Security of the Bennett 1992 quantum key distribution protocol in the presence of noise

Mhlambululi Mafu[1], Makhamisa Senekane[2], Kevin Garapo[2] and Francesco Petruccione[2,3]

[1] Department of Physics and Astronomy, Botswana International University of Science and Technology, P/Bag 16, Palapye, Botswana
[2] Centre for Quantum Technology, School of Chemistry and Physics, University of KwaZulu-Natal, P/Bag X54001 Durban, South Africa
[3] National Institute for Theoretical Physics (NITheP-KZN), P/Bag X54001 Durban, South Africa

E-mail: mafum@biust.ac.bw, makhamisa12@gmail.com, petruccione@ukzn.ac.za

Abstract. Quantum key distribution allows two parties, Alice and Bob to generate a secret key in the presence of an eavesdropper, Eve [Gisin N, Ribordy G, Tittel W and Zbinden H 2002 *Rev. Mod. Phys.* **74** 145-195]. It promises the legitimate parties to exchange private information by means of provably-secure protocols. The security is based solely on the quantum mechanical laws of physics. Since quantum key distribution is at the level of implementation and since these protocols usually operate in some noisy channels, we investigate how the addition of noise in the communication channel affects the secret key generation rates. The effect of noise for four-state and six-state protocols has been already studied [Mertz M, Kampermann H, Shadman Z and Bruß D 2013 *Phys. Rev. A* **87(4)** 042312]. Here, we investigate the behavior of the secret key when one adds some noise before classical processing for the two-state Bennett 1992 quantum key distribution protocol.

1. Introduction

Quantum key distribution (QKD) uses quantum mechanical concepts such as the quantum no-cloning theorem, Heisenberg's uncertainty principle and quantum entanglement to guarantee a secure communication between two ligitimate communicating parties Alice (the sender) and Bob (the receiver) in such a way that the presence of an eavesdropper (Eve) could be revealed. The first QKD protocol was proposed in 1984 by C. Bennett and G. Brassard, and is known as the BB84 protocol [1]. Another major QKD protocol was proposed by Artur Ekert in 1991, and is known as the E91 protocol [2].

QKD protocols can be divided into two major classes, namely discrete-variable and continuous variable QKD protocols [3]. This manuscript only investigates a class of discrete-variable QKD protocols. This class can be classified into two schemes, namely prepare and measure (P&M) and entanglement-based schemes. The BB84 protocol falls in the former scheme, while the E91 protocol is in the latter. Other notable P&M protocols are the B92 protocol proposed by C. Bennett in 1992 [4], SARG04 proposed by V. Scarani, A. Acin, G. Ribordy and N. Gisin in 2004 [5] and a six-state QKD protocol proposed by D. Bruß [6]. Security proofs for these P&M protocols have been reported [7, 8, 9, 9, 10, 11, 12, 13]. Addittionally, in Ref. [14], security of

both four-state and six-state QKD protocols in the presence of noise is reported. However, no work has been reported on the security analysis of the two-state B92 protocol in the presence of noise. This is despite the fact that the B92 protocol, being a two-state protocol, uses least resources and hence is the simplest to implement. In this manuscript, we analyze the security of the B92 protocol when the quantum noise is added to the quantum communication.

The remainder of this manuscript is structured as follows. The next section provides a background information on the B92 protocol. Section 3 provides a primer on quantum channels. This is followed by Section 4, which provides security analysis for the B92 QKD protocol. The last section concludes this manuscript.

2. The B92 QKD protocol

The B92 protocol was proposed by C. Bennett in 1992 [4]. It is a simplified version of the original BB84 protocol, and it only uses two non-orthogonal states. The protocol is then realized through unambiguous discrimination of these two non-orthogonal states [15, 16, 17]. Since this protocol uses only two states, as opposed to the four-state BB84 protocol, it uses less resources, hence it is simpler to implement. The two states used for this protocol can be denoted as

$$|\psi_0\rangle = |0\rangle, \tag{1}$$

for the bit-value 0 and

$$|\psi_1\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), \tag{2}$$

for the bit-value 1.

The B92 protocol uses two communication channels, namely the quantum channel and the classical channel. To initialize the protocol, Alice generates a random bit sequence. The operation of this protocol using the quantum channel can be summarized as follows [16]:

- Alice encodes each bit generated into a qubit, encoding 0 on $|\psi_0\rangle$ and 1 on $|\psi_1\rangle$.
- Alice then sends the resulting qubit sequence to Bob.
- Bob in return applies unambiguous state discrimination on each qubit he receives from Alice.

Once the quantum communication is finished, Alice and Bob then communicate over the classical channel to complete the protocol [17]. The classical communication procedure can be summarized as thus:

- Bob communicates to Alice about the instances where unambiguous discrimination succeeded.
- They both (Alice and Bob) then keep those bits which correspond to instances where unambiguous discrimination succeeded, and discard the rest. The remaining bits then form a raw key.
- They then compare some of their bits to detect the presence of an eavesdropper. The presence of an eavesropper would result in an error rate of 35% or more [16]. If an eavesdopper is detected, the protocol is aborted, else the protocol proceeds.
- Both Alice and Bob use an error correction technique to correct some errors left in the raw key.
- Finally, Alice and Bob use a privacy amplification scheme to considerably reduce the amount of information that an eavesdropper might have about the key. The result of this is a secret key for both Alice and Bob.

3. A primer on quantum channels

A quantum channel is a quantum operation (mapping) with the following properties [18, 19]:

- linearity,
- trace-preservation, and
- complete positivity.

3.1. Bit-flip channel

A bit flip channel applies the identity operator $\mathbf{I}$ with probability p and Pauli $\mathbf{X}$ (σ_x) operation to a quantum state with probability 1-p. For a quantum state ρ, the bit-flip channel transforms the state such that:

$$\rho \mapsto p\mathbf{X}\rho\mathbf{X}^\dagger + (1-p)\rho. \tag{3}$$

3.2. Dephasing channel

The dephasing channel is also known as the phase-flip channel. For any quantum state ρ, the phase-flip channel transforms the state such that for probability p:

$$\rho \mapsto (1-p)\rho + p\mathbf{Z}\rho\mathbf{Z}, \tag{4}$$

where $\mathbf{Z}$ is the Pauli σ_z operator.

3.3. Pauli channel

The Pauli channel is the generalization of the bit-flip channel and the dephasing channel. This channel is very important for QKD security analysis, since Eve induces such a channel on the QKD protocol [19]. For a two-dimensional quantum state ρ, the mapping due to the Pauli channel is given as:

$$\rho \mapsto \sum_{i,j=0}^{1} p(i,j)\mathbf{Z}^i\mathbf{X}^j\rho\mathbf{X}^j\mathbf{Z}^i. \tag{5}$$

3.4. Depolarizing channel

This channel is the most pessimistic channel [19]. It maps a given state ρ such that for a probability p:

$$\rho \mapsto (1-p)\rho + p\pi, \tag{6}$$

where π is given as $\frac{\mathbf{I}}{d}$ for a d-dimensional system. Hence, for a two-dimesional quantum system, π is simply given as $\frac{\mathbf{I}}{2}$.

4. Security of the B92 protocol

One of the techniques used to analyze the security of a P&M protocol is to reduce it to an entanglement distillation protocol (EDP). We employ this technique in our security analysis of the B92 QKD protocol in the presence of noise. Additionally, it is worth noting that if

$$|\langle\psi_0|\psi_1\rangle|^2 = \frac{1}{2}, \tag{7}$$

for two non-orthogonal states, the security analysis of the B92 protocol reduces to the analysis of symmetric QKD protocols like the BB84 and the six-state protocols.

In order to realize the B92 protocol, let the state being sent by Alice to Bob be given as

$$|\varphi_j\rangle = \beta|0\rangle + (-1)^j\alpha|1\rangle, \tag{8}$$

where $j = 0$ or 1, $\beta = \sqrt{1-\alpha^2}$, and $0 < \alpha < 1/\sqrt{2}$. Additionally, let $|\varphi'_j\rangle$ be a vector orthonormal to $|\varphi_j\rangle$. During the sifting stage, Alice and Bob discard the signals where Bob measured $|\varphi_j\rangle$ and retain those signals where he measured $|\varphi'_j\rangle$. The joint state between Alice and Bob can be given as

$$|\Psi\rangle = \frac{1}{\sqrt{2}}[|0\rangle_A|\varphi_0\rangle_B + |1\rangle_A|\varphi_1\rangle_B]. \tag{9}$$

Finally, let X be a collection of Alice's signals, Y be Bob's signals and E be a collection of Eve's signals, then the asymptotic secret key rate is given as

$$r = S(X|E) - H(X|Y), \tag{10}$$

where H(.) is Shannon binary entropy and S(.) is von Neumann entropy [18]. For discrete variable X and probability p_i, Shannon binary entropy H(X) is given as

$$H(X) = -\sum_i p_i \log p_i. \tag{11}$$

On the other hand, for a density operator ρ, von Neumann entropy is given as

$$S(X)_\rho = -tr(\rho \log \rho) = -\sum_i \lambda_i \log \lambda i, \tag{12}$$

where λ_i are the eigenvalues of ρ.

Let U_{BE} be Eve's evolution state, then the total state ρ_{ABE} after an action U_{BE} is given by

$$\rho_{ABE} = (\mathbf{I}_A \otimes U_{BE})(|\Psi\rangle\langle\Psi|_{AB} \otimes |X\rangle\langle X|_E). \tag{13}$$

Conventional security analyses adopt a very pessimistic view, where all the disturbances are attributed to Eve's intervention. This limits the key rates that could be generated. In this work, we adopted a different approach as follows. Depending on the nature of the channel, we can discern whether disturbance is due to eavesdropping or due to channel loss. This means that the disturbances due to channel losses would not give Eve any information about the key. This way, key generation rates would be enhanced.

In what follows, we provide the security analyses of the B92 protocol under different scenarios of quantum noise. It is also worth noting that an introduction of noise varies a quantum state ρ, which in turn changes von Neumann entropy S(ρ), since it (von Neumann entropy) is the function of ρ. Because key rate r is dependent on S(ρ), then varying noise (and hence ρ) will also affect the key rate r.

4.1. Security of the B92 protocol using bit-flip channel

When a bit-flip channel is used, the joint state of Alice, Bob and Eve can be derived to be

$$\rho_{ABE} = (\mathbf{I}_A \otimes U_{BE})(\mathbf{I}_A \otimes \mathbf{N}_{bf}\mathbf{I}_E)(|\Psi\rangle\langle\Psi|_{AB} \otimes |X\rangle\langle X|_E), \tag{14}$$

where $|X\rangle$ is Eve's initial state and $\mathbf{N}_{bf}$ is the bit-flip channel noise introduced by Alice, and is given in equation (3). Eve's unitary interaction (U_{BE}) can be given as

$$U_{BE}|0\rangle|X\rangle_E = \sqrt{1-\delta}|0\rangle_B|A\rangle_E + \sqrt{\delta}|1\rangle_B|B\rangle_E \tag{15}$$

$$U_{BE}|1\rangle|X\rangle_E = \sqrt{1-\delta}|1\rangle_B|C\rangle_E + \sqrt{\delta}|0\rangle_B|D\rangle_E, \tag{16}$$

where δ is the disturbance ($\delta = [0, \frac{1}{2}]$), $|X\rangle_E$ is Eve's initial state, and $|A\rangle_E$, $|B\rangle_E$, $|C\rangle_E$ and $|D\rangle_E$ are her states after the interaction. The disturbance corresponds to the QBER introduced

by Eve if the channel is noiseless. Using the argument given in [14], $|A\rangle_E$, $|B\rangle_E$, $|C\rangle_E$ and $|D\rangle_E$ are then determined. They are chosen in a way such that U_{BE} is a unitary operator. For example in the first instance, $\langle X|\langle 0|U^\dagger U|1\rangle|X\rangle = (\sqrt{1-\delta}\langle A|\langle 0| + \sqrt{\delta}\langle B|\langle 1|)(\sqrt{1-\delta}|1\rangle|C\rangle + \sqrt{\delta}|0\rangle|D\rangle)$ where the unitary results in the first constraint $\langle A|D\rangle + \langle B|C\rangle = 0$. One can apply the same unitary transformation U should be applied to the other initial states to get the other constraints in order to evaluate the states $|A\rangle_E$, $|B\rangle_E$, $|C\rangle_E$ and $|D\rangle_E$.

By tracing out Eve's state in ρ_{ABE}, the shared state between Alice and Bob, ρ_{AB}, can is then determined. Finally, by performing local von Neumann measurements on ρ_{ABE}, the state ρ_{XYE} is obtained. By tracing out either Bob's part or Eve's part, states ρ_{XE} and ρ_{XY} are obtained respectively, and these states are then used in Equation(10) to calculate the key rate r.

The procedure explained above is also used to calculate the key rate for the remaining noise scenarios given below. It is worth noting that for different noise scenarios, the formalism would still be the same. The only difference would be introduced by the noise scenario under consideration.

4.2. Security of the B92 protocol using dephasing channel

When Alice deliberately adds the dephasing noise, the joint state of three parties can be given as

$$\rho_{ABE} = (\mathbf{I}_A \otimes U_{BE})(\mathbf{I}_A \otimes \mathbf{N}_{deph}\mathbf{I}_E)(|\Psi\rangle\langle\Psi|_{AB} \otimes |X\rangle\langle X|_E), \tag{17}$$

where U_{BE} is Eve's evolution state, $|X\rangle$ is Eve's initial state, and $\mathbf{N}_{deph}$ is the phase-flip channel noise introduced by Alice, and is given in equation (4).

4.3. Security of the B92 protocol using Pauli channel

For the Pauli channel noise added to the communication channel by Alice, similarly to equations (14) and (17), and with the Pauli channel mapping $\mathbf{N}_{Pauli}$, the joint state of three parties is then given as

$$\rho_{ABE} = (\mathbf{I}_A \otimes U_{BE})(\mathbf{I}_A \otimes \mathbf{N}_{Pauli}\mathbf{I}_E)(|\Psi\rangle\langle\Psi|_{AB} \otimes |X\rangle\langle X|_E). \tag{18}$$

4.4. Security of the B92 protocol using depolarizing channel

Lastly, for the joint state of the depolarizing channel can be derived to be

$$\rho_{ABE} = (\mathbf{I}_A \otimes U_{BE})(\mathbf{I}_A \otimes \mathbf{N}_{dep}\mathbf{I}_E)(|\Psi\rangle\langle\Psi|_{AB} \otimes |X\rangle\langle X|_E), \tag{19}$$

where $\mathbf{N}_{dep}$ is the depolarizing noise added by Alice.

5. Conclusion

We have reported the security of the B92 protocol when the noise is added to the quantum channel. We considered different scenarios of quantum noise, and investigated security and hence robustness of the protocol in the presence of such a noise. Our work was only limited to the asymptotic key analysis. Future work will focus on the finite key analysis. Additionally, addition of noise using concatenated quantum channels deserves an investigation, because this might shed more light on how to minimize Eve's knowledge of the secret key.

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. M.M. acknowledges support from the BIUST.

References

[1] Bennett C H, Brassard G *et al.* 1984 Quantum cryptography: Public key distribution and coin tossing *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing* vol 175 (New York)

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

[3] Van Assche G 2006 *Quantum cryptography and secret-key distillation* (Cambridge University Press)

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

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

[6] Bruß D *Phys. Rev. Lett.* **81** 3018

[7] Lo H K and Chau H F *Science* **283** 2050–2056

[8] Shor P and Preskill J *Phys. Rev. Lett.* **85** 441

[9] Gottesman D, Lo H K, Lütkenhaus N and Preskill J 2004 Security of quantum key distribution with imperfect devices *Proceedings of IEEE International Symposium on Information Theory* (IEEE) p 136

[10] Christandl M, Renner R and Ekert A *Arxiv Preprint: quant-ph/0402131*

[11] Renner R, Gisin N and Kraus B *Physical Review A* **72** 012332

[12] Scarani V, Bechmann-Pasquinucci H, Cerf N J, Dušek M, Lütkenhaus N and Peev M 2009 *Reviews of modern physics* **81** 1301

[13] Tomamichel M, Lim C C W, Gisin N and Renner R 2012 *Nature Communications* **3** 1

[14] Mertz M, Kampermann H, Shadman Z and Bruß D 2013 *Physical Review A* **87** 042312

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

[16] Bergou J and Hillery M 2013 *Introduction to the theory of quantum information processing* (Springer)

[17] Senekane M, Mirza A, Mafu M and Petruccione F 2012 Realization of B92 qkd protocol using id3100 Clavis^2 system *Proceedings of the 56th SAIP Conference* (SAIP) pp 1–6

[18] Nielsen M and Chuang I 2010 *Quantum computation and quantum information* (Cambridge University Press)

[19] Wilde M 2013 *Quantum information theory* (Cambridge University Press)