Applied Mathematics & Information Sciences
An International Journal

http://dx.doi.org/10.18576/amis/150515

Implementation and Security Analysis of the B92 Protocol using Id3100 Clavis^2 System

Mhlambululi Mafu[1,*] *and Makhamisa Senekane*[2]

[1]Department of Physics and Astronomy, Botswana International University of Science and Technology, P/Bag 16, Palapye, Botswana
[2]Institute of Intelligent Systems, University of Johannesburg, Corner Kingsway and University Road, Auckland Park, Johannesburg, 2092, South Africa

Received: 2 May 2021, Revised: 12 Jun. 2021, Accepted: 12 Aug. 2021
Published online: 1 Sep. 2021

Abstract: We present an experimental demonstration of the B92 quantum key distribution protocol using the id3100 Clavis^2 system from idQuantique. The B92 protocol implemented on this device utilizes the hardware more efficiently than the factory loaded four state protocols (BB84 and SARG04). The system shows a secure key generation rate of 6.42 kilobits per second and a quantum bit error rate of 1.75% at a mean photon number (μ) = 0.03 over an optical line length of up to 80 km. Our results scale similarly to the BB84 protocol results, thus showing the feasibility of implementing a two-state protocol over a fibre network in a system traditionally used for running the four-state BB84 and SARG04 protocols. Additionally, the B92 protocol is found to be simpler to implement as compared to the BB84 protocol. This is because it uses only two states provided they are non-orthogonal; hence requires fewer resources.

Keywords: Bennett 1992 protocol; Clavis^2 system; quantum key distribution

1 Introduction

Quantum Key Distribution (QKD) is the process of sharing a secure key that is used to encode a secret message between two legitimate parties, conventionally known as Alice and Bob, in the presence of an eavesdropper, Eve [1,2]. The security of the QKD scheme may be derived from the uncertainty principle and the no-cloning theorem to allow the exchange of a secure cryptographic key between Alice and Bob. Since the development of the BB84 protocol [1], which is currently the most established protocol, several schemes have been realized due to practical considerations and different implementation requirements. Amongst these protocols are, prepare and measure schemes which include the BB84 [1], B92 [3], six-state [4], and SARG04 [5] protocol and the entanglement based schemes such as the E91 protocol [6].

This paper aims to show the feasibility of an implementation of the B92 protocol by using the id3100 Clavis^2 system from idQuantique. Despite the B92 protocol being more straightforward to implement than the BB84 protocol, surprisingly, this advantage has not been fully exploited. Therefore, in this paper we exploit this advantage and implement the B92 protocol using the id3100 Clavis^2 system. Moreover, we also perform the security analysis of the protocol. This article is organized as follows. Section 2 discusses the background of the B92 QKD protocol and the Plug and Play scheme implemented through the id3100 Clavis^2 system. This is followed by the experimental setup we used to implement the B92 protocol in Section 3. In Section 4, we discuss the results, and finally, Section 5 provides the conclusion.

2 Theory

2.1 B92 QKD protocol

Like the typical BB84 protocol, the B92 protocol follows the usual QKD procedure, with quantum and classical phases. However, opposed to the BB84 protocol, which uses four quantum states, the B92 protocol uses two non-orthogonal quantum states to encode information. In principle, encoding information between two non-orthogonal states makes it impossible for an eavesdropper to distinguish between the two quantum states of the system [2]. Again instead of single-photon

* Corresponding author e-mail: mafum@biust.ac.bw

states, the B92 protocol relies on the coherent states and implements a homodyne measurement at Bob [3]. Moreover, the type of encoding in the B92 protocol makes it less tolerant to noise because of Eve's high probability of unambiguous discrimination of the encoded key bit. However, this is impossible in the BB84 protocol because Alice's encoding is chosen at random [7].

In the B92 protocol, Alice chooses one of two non-orthogonal states with a priori probability of $1/2$. The bits '0' and '1' are encoded into these two quantum states. The non-orthogonal quantum states are encoded into weak coherent states $|\pm\alpha\rangle$ for $\alpha \in \mathbb{R}$, which are accompanied by a strong reference pulse [2]. Several theoretical and experimental progress has been reported in various papers for the B92 protocol in the last decade. In particular, an unconditional security proof of the B92 protocol where it is first reduced to an entanglement distillation protocol initiated by a local filtering process was reported by Tamaki and Lütkenhaus in 2003 [8,9]. On the other hand, Tamaki obtained proof against individual attacks over a realistic channel [10]. The unconditional security proof for the B92 protocol implemented by a strong phase-reference pulse instead of the weak pulse assumption was shown by Koashi in 2004 [11].

Later, again Tamaki and Lütkenhaus showed that this protocol could be implemented over the loss-free channel by adapting it to accommodate the loss. Additionally, they demonstrated the unconditional security proof of the B92 protocol over a lossy and noisy channel. In the proof, it is assumed that Alice and Bob employ an error discarding protocol [12]. Compared to the BB84 protocol, the B92 protocol is weaker against the eavesdropping attacks, i.e., intercept and resend attacks that add to channel noise. Therefore, to compensate for channel noise, the protocol uses weak coherent states and a strong reference pulse. In particular, using a strong reference pulse, the eavesdropper Eve, is prevented from blocking the whole signal without causing any errors. This is seen in Tamaki *et al.* (2009), where they reported an unconditional security proof when this protocol is implemented with a strong reference pulse [14].

Regardless of the challenges that come with aligning and stabilizing both interferometers, which makes the system very sensitive and requiring the need for active control in the B92 scheme, successful implementation of the protocol was demonstrated in Ref. [15]. A key distribution for over a 48 km optical length for both the B92 and BB84 protocols was shown by Hughes *et al.* (2000) [16]. Additionally, an experiment of the B92 protocol reaching a distance of 122km of standard telecom fiber was demonstrated by Gobby *et al.* (2000) [17]. A prototype of a free-space QKD scheme based on the B92 protocol has also been reported by Canale *et al.* (2011) [18].

2.2 Plug and Play scheme

The Plug and Play scheme for QKD was introduced by Muller *et al.* (1997) [19]. Figure 1 shows the Plug and Play system. The Plug and Play scheme features Bob's equipment which consists of the laser, couplers, Faraday rotators (FR), mirrors, Mi's, and a single photon detector (D0). In contrast, Alice's equipment consists of a coupler (C), a classical detector (D), a phase modulator (PM), and a Faraday rotator (FR). Bob sends a classical signal to Alice in the scheme, which she attenuates to a single photon average per pulse. Alice then encodes the intended key value into the pulses of the received signal. She then sends the received signal back to Bob, who then performs measurements. This scheme's advantage is that it automatically and passively compensates for a phase drift during the signal transmission, thereby providing stability in optical fiber communication. Another significant advantage of the Plug and Play system is that it does not require additional optical adjustment during operation. Therefore, it is justifiable to implement the B92 protocol on the Plug and Play system (an interferometric set-up) since the original B92 protocol was based on an interferometric set-up [3]. Moreover, the scheme is robust against environmental noises. Although there are still some outstanding security issues regarding this configuration [20,13], the implementation of QKD for over 67 km using a Plug and Play system was demonstrated by Stucki *et al.* (2002) [21]. Again, the Plug and Play was use as part of the SECOQC quantum key distribution network in Vienna [22], and Durban [23].

3 Experimental setup

The Clavis^2 system is a QKD research platform that was developed by idQuantique, Switzerland. The system is used to deploy the Plug and Play implementations of the QKD protocols. The Clavis^2 system uses a proprietary auto-compensating optical platform which reduces the value of the QBER. The Clavis^2 system can provide secure key exchanges up to a distance of about 100km. Our system consists of a dual-computer Plug and Play configuration where two separate computers are used to control the two quantum communication nodes, on the left for Alice's equipment and on the right for Bob's equipment. The set-up is shown in Figure 2. The two nodes are themselves connected by an optical fiber, which acts as a quantum channel. The system operates at the telecommunication wavelength (λ=1500 nm). The classical channel is realized through the ethernet connection between the two communicating computers.

When the Clavis^2 system implements the four-state QKD protocol, Alice encodes the quantum system by applying a phase shift of 0, π, $\frac{\pi}{2}$ or $\frac{3\pi}{2}$. Bob then completes the protocol by performing some measurements, where he chooses the measurement basis by applying a phase shift of either 0 or $\frac{\pi}{2}$ and either π or

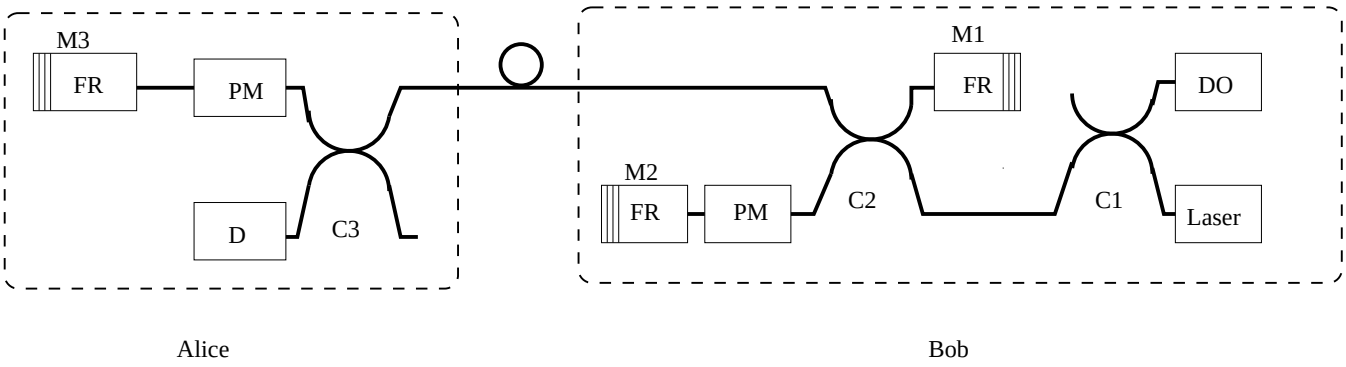

Fig. 1: The Plug and Play system as introduced by Muller *et al.* (1997) [19]. The system makes use of the following components: single-photon detector, D0; fiber coupler, C_i; phase modulator, PM; Faraday rotator, FR; mirror, M_i; classical detector, D.

$\frac{3\pi}{2}$. However, we implemented a two-state protocol in our experiment by limiting the phase shift to two states only. We achieved the implementation by restricting the values of the phase modulator. The first two states are replicated on the first two states, effectively outputting the states required to implement the B92 protocol.

The phase modulators are adjusted to compensate for this change. The voltages applied to the modulators define the phase shift applied to each pulse. These voltages are adjusted such that Alice outputs only two relative phases following the bit choice. The Bob measurement basis induces an interference at the interferometer's exit to provide discrete measurements upon a compatible basis choice. Notably, the software was reprogrammed to accommodate these changes. The B92 protocol is very vulnerable to bright-pulse attacks [4], but fortunately, the Clavis^2 system has a strong classical reference frame. This enables a secure implementation of the B92 protocol. Laser output power was measured to be -14 dBm.

Additionally, detection probabilities were determined for different optical losses, together with the corresponding visibility measurements, and the results are given in Table 2. The next step was the raw key exchange session. This session is more or less similar to the one used for the SARG04 protocol in the Clavis^2 System. The difference is that for the B92 protocol, only one pair of non-orthogonal states is used by Alice for state preparation, while Bob uses the other pair for measurement. This was followed by the key distillation step, from which the QBER and secure key rates for different optical losses were determined. Finally, the key generation rates for the B92 protocol were compared to the key generation rates for the BB84 protocol to ascertain the utility of the B92 implementation. Quantum signals were detected at either detector D1 or D2 shown in Figure 2. During initialization, the dark count probabilities of D1 and D2 were measured to be 5.78 $\times 10^{-5}$ and 5.60 $\times 10^{-5}$, respectively.

Table 1: The experimentally measured QKD parameters for the set-up shown in Fig 2. The parameters are; Loss(dB), which is achieved by varying the attenuation of the signal; Quantum Bit Error Rate (QBER), which is obtained by using Equation (7); P_t refers to the overall probability of photon detection on Bob's side. This probability is evaluated from Equation (5); P_d refers to the dark count probability, and V is the visibility of the fringes as a percentage.

Loss (dB)	QBER	P_t	P_d	V (%)
1	0.0098324	0.1393725	0.0000560	99.65
2	0.0102556	0.1245905	0.0000552	99.55
3	0.0104741	0.1130995	0.0000540	99.30
4	0.0107115	0.105114	0.0000536	99.18
5	0.0109773	0.0947909	0.00005447	98.46
6	0.0110112	0.0856511	0.0000596	97.24
7	0.0110323	0.0417971	0.0000500	94.83

4 Results and Discussion

Table 2 presents the QKD parameters that were measured and later used in the security analysis. These parameters are loss, QBER, P_t probability of detection, and P_d dead time probability and visibility.

The number of photons n in the pulse is Poisson distributed with a mean photon number, μ. Therefore, the probability of finding n photons in a pulse $P(n,\mu)$ can be expressed as [2]

$$P(n,\mu) = \frac{\mu^n e^{-\mu}}{n!}. \quad (1)$$

The signals sent through an optical fiber, in practice, suffer from losses as the distance of transmission increases. This loss is mainly due to scattering in the fiber.

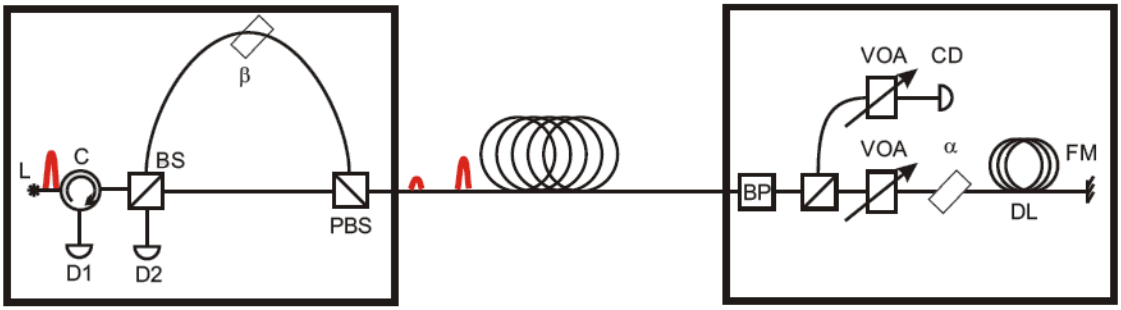

Fig. 2: The experimental set-up for the id3100 Clavis^2 System used for the implementation of the B92 protocol. Two separate computers are used to control nodes: Alice on the right and Bob on the left. The nodes are themselves connected by the optical fiber. The system uses the following; light source, L; beam splitter, BS; detectors; D1&D2; faraday mirror, FM; coupler, C; delay line, DL; variable optical attenuator, VOA.

The most critical parameter which needs to be evaluated in any QKD system is the raw key rate, R_{raw} [2]. The R_{raw} between Alice and Bob is expressed as

$$R_{\text{raw}} = q\nu\mu t_{AB} t_B \eta_B, \tag{2}$$

where q relies on the implementation, ν is the repetition frequency, μ is the average number of photons per pulse, t_{AB} is the transmission on the line between Alice and Bob, t_B is Bob's internal transmission per pulse, and η_B is Bob's detection efficiency. The transmittivity t, of a fiber is given by $t = 10^{-\alpha d/10}$, where α is the attenuation constant and is currently optimal at α=0.2 and d is the transmission distance in km. The internal transmission of the system, including the detection probability and is expressed as [2]

$$\eta_B = t_A t_B \eta_D, \tag{3}$$

where η_B is the detection efficiency of Bob, t_A, t_B is the transmission efficiency of Alice and Bob, respectively, and η_D is the quantum efficiency of Bob's detector. The overall transmission can be expressed similarly as $\eta = t_c \eta_B$ where t_c is the channel transmission. The probability P_s of detecting a signal at the detector is expressed as

$$P_s = 1 - e^{-\eta\mu}. \tag{4}$$

Now, we can evaluate the overall detection probability, P_t, which can be expressed as

$$\begin{aligned} P_t &= P_s + P_d - P_s P_d \\ &\cong P_s + P_d, \end{aligned} \tag{5}$$

where P_d is the dark count probability, and $P_s P_d$ is the coincidence of detection between signal and dark count and is usually neglected in the experiment.

To test the quality of our QKD scheme, we use the quantum bit error rate (QBER). The QBER is an essential parameter in QKD used to investigate the security in QKD protocols [2]. The QBER is simply the fraction of error bits f_c to the total number of bits t_c. The QBER, which is expressed as

$$QBER = \frac{f_c}{t_c} \tag{6}$$

where f_c are false counts and t_c are total counts. The false counts, $f_c = e_0 P_d + P_s$ where e_0 is the error detection due to background and signal respectively while $t_c = P_t$. This is achieved through the use of some extra classical post-processing steps in order to extract the secret key. The QBER can also be written as

$$\begin{aligned} QBER = {} & QBER_{\text{opt}} + QBER_{\text{dark}} + QBER_{\text{after}} \\ & + QBER_{\text{stray}}. \end{aligned} \tag{7}$$

In this expression, $QBER_{\text{opt}}$ is the probability that a photon hits the wrong detector. This can also be used to determine the optical alignment of the polarization components and the stability of the fibre link. This is expressed as

$$QBER_{\text{opt}} = \frac{1-V}{2}, \tag{8}$$

where V is the visibility, $QBER_{\text{dark}}$ is the error due to dark counts. The $QBER_{\text{dark}}$ is expressed as

$$QBER_{\text{dark}} \cong \frac{p_{\text{dark}}}{\mu t_{AB} t_B \eta_B}. \tag{9}$$

The $QBER_{\text{dark}}$ forms the essential parameter in the sense that it increases with distance and therefore limits the range of key distribution. The $QBER_{\text{after}}$ is the error due to after pulses. It is expressed as

$$QBER_{\text{after}} \cong \sum_{n=0}^{n=1/p_{det}} p_{\text{after}}(\tau + \frac{n}{\nu}), \tag{10}$$

where τ refers to the dead time, and $QBER_{\text{stray}}$ refers to error induced by stray light.

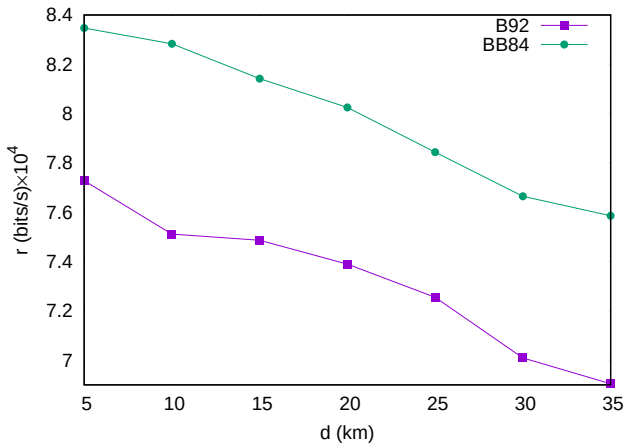

Fig. 3: An illustration of the experimental secret key generation rates for the B92 and BB84 protocols as a function of distance. To find the key rates, we use the formalism developed in Ref [21].

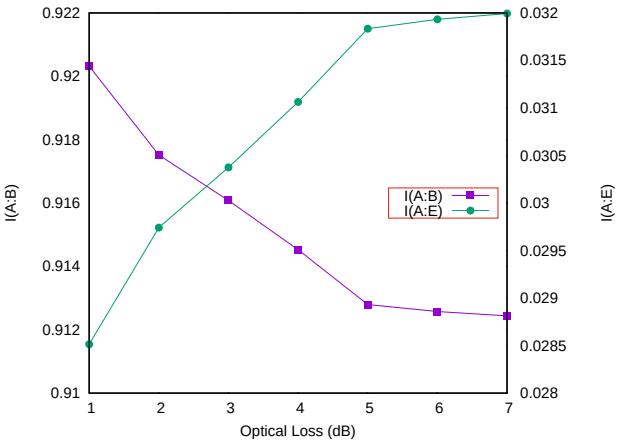

Fig. 4: An illustration of the experimental values for the Shannon mutual information between Alice and Bob $I(A:B)$ and between Alice and Eve $I(A:E)$ against optical loss. The mutual information is evaluated by using the formalism in Ref [21].

Based on our measured parameters, we can calculate the secret key generation rate R, against the photon number splitting (PNS) attacks [24] as

$$R = P_t[(1-\xi')\beta - f_{EC}h(Q)], \tag{11}$$

where $\xi' = \xi(Q/\beta)$ and again $\xi(Q) = \log_2(1+4Q-4Q^2)$, $\beta = (P_t - P')/P_t$, $f_{EC} = 1.05$ is the error correction efficiency and Q is the QBER. Again, in the expression, ξ is the fraction of key discarded during privacy amplification and $P' = 1-(1+\mu+\mu^2/2+\mu^3/12)Q^{-\mu}$. The term $h(Q)$ is the binary entropy function and is expressed as $h(Q) = -Q\log_2(Q) - (1-Q)\log_2(1-Q)$. The variation of the secret rate against distance for the B92 protocol is shown in Figure 3. As expected, the secret key rate obtained is slightly lower than that of BB84 protocol [2]; however, it still scales similarly with that of the standard BB84 protocol.

In Figure 4, we show the variation of $I(A:B)$ and $I(A:E)$ against optical loss. The difference between the two mutual information is given as

$$\eta_{\text{dist}} = I(A:B) - I(A:E), \tag{12}$$

where $I(A:B) = 1 + D\log_2 D + (1-D)\log_2(1-D)$ and D is equal to the total QBER and $I(A:E) \cong 0.03 + I_{2v}$. I_{2v} is a consequence of multi-photon pulses and is about 0.06, 014 and 0.40 for 5, 10 and 20dB losses, respectively, for μ=0.25dB/km. It can also be observed from Figure 4 that an increase in optical loss results in an increase in mutual information between Alice and Eve, as well as a decrease in mutual information between Alice and Bob.

5 Conclusion

In this work, we have experimentally demonstrated that we can adapt the set-up initially designed to run the BB84 and SARG04 protocols and implement the B92 protocol. We have shown how the quantum bit error rate behaves as we vary loss. In particular, we demonstrate that we can achieve reasonable secret key rates that scale similarly to the BB84 protocol for some reasonable communication distance on a fiber optic network in our implementation. In summary, these results show that it is possible to implement the B92 QKD protocol using the Clavis^2 system. This is very useful because, as opposed to the four-state protocol, the B92 protocol uses fewer resources; hence it is more straightforward to implement, thus extending the applicability of the id3100 Clavis^2 system.

Acknowledgement

The first author acknowledges the financial support from the Botswana International University of Science and Technology Research Initiation Grant (Grant number: R00015).

Conflict of Interest

The authors declare that they have no conflict of interest.

References

[1] Bennett, C. H.; Brassard G. Quantum cryptography: Public key distribution and coin tossing. In *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing* New York: Bangalore, India, 1984, pp.175-179.

[2] Gisin, N; Ribordy, G; Tittel, W; Zbinden, H; Quantum cryptography. Rev. Mod. Phys. **2002**, *74*, 145-195.

[3] Bennett, C. H; Quantum cryptography using any two nonorthogonal states. *Phys. Rev. Lett.* **1992**, *68*, 3121.

[4] Bruss D; Optimal Eavesdropping in Quantum Cryptography with Six States. *Phys. Rev. Lett.* **1998**, *81*, 3018-3021.

[5] Scarani, V; Acín, A; Ribordy, G; Gisin, N; Quantum Cryptography Protocols Robust against Photon Number Splitting Attacks for Weak Laser Pulse Implementations *Phys.Rev. Lett.* **2004**, *92*, 057901.

[6] Ekert, A; Quantum cryptography based on Bell's theorem. *Phys. Rev. Lett.* **1991**, *67*, 661-663.

[7] Chefles, A; Barnett, S; Optimum unambiguous discrimination between linearly independent symmetric states. *Phys. Lett. A.* **1998**, *250*, 223-229.

[8] Tamaki, K; Koashi, M; Imoto, N; Unconditionally secure key distribution based on two nonorthogonal states. *Phys. Rev. Lett.* **2003**, *90*, 167904.

[9] Mafu, M; A Simple security proof for entanglement-based quantum key distribution. *Journal of Quantum Information Science* **2016**, *6*, 296-303.

[10] Tamaki, K; Koashi, M; Imoto, N; Security of the Bennett 1992 quantum-key distribution protocol against individual attack over a realistic channel. *Phys. Rev. A.* **2003**, *67*, 032310.

[11] Koashi, M; Unconditional security of coherent-state quantum key distribution with a strong phase-reference pulse. *Phys. Rev. Lett.* **2004**, *93*, 120501.

[12] Tamaki, K; Lütkenhaus, N; Unconditional security of the Bennett 1992 quantum key-distribution protocol over a lossy and noisy channel. *Phys. Rev. A.* **2004**, *69*, 032316.

[13] Mafu M, Garapo K and Petruccione F; Finite-size key in the Bennett 1992 quantum-key-distribution protocol for Rényi entropies. *Phys. Rev. A.* **2013**, *88*, 062306

[14] Tamaki, K; Lütkenhaus, N; Koashi, M; Batuwantudawe, J; Unconditional security of the Bennett 1992 quantum-key-distribution scheme with a strong reference pulse. *Phys. Rev. A.* **2009**, *80*, 032302.

[15] Bourennane, M; Ljunggren, D; Karlsson, A; Jonsson, P; Hening, A; Ciscar, J. P; Experimental long wavelength quantum cryptography: from single-photon transmission to key extraction protocols. *J. Mod. Optics* **2000**, *47*, 563-579.

[16] Hughes, R. J; Morgan, G. L; Peterson, C. G; Quantum key distribution over a 48 km optical fibre network. *J. Mod. Optics* **2000**, *47*, 533-547.

[17] Gobby, C; Yuan, Z; Shields, A; Quantum key distribution over 122 km of standard telecom fiber. *Appl. Phys. Lett.* **2004**, *84*, 3762-3764.

[18] Canale, M; Bacco, D; Calimani, S; Renna, F; Laurenti, N; Vallone, G; Villoresi, P; A prototype of a free-space QKD scheme based on the B92 protocol. In *Proceedings of the 4th International Symposium on Applied Sciences in Biomedical and Communication Technologies (ACM)* 2011, pp. 186.

[19] Muller, A; Herzog, T; Huttner, B; Tittel, W; Zbinden, H; Gisin, N; Plug and Play systems for quantum cryptography. *Appl. Phys. Lett.* **1997**, *70*, 793.

[20] Zhao, Y; Qi, B; Lo, H. K; Quantum key distribution with an unknown and untrusted source. *Phys. Rev. A.* **2008**, *77*, 052327.

[21] Stucki, D; Gisin, N; Guinnard, O; Ribordy, G; Zbinden, H; Quantum key distribution over 67 km with a plug&play system. *New. J. Phys* **2002**, *4*, 41.

[22] Peev, M; Pacher, C; Alléaume, R; Barreiro, C; Bouda, J; Boxleitner, W; Debuisschert, T; Diamanti, E; Dianati, M; Dynes, J; *et al.* The SECOQC quantum key distribution network in Vienna. *New J. Phys.* **2009**, *11*, 075001

[23] Mirza, A; Petruccione, F; Realizing long-term quantum cryptography. *JOSA. B* **2010**, *27*, 185-188.

[24] Acín, A; Gisin, N; Scarani, V; Coherent-pulse implementations of quantum cryptography protocols resistant to photon-number-splitting attacks. *Phys. Rev. A.* **2004**, *69*, 012309.

Mhlambululi Mafu is a Senior Lecturer at Botswana International University of Science and Technology, Botswana. He received his Ph.D. degree in Physics from the University of KwaZulu-Natal. His research interests are in theoretical and experimental quantum key distribution.

Makhamisa Senekane is a Senior Researcher in the Institute of Intelligent Systems, at the University of Johannesburg, South Africa. He obtained his Ph.D. in Physics from the University of KwaZulu-Natal, his MSc. Eng. in Electrical Engineering from the University of Cape Town, and his B. Eng. in Electronics from the National University of Lesotho.