented in the COW protocol is distributed over two consecutive pulses. One pulse contains a photon and the other is empty. The order of these two pulses creates the 2-level system used for the encoding as follows,

$$|0_k\rangle = \left|\sqrt{\mu}\right\rangle_{2k-1}|0\rangle_{2k} \quad \text{and} \quad |1_k\rangle = |0\rangle_{2k-1}\left|\sqrt{\mu}\right\rangle_{2k}, \tag{1,2}$$

where μ is the mean photon number and k is the time bin index. A portion of the pulses are also encoded as decoy pulses. In this case, both the pulses contain a photon. Figure 1 shows a schematic of the COW protocol and discusses its implementation.

3. Optical synchronisation system

As with all QKD systems, the transmitter and receiver must be initially synchronized before the key distribution begins. The synchronisation of the devices is necessary to ensure that the single photon detectors open at precisely the time of arrival of the photon pulses. If the detectors make a measurement

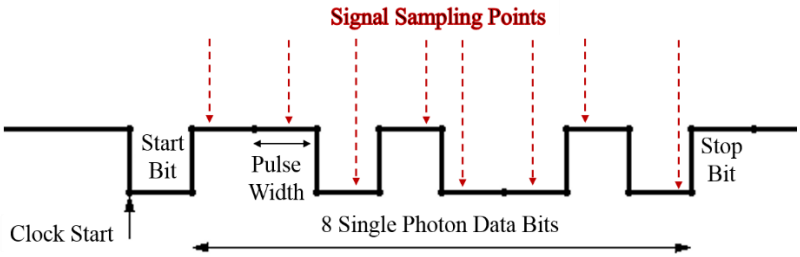

Figure 2. Asynchronous transmission begins with a Start bit which serves as the synchronisation indicator. The pulse width of each bit is agreed upon before the transmission begins and the receiver is able to measure the 8 data bits following the Start bit. The Stop bit indicates that the data has stopped, pending the transmission of another Start bit.

at the wrong time, the system will register a high loss rate. The COW protocol particularly requires precise synchronisation since the transmitter and receiver must compare their bits at specific time bins.

The previous synchronisation system designed for the handheld COW protocol device used an additional light source to synchronise the transmitter and the detectors of the receiver [11]. A 532 nm LED was installed in the transmitter as the synchronisation source. The LED was aligned to pass through the pulse modulator without being influenced by the bit encoding. The LED signal was measured by the receiver using a photodiode. The signal from the photodiode was squared using a Smith trigger and transmitted to a microcontroller. The microcontroller triggered the single photon detectors, commanding the detector gates to open only when a pulse was incident on the detector. It is important to note that, due to the varying bit encoding or the losses in the channel, some of the pulses did not contain a photon, but the detector must still measure these pulses in order to register an empty pulse.

4. Asynchronous Transmission

Asynchronous transmission intersperses the data signal with a synchronisation sequence using the same light source [12]. The advantage of aligning just one light source makes this method simpler to implement than a synchronous method such as the optical synchronisation mentioned above. The bit rate of the signal is established before the transmission begins and it is, therefore, only necessary for the transmitter to indicate when the receiver should start to take measurements. The bit sequence for asynchronous transmission must begin with an indicative “Start” bit followed by 8 bits of data. A “Stop” bit indicates the end of the data and the beginning of another synchronisation iteration, as seen in Figure 2. The key generation rate of the system will decrease when using asynchronous transmission since the start and stop indicators do not contribute to the key. However, the COW protocol produces a higher bit rate compared to other QKD protocols, therefore compensating for the large overhead.

In order to implement asynchronous transmission for a handheld QKD device, the pseudo-single photon source in the transmitter must be controlled by a variable attenuator so that the mean photon number of each pulse can be adjusted. It is necessary for each start and stop pulse to be measured by the single photon detectors. Since single photons can be lost during transmission, the mean photon number of the start and stop pulses should be increased to increase the probability of detection. Should the start and stop pulses not be measured, the receiver will not open the detector gates to receive a new set of bits, thus resulting in high losses in the channel. The mean photon number can be decreased to one during the transmission of the data bits.

5. Radio Synchronisation using BPSK

A radio signal can serve as a simple method to synchronise QKD modules. A similar system using a radio signal and BPSK encoding was proposed in [13]. A radio transmitter and receiver are easier to align in comparison to an optical signal. The radio signal can also be used for initial authentication between the modules, as well as the public channel used for post processing of the quantum signal, making a radio signal versatile and robust. Generally, free-space QKD modules use a GPS signal for

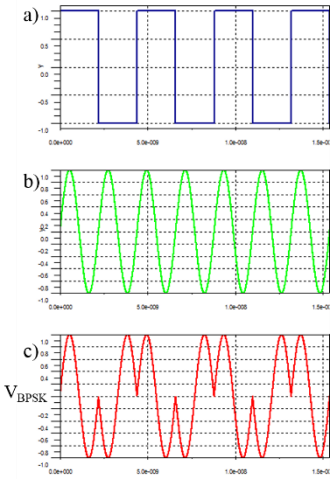

Figure 3. Diagram a) shows the modulating signal which represents the information to be transmitted over the public channel. The carrier signal, shown in b), is a sinusoidal radio signal which will be used for synchronisation. The modulated signal V_{BPSK}, shown in c), carries general binary data through the public channel.

tracking and synchronisation [8]. A radio signal is a reliable alternative which will work in the absence of a GPS signal. Since QKD is an unconditionally secure means to share encryption keys, it can be useful for both the banking and defense sectors. A reliable synchronisation system is therefore necessary to facilitate the key exchange. A radio signal can be encoded with a binary string using Binary Phase-Shift Keying (BPSK) [14]. Phase-Shift Keying refers to the phase modulation of a sine or cosine wave, where BPSK specifically modulates the wave by 180°, creating a binary code, as seen in Figure 3. BPSK is more resistant to errors compared to other types of Phase-Shift Keying since the binary values are 180° apart. An erroneous phase-shift will have to be greater than 90° to change the binary bit value.

5.1. The Costas Loop

The coherent demodulation and the carrier recovery can be performed by using a Costas loop [15]. The Costas loop is based on a phase-locked loop and can be used to recover the carrier frequency of a phase-modulated signal, such as BPSK. A circuit diagram of the Costas loop is shown in Figure 4. In the Costas loop, the Voltage Controlled Oscillator (VCO) is a free oscillator centered on the error frequency ω_0, that can change the frequency in function of an applied voltage, named V_{CON}. The output signal can be synthesized by the equation

$$V_{\mathrm{VCO}}(t) = cos\left[\omega_0 t + \int_0^t kv\, V_{\mathrm{CON}}(\tau)d\tau\right], \tag{4}$$

where *kv* is the sensitivity expressed in *rad/V*. A BPSK signal can be represented according to the following function:

$$V_{\mathrm{BPSK}}(t) = AS_{\mathrm{p}}(t)\cos(\omega_0 t)\,, \tag{5}$$

where ω_0 is the angular frequency of the carrier, $S_p(t)$ contains the bit to transmit and A is the amplitude of the received carrier. The angular frequency ω_0 is the frequency of the local oscillator of the VCO. The timing frequency for the QKD device is extracted from the carrier frequency.

Suppose that the signal from the VCO is

$$V_{\mathrm{VCO}}(t) = \cos(\omega_0 t + \varphi_e)\,, \tag{6}$$

where φ_e represents the difference in phase between V_{BPSK} and V_{VCO}. The VCO signal in Equation (6) is sent to analog multiplier 1 and a -90° phase shifter. The signal at the output of the analog multiplier is

$$V_1(t) = V_{\mathrm{BPSK}} \cdot V_{\mathrm{VCO}} = \frac{AS_p}{2}[cos\varphi_e + \cos(2\omega_0 t + \varphi_e]\,.$$

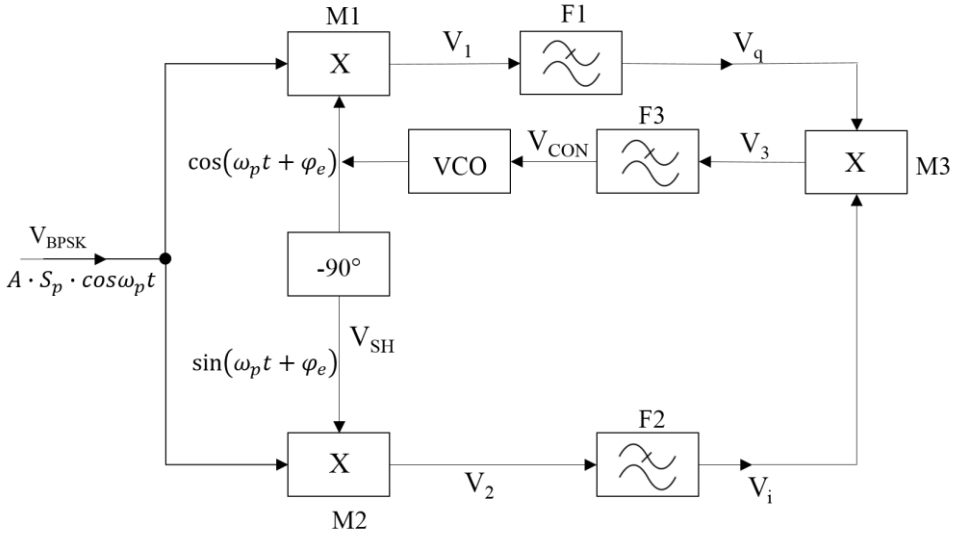

Figure 4. A diagram of the Costas loop, used to demodulate the BPSK signal. VCO is a voltage controlled oscillator which oscillates with the same frequency as the received V_{BPSK} signal. Any phase difference between the signals must be resolved. V_{BPSK} is multiplied by VCO at multiplier M1. VCO undergoes a -90° phase shift and is multiplied to V_{BPSK} at M2. Both signals are passed through respective low pass filters F1 and F2 and are multiplied at M3. The resultant signal is passed through low pass filter F3 in order to remove any noise and is then applied to VCO to correct the phase difference. The signal from VCO can then be used to synchronise the receiver module.

It is possible to attenuate the components cos ($\omega_p t + \varphi_e$) of the signal $V_1(t)$ through the low pass filter F1. The signal at the output of F1 is:

$$V_q = \frac{AS_p}{2} cos\varphi_e \ . \tag{7}$$

V_q is not dependent on the frequency ω_0. When V_{VCO}, crosses the phase shifter, the signal $V_{SH}(t)$ is

$$V_{SH}(t) = \cos(\omega_0 t + \varphi_e - 90°) = \sin(\omega_0 t + \varphi_e) \ .$$

V_{SH} multiplied by V_{BPSK} is

$$V_2(t) = \frac{AS_p}{2}[\cos(90° - \varphi_e) + \cos(2\omega_0 t + \varphi_e + 90°)] \ .$$

Since the signal has double frequency components, the signal can be filtered to obtain a signal $V_i(t)$,

$$V_i(t) = \frac{AS_p}{2}\cos(90° - \varphi_e) = \frac{AS_p}{2}\sin(\varphi_e) \ . \tag{8}$$

The signals V_q and V_i are multiplied to obtain the voltage control of the VCO, V_{CON},

$$V_{CON} = V_q \cdot V_i = \frac{A^2 {S_p}^2}{32}\sin(2\varphi_e) \ . \tag{9}$$

From Equation (4), it is possible to observe that V_{CON} changes the frequency V_{VCO} proportionally to the phase φ_e. If φ_e increases, V_{CON} and V_{VCO} increase in order to follow the signal V_{BPSK} received. When φ_e=0, V_{VCO} is 0 and the signal V_{VCO} is in phase with V_{BPSK}. The synchronisation signal for the handheld QKD device is now obtained from the V_{VCO} signal.

6. Conclusion

Handheld QKD devices are an emerging field of research with future commercial applications. An optical synchronisation system was previously developed for a handheld device implemented with the COW protocol. An investigation of other synchronisation methods was done. Asynchronous transmission using the single photon source provided the advantage of aligning only one laser source to use for both synchronisation and bit encoding. A radio channel between the transmitter and receiver can also provide a reliable synchronisation link, as well as a public channel used for the QKD authentication and post processing. The radio signal can be encoded using BPSK and demodulated by the receiver using a Costas loop.

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.

References

[1] Lo H K and Chau H F, 1999 Unconditional security of quantum key distribution over arbitrarily long distances *Science* **283**(5410) 2050-2056.
[2] Gisin N, Ribordy G, Tittel W and Zbinden H 2002 Quantum Cryptography *Review of Modern Physics* **74** 145.
[3] Wooters W K and Zurek W H 1982 A single quantum cannot be cloned *Nature* **299**(5886) p802.
[4] Zettili N 2009 *Quantum mechanics: Concepts and applications* (John Wiley & Sons Inc.) p.28.
[5] Bennett C and Brassard G 1984 Quantum Cryptography: Public key distribution and coin tossing *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing* pp 175-179.
[6] Scarani V, Acin A, Ribordy G and Gisin N 2004 Quantum cryptography protocols robust against photon number splitting attacks for weak laser pulse implementations *Physical Review Letters* **92**(5) 57901.
[7] Gobby C, Yuan Z L and Shields A J 2004 Quantum key distribution over 122 km of standard telecom fiber *Applied Physics Letters* **84** pp 3762-3764.
[8] Schmitt-Manderbach T, Weier H, Furst M, Ursin R, Tiefenbacher F, Scheidl T, Perdigues J, Sodnik Z, Kurtsiefer C, Rarity J G, Zeilinger A and Weinfurter H 2007 Experimental Demonstration of Free-Space Decoy-State Quantum Key Distribution over 144 km *Physical Review Letters* **98**(1) 010504.
[9] Duligall J L, Godfrey M S, Harrison K A, Munro W J and Rarity J G 2006 Low cost and compact quantum key distribution *New Journal of Physics* **8**(10) 249.
[10] Gisin N, Ribordy G, Zbinden H, Stucki D, Brunner N and Scarani V 2004 Towards practical and fast quantum cryptography *arXiv preprint quant-ph/0411022.*
[11] Pillay S, Mariola M, Mirza A and Petruccione F 2015 Handheld QKD device using the COW protocol, in The Proceedings of the 60th Annual Conference of the South African Institute of Physics (SAIP2015)(ADDENDUM), edited by Makaiko Chithambo (RU) and André Venter (NMMU) pp 29 - 35. ISBN: 978-0-620-70714-5.
[12] [online] Asynchronous and Synchronous Communication http://www.pccompci.com/Asynchronous%20and%20Synchronous%20Communication.html.
[13] Mariola M, Mirza A and Petruccione F 2011 Quantum cryptography for satellite communication, in Proceedings of SAIP2011, the 56th Annual Conference of the South African Institute of Physics, edited by I. Basson and A.E. Botha (University of South Africa, Pretoria) pp 403 - 408. ISBN: 978-1-86888-688-3.
[14] Bernardini A 2008 *Lezioni del corso di sistemi di comunicazione satellitari* Vol 1 ed Edizioni Ingegneria 2000 (Rome) pp 251-256.
[15] Kostopoulos A 1995 *Corso di telecomunicazioni. Dai sistemi di comunicazione ai servizi telematici* ed 2 (Petrini) pp 466-467.