Realization of B92 QKD protocol using id3100 Clavis^2 system

Makhamisa Senekane[1], Abdul Mirza[1], Mhlambululi Mafu[1] and Francesco Petruccione[1,2]

[1] Centre for Quantum Technology, School of Chemistry and Physics, University of KwaZulu-Natal, P/Bag X54001 Durban, South Africa

[2] National Institute for Theoretical Physics (NITheP), University of KwaZulu-Natal, P/Bag X54001 Durban, South Africa

E-mail: `211560527@stu.ukzn.ac.za, mirzaa@ukzn.ac.za, 209526077@stu.ukzn.ac.za, petruccione@ukzn.ac.za`

Abstract. Quantum key distribution is an encryption technique for securely exchanging a bit string (known as a key) between two communicating parties, traditionally known as Alice, the sender and Bob, the receiver, in the presence of an eavesdropper, Eve. This technique is based on two laws of quantum mechanics, namely the Uncertainty Principle and the no-cloning theorem. The first operational quantum key distribution protocol known as the BB84 protocol was developed by Charles Bennett and Gilles Brassard. Since then, various QKD protocols have been developed. Examples include B92, SARG04 and six state protocols. Currently, BB84 forms the most established protocol and therefore is the most widely used protocol. However, since the B92 protocol uses two quantum states, as opposed to BB84's four, it requires less resources for its implementation. Despite the B92 protocol being simpler to implement than the BB84 protocol, surprisingly this advantage has not been fully exploited. Therefore, in this paper we investigate the feasibility of implementing the B92 protocol by using the id3100 Clavis^2 system from idQuantique.

1. Introduction

Cryptography is the art of transforming information into something unintelligible to anyone other than the intended recipient [1]. It provides communication between legitimate parties in the presence of an adversary. Therefore, the goal of cryptography is to transmit information from the sender to the receiver in such a way that the information sent could not be intercepted/modified by an eavesdropper.

There are two main branches of cryptography, namely secret- (symmetric-) key cryptography and public- (asymmetric-) key cryptography [2]. For practical purposes, since it is difficult to distribute keys using secret-key cryptography, public-key cryptography is widely used in conventional cryptosystems. The main problem of public-key cryptosystems is that they can be undermined by advances in technology and mathematical algorithms; since their security is conditioned on the assumption that Eve would have limited computational power and that some mathematical functions (one-way functions) are difficult to compute [3]. It is here that quantum mechanics offers a solution in the form of quantum key distribution (QKD). Unlike conventional cryptographic protocols, whose security is based on unproven assumptions

concerning mathematical complexities, QKD's theoretical unconditional security is based on the fundamental laws of quantum mechanics.

The remainder of this paper is divided into three sections. Section 2 provides some background information on the BB84 protocol, the B92 protocol, the "Plug and Play" optical scheme and the Clavis^2 system. This is followed by Section 3 which explains explains the implementation of the B92 protocol on the Clavis^2 system. Lastly, Section 4 concludes this paper.

2. Background Information

QKD allows two users to establish an identical and purely random sequence of bits at two different locations while also allowing for the detection of an eavesdropper [4]. This string of bits is used as a one-time pad for cryptographic purposes. QKD security is based on the fact that it is theoretically impossible to gain information about non-orthogonal quantum states without disturbing these states [5, 6, 7, 8, 3, 9].

QKD protocols can be classified into two types [10]:

- Prepare and Measure schemes: Alice prepares a quantum signal according to her basis and bit values and sends them through a quantum channel to Bob, whom upon reception, measures them. Examples of Prepare and Measure schemes are BB84 [5], B92 [11] and SARG04 [12] protocols.
- Entanglement-based schemes: an entangled source emits a pair of entangled signals, and this pair is then measured by Alice and Bob separately. An example of entanglement-based protocol is the one which was proposed by Artur Ekert in 1991 (E91) [13].

QKD uses two communication channels, namely:

- Quantum channel: which is used for key exchange between Alice and Bob, this channel uses the laws of quantum mechanics to reveal (if any) the presence of Eve.
- Classical channel: which is used to perform classical post-processing tasks such as sifting, error correction and privacy amplification.

2.1. BB84 Protocol

The BB84 protocol is the first QKD scheme that has been proposed [5, 3]. It encodes a quantum state (usually a single photon polarization) using two non-orthogonal bases, namely rectilinear and diagonal bases, with four polarization states (0°, 90°, 45° and 135°). The Uncertainty Principle dictates that if a measurement (on Bob's side) is performed in a different basis from the one in which it was prepared (by Alice), then such a measurement would yield a random outcome and such a state would be disturbed. This means that Eve's presence would introduce errors which could be detected [14, 15]. On the other hand, if Bob's measurement basis is the same as Alice's preparation basis, then such a quantum bit (qubit) would be used to generate a raw key [3].

As already stated, the BB84 protocol uses two channels: one for quantum key exchange (quantum channel) and one for classical post-processing (classical channel). The steps which are followed for quantum key exchange between Alice and Bob are [5, 8, 14]:

- Alice generates a qubit sequence and sends it to Bob, randomly choosing which basis to use to represent such a sequence.
- Bob randomly measures the polarization of the incoming sequence of quantum states by using any of the bases.

The second and last stage of the BB84 protocol is a classical post-processing procedure which uses the classical channel. This stage involves [5, 8, 14]: sifting, error correction and privacy

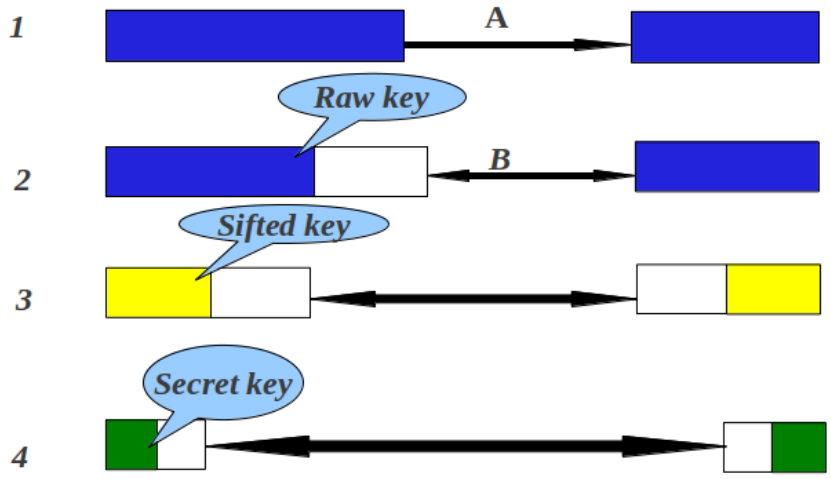

Figure 1. Key generation stages in BB84 protocol. A: Quantum channel, B: public channel, 1: Qubit transmission, 2: After sifting, 3: After error correction, 4: After privacy amplification.

amplification. Figure 1 shows the stages of the BB84 protocol and reductions in key length due to sifting, error correction and privacy amplification.

2.2. B92 Protocol

The B92 protocol forms a simpler version of the BB84 protocol [16]. It is a two-state protocol (it uses two non-orthogonal quantum states) which was proposed by Charles Bennett in 1992. It is based on the fact that two non-orthogonal quantum states are sufficient to guarantee the detection of an eavesdropper.

In the B92 protocol, quantum key exchange stage for B92 is implemented as follows:

- Alice randomly generates a qubit sequence and sends it using any of the two non-orthogonal states.
- Bob randomly chooses the time-slots (instances) to measure the incoming qubit sequence.

The classical post-processing procedure is similar to that of the BB84 protocol. However, the subtle difference lies in the sifting step. In this step Alice and Bob compare their time-slots in order to generate a raw key unlike in BB84 protocol where Alice and Bob compare their bases. Bob communicates to Alice the time-slots he used to determine non-erasures [8], and Alice compares those time-slots to hers. They both record time-slots where non-erasures were detected, and use bits corresponding to those slots as a raw key. The other steps (error correction and privacy amplification) of B92 are the same as those of BB84.

2.3. "Plug and Play" Scheme

QKD can be implemented by using either free-space or optical fibers as a quantum channel. Free-space QKD systems are easier to design and are also resistant to birefringence [3]. However, optical fibers (using phase coding) constitute the frequently used quantum channel for QKD applications. Of the phase coding schemes, the most commonly used (for commercial applications) is the "Plug and Play" scheme [1].

The "Plug and Play" scheme for quantum key distribution was first introduced by Muller *et al.* in 1997 [17]. Basically, this scheme features Bob sending a classical signal to Alice in order to initiate a key exchange session. Alice then attenuates (to an average of a single photon per pulse)

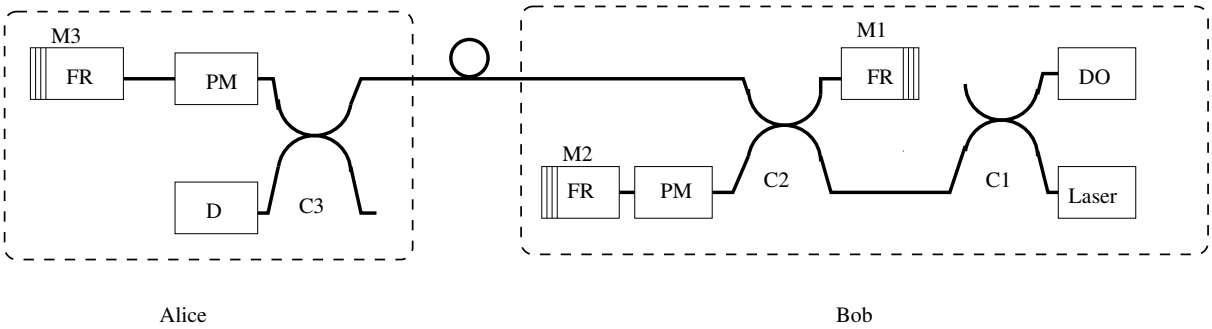

Figure 2. "Plug and Play" system. DO: single photon detector, C1, C2 & C3: fibre couplers, PM: phase modulator, FR: Faraday rotator, M1, M2 & M3: mirror, D_A: classical detector.

and encodes the received signal and sends it back to Bob, who then performs a measurement. The major advantage of "Plug and Play" systems is that they do not require additional optical adjustments during operation. Figure 2 shows a typical "Plug and Play" scheme.

2.4. Clavis^2 System

The Clavis^2 system is a QKD research platform used for deploying a "Plug and Play" scheme. It is a product of idQuantique from Geneva, Switzerland. It uses a proprietary auto-compensating optical platform which guarantees a low quantum bit error rate (QBER). Currently, this system supports BB84 and SARG04 protocols only. Figure 3 shows the set-up of the Clavis^2 system which we used for the implementation of the B92 protocol.

3. B92 on a Clavis^2 System

Usually, the B92 protocol is implemented using frequency coding scheme [1, 18]. However, these schemes do not enjoy any commercial success because of difficulties involved with deploying optical networks based on them. Also, the security of this scheme has not been studied in depth [1].

We take advantage of the commercial success and ease of deployment of "Plug and Play" scheme to implement the B92 protocol. This implementation does not alter the hardware of the Clavis^2 system, but alters Alice's preparation process (by using two quantum states instead of four), Bob's measurement process (using two quantum states instead of four) and sifting (using comparison of time-slots instead of comparisons of the bases). The two sifting processes are equally feasible because in order to extract the key the BB84 and SARG protocol uses comparisons of bases and states respectively whilst the B92 protocol uses erasures. However, this difference in the sifting process only determines which protocol can suit a particular implementation but it cannot be used to directly compare the efficiency between different protocols.

In order to compare the B92 protocol and the other two standard protocols (BB84 and SARG04), we use the raw key length and the QBER. The QBER forms one of the most important parameters when investigating the security of a protocol. The QBER is the fraction of positions where Alice's and Bob's string values differ [3]. The QBER forms a direct measure for the secrecy of the shared string. If the QBER is above a certain threshold, the two parties abort the protocol, otherwise they apply a post-processing scheme to distill the secret key from the raw key. Therefore, the higher the QBER, the lower the raw key length (fraction of correlated bit strings) which the two legitimate parties share. This means that the protocol only allows a small fraction of errors to occur in order for the two parties to establish a shared secret key, thus making the implementation of the protocol less efficient. The theoretical QBER is given as

Figure 3. Clavis^2 QKD system in our laboratory at the University of KwaZulu-Natal. Bob's side is on the left while Alice's side is on the right.

Cycle	Protocol	Raw Key Length (Frames)	Theoretical QBER (%)
1	BB84	12804	0.72
2	BB84	13443	0.72
3	BB84	13692	0.72
1	B92	12636	0.68
2	B92	13023	0.68
3	B92	12835	0.68
1	SARG04	13329	1.25
2	SARG04	12492	1.25
3	SARG04	13143	1.25

Table 1. A comparison of BB84, SARG04 and B92 protocols using raw key length and theoretical QBER.

[3]

$$QBER = R_{\text{error}}/R_{\text{sift}}, \tag{1}$$

where $R_{\text{sift}} = 1/2R_{\text{raw}}$ is the sifted key rate and R_{error} is the rate of getting a wrong signal on Bob's side.

The theoretical QBER values and raw key length were compared among the three Prepare and Measure protocols; BB84, B92 and SARG04 protocols. Each protocol session was executed for three cycles, with each cycle running for 100 seconds. Table 1 summarizes the findings. From

Table 1, it can be observed that the B92 has the lowest theoretical QBER. However, it is also observed that the raw key of the B92 protocol generated is the shortest of the three compared protocols. This observation also agrees with theory [19].

4. Conclusion

We have demonstrated the realization of the B92 QKD protocol using the id3100 Clavis^2 system without modifying the Clavis^2 hardware. Prior to our work, the system only supported two protocols, namely BB84 and SARG04 protocols. Based on the results obtained (shown in Table 1), the B92 displays raw key length and theoretical QBER comparable to BB84 and SARG04 protocols, which implies that it is feasible and efficient to implement the B92 protocol on the Clavis^2 system. As expected, the B92 displays a lower key rate as compared to BB84 and SARG04 protocols. However, an advantage of such an implementation is that the B92 protocol requires less resources and when compared to the other two protocols. The security analysis of this approach is left for future work.

Acknowledgments

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] Makarov V 2007 *Quantum cryptography and quantum cryptanalysis* Ph.D. thesis Norwegian University of Science And Technology

[2] Lo H and Lütkenhaus N 2007 *arXiv:0702202*

[3] Gisin N, Ribordy G, Tittel W and Zbinden H 2002 *Reviews of Modern Physics* **74** 145–195

[4] Scarani V, Bechmann-Pasquinucci H, Cerf N J, Dušek M, Lütkenhaus N and Peev M 2009 *Reviews of Modern Physics* **81** 1301

[5] Bennett C and Brassard G 1984 *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing* vol 175 (Bangalore, India) pp 175–179

[6] Alleaume R, Bouda J, Branciard C, Debuisschert T, Dianati M, Gisin N, Godfrey M, Grangier P, Langer T, Leverrier A *et al.* 2007 *arXiv:0701168*

[7] Qi B, Qian L and Lo H 2010 *arXiv:1002.1237*

[8] Lomonaco S 1999 *Cryptologia* **23** 1–41

[9] Bennett C, Bessette F, Brassard G, Salvail L and Smolin J 1992 *Journal of Cryptology* **5** 3–28

[10] Fung C, Ma X and Chau H 2010 *Physical Review A* **81** 012318

[11] Bennett C 1992 *Physical Review Letters* **68** 3121–3124

[12] Scarani V, Acin A, Ribordy G and Gisin N 2004 *Physical Review Letters* **92** 57901

[13] Ekert A 1991 *Physical Review Letters* **67** 661–663

[14] Kollmitzer C and Pivk M 2010 *Applied Quantum Cryptography* vol 797 (Springer Verlag)

[15] Zeng G 2010 *Quantum Private Communication* (Springer)

[16] Desurvire E 2009 *Classical and Quantum Information Theory* (Cambridge University Press)

[17] Muller A, Herzog T, Huttner B, Tittel W, Zbinden H and Gisin N 1997 *Applied Physics Letters* **70** 793

[18] Kumar P and Prabhakar A 2009 *IEEE Journal of Quantum Electronics* **45** 149–156

[19] Christandl M, Renner R and Ekert A 2004 *arXiv:0402131v2*