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 Uncertainty Principle and no-cloning theorem. The first operational quantum key distribution protocol was developed by Charles Bennett and Gilles Brassard (BB84). Since then, various QKD protocols have been developed. Examples include a B92, SARG04 and six state protocols. Currently, BB84 is the standard protocol and it is the most widely used protocol. However, since the B92 protocol uses two quatum states, as opposed to BB84's four, it is easier to implement. Despite the advantage of the B92 protocol being simpler to implement than the BB84 protocol, this advantage has not been fully exploited. Therefore, in paper, we investigate the feasibility of implementing the B92 protocol by using the id3100 Clavis^2 system from id Quantique.

1. Introduction

Cryptography is the art of transforming information into something unintelligible to anyone other than the intended recipient [1]. It is intended to provide communication in the presence of an adversary. The essence 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, 4]. It is here that quantum mechanics offers a solution in the form of quantum key distribution (QKD).

The first QKD protocol, known as BB84, has been the most widely used protocol [4]. Unlike conventional cryptographic protocols, whose security is based on unproven assumptions

concerning mathematica 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 a background information on BB84, B92, "plug and play" optical scheme and the Clavis^2 system. This is followed by the section which explains this paper's contribution in the field of QKD. The last section 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 [3]. 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, 9, 10].

QKD protocols can be classified into two types [11]:

- Prepare and Measure schemes: where 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 [12] and SARG04 [13] 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 proposed by Artur Ekert in 1991 (E91).

QKD uses two communication channels, namely:

- Quantum channel: which is used for key exchange between Alice and Bob, using 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

BB84 is the first QKD scheme that was proposed [5, 9]. 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°0). 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 [3, 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, BB84, being a QKD protocol, uses two channels: one for quantum key exchange (quantum channel) and one for classical post-processing (classical channel). Steps followed for quantum key exchange between Alice and Bob are [5, 3, 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 using any of the bases.

The second and last stage of BB84 is classical post-processing using the classical channel. This stage involves [5, 8, 14]: sifting, error correction and privacy amplification. Figure 1 shows the stages of the BB84 protocol and reductions in key length due to sifting, error correction and privacy amplification.

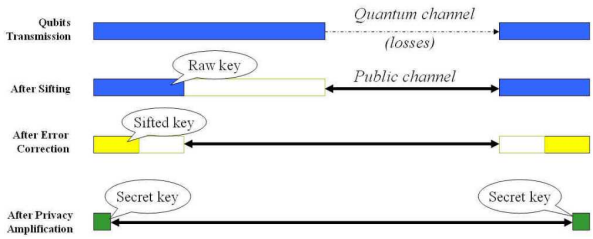

Figure 1. Key generation stages in BB84 protocol. An image courtesy of [4].

2.2. B92 Protocol

The B92 protocol is a simpler version of BB84 [16]. It is a two-state protocol (it uses two non-orthogonal quantum states) invented 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.

Classical post-processing is almost similar to that of BB84. The subtle difference is in the sifting step. In this step, unlike in BB84, where Alice and Bob compare their bases in order to generate a raw key, in B92, Alice and Bob compare their time-slots in order to generate a raw key. 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 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 [9]. 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].

"Plug and play" scheme for quantum key distribution was first introduced by Muller and his colleagues in 1997 [17]. Basically, this scheme features Bob sending a classical signal to Alice to initiate a key exchange session. Alice then attenuates (to an average of a single photon per pulse) and encodes the received signal and sends it back to Bob, who then performs 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.

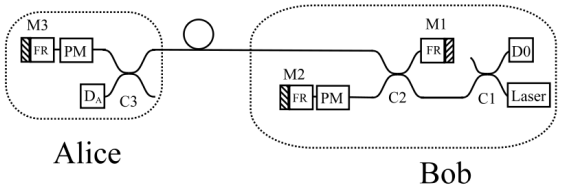

Figure 2. A "plug and play" system [17].

2.4. Clavis^2 System

Clavis^2 system is a QKD research platform deploying the "plug and play" scheme. It is a product of id Quantique in Geneva, Switzerland. It uses a proprietary auto-compensating optical platform which guarantees a low quantum bit error rate (QBER). Currently, the system supports BB84 and SARG04 only. Figure 3 shows a Clavis^2 system.

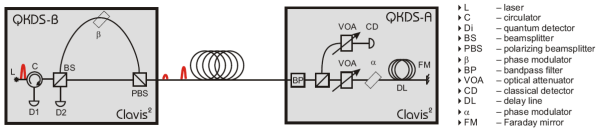

Figure 3. Clavis^2 QKD system from id Quantique.

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).

Theoretical QBER and raw key length were compared among the three Prepare and Measure protocols; BB84, B92 and SARG04. Table 1 summarises the findings. From the table, it can be observed that B92 has the lowest theoretical QBER. However, the raw key generated is the shortest of the three compared protocols.

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 between BB84, SARG04 and B92 protocols using raw key length and theoretical QBER.

4. Conclusion

We have demonstated the realization of the B92 QKD protocol using id3100 Clavis^2 system. Prior to our work, the system only supported two protocols, namely BB84 and SARG04. With

this work, based on the results shown in Table 1, we have demonstrated that even without modifying Clavis^2 hardware, the system can still be used to realize B92. However, the security of this approach is yet to be explored.

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 preprint quant-ph/0702202*
[3] Scholz M 2004 Quantum key distribution via bb84: an advanced lab experiment
[4] IdQuantique 2005 Understanding quantum cryptography
[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 preprint quant-ph/0701168*
[7] Qi B, Qian L and Lo H 2010 *Arxiv preprint arXiv:1002.1237*
[8] Lomonaco S 1999 *Cryptologia* **23** 1–41
[9] Gisin N, Ribordy G, Tittel W and Zbinden H 2002 *Reviews of modern physics* **74** 145–195
[10] Bennett C, Bessette F, Brassard G, Salvail L and Smolin J 1992 *Journal of cryptology* **5** 3–28
[11] Fung C, Ma X and Chau H 2010 *Physical Review A* **81** 012318
[12] Bennett C 1992 *Physical Review Letters* **68** 3121–3124
[13] Scarani V, Acin A, Ribordy G and Gisin N 2004 *Physical Review Letters* **92** 57901
[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