Upper bound to accessible information for the six-state quantum key distribution protocol

Mhlambululi Mafu[1], **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: 209526077@stu.ukzn.ac.za, petruccione@ukzn.ac.za

Abstract. It is necessary for any quantum key distribution protocol to have an unconditional security proof which is robust against any kind of attacks that are allowed by the laws of physics. This is the main advantage of quantum key distribution schemes over classical ones aiming to achieve the same task. We derive an upper bound on the achievable information that an eavesdropper may obtain. Instead of the known method of conditioning on the random variable, we express Eve's information about the raw key as a function of the error since it is related to the secret key function. The proposed method reproduces the upper bound that was derived previously.

1. Introduction

Quantum key distribution (QKD) allows two distant parties, traditionally known as Alice and Bob who are connected by an authenticated classical channel and insecure quantum channel to establish a secure random cryptographic key under the intervention of an eavesdropper, Eve [1]. However, there stands a theoretical challenging problem of determining the necessary conditions for security in QKD schemes. The main task for a security analysis is to figure out what the length of the final secure key is and perform hashing in order to obtain the final key. The lower and upper bounds on the secret key rate which involve entropies of two qubit density operators for the six-state protocol has been found [2]. The security of the protocol against optimal eavesdropping on noisy states has been studied [3, 4]. We highlight that the unconditional security proof of the six-state protocol has been shown in various papers [5, 6, 7].

In this paper our goal is to re-derive an upper bound on the achievable information that an eavesdropper may obtain about the key and also to improve the security threshold. We highlight that in order to improve the security threshold a known method of conditioning on the random variable is used for the BB84 protocol [8]. However, in this paper we apply it to the six-state protocol by expressing Eve's information about the raw key as a function of the error since it is related to the secret key function. The proposed method reproduces the upper bound that was derived previously. This maximum threshold in the secret key fraction is important in the QKD security of the protocol as it determines the maximum value in which the secret key can be extracted in the presence of an eavesdropper while the protocol remains secure.

2. The Six-state protocol

The six-state protocol makes use of three different encodings which are defined by the x basis $\{|0\rangle_x, |1\rangle_x\} := \{\frac{1}{2}(|0\rangle_z \pm |1\rangle)\}$, the y basis $\{|0\rangle_y, |1\rangle_y\} := \{\frac{1}{2}(|0\rangle_z \pm i|1\rangle)\}$ and the z basis as $\{|0\rangle_z, |1\rangle_z\}$. In this protocol, Alice randomly selects with equal probability ($p = 1/3$) the basis she uses and then sends the appropriate qubit to Bob in the base she chose. By making use of the classical channel, Alice announces to Bob which bases she used. In the event that Bob measures in Alice's basis (the sent qubit agrees with the measured qubit) they use these values to form the key.

Similarly, the six-state protocol [9] displays symmetry just like the BB84 protocol [10]. However, the six-state protocol is more symmetrical due to the fact that three bases span the full Bloch sphere (symmetrically distributed) as opposed to the BB84 where only a two-dimensional plane is spanned. In the six-state protocol only 1/3 of the qubits are kept and the rest discarded. For comparison in the BB84 protocol only 1/2 of the qubits are kept and the rest are discarded. Due to the symmetry in the six-state protocol, one can compute the bounds restricting consideration to collective attacks and the joint attacks such that the final state of Alice and Bob is Bell-diagonal as shown below

$$\rho_{AB} = \gamma_1|\phi^+\rangle\langle\phi^+| + \gamma_2|\phi^-\rangle\langle\phi^-| + \gamma_3|\psi^+\rangle\langle\psi^+| + \gamma_4|\psi^-\rangle\langle\psi^-|, \tag{1}$$

with $\gamma_1 + \gamma_2 + \gamma_3 + \gamma_4 = 1$, where the Bell states are defined as

$$|\phi^\pm\rangle = \frac{1}{\sqrt{2}}(|00\rangle \pm |11\rangle), \qquad |\psi^\pm\rangle = \frac{1}{\sqrt{2}}(|01\rangle \pm |10\rangle). \tag{2}$$

If we perform the substitution of Equation (2) into Equation (1) we proceed as follows

$$\begin{aligned}
\rho_{AB} &= \gamma_1|\phi^+\rangle\langle\phi^+| + \gamma_2|\phi^-\rangle\langle\phi^-| + \gamma_3|\psi^+\rangle\langle\psi^+| + \gamma_4|\psi^-\rangle\langle\psi^-| \\
&= \tfrac{\gamma_1}{2}(|00\rangle\langle 00| + |11\rangle\langle 11| + |00\rangle\langle 11| + |11\rangle\langle 00|) + \tfrac{\gamma_2}{2}(|00\rangle\langle 00| + |11\rangle\langle 11| - |00\rangle\langle 11| - |11\rangle\langle 00|) \\
&= \tfrac{\gamma_3}{2}(|01\rangle\langle 01| + |10\rangle\langle 10| + |10\rangle\langle 01| + |01\rangle\langle 10|) + \tfrac{\gamma_4}{2}(|01\rangle\langle 01| + |10\rangle\langle 10| - |10\rangle\langle 01| - |01\rangle\langle 10|) \\
&= (\tfrac{\gamma_1}{2} + \tfrac{\gamma_2}{2})(|00\rangle\langle 00| + |11\rangle\langle 11|) + (\tfrac{\gamma_1}{2} - \tfrac{\gamma_2}{2})(|00\rangle\langle 00| + |11\rangle\langle 11|) + (\tfrac{\gamma_3}{2} + \tfrac{\gamma_4}{2})(|01\rangle\langle 01| + |10\rangle\langle 10|) \\
&= (\tfrac{\gamma_1}{2} - \tfrac{\gamma_2}{2})(|00\rangle\langle 00| + |11\rangle\langle 11| + |00\rangle\langle 11|) + 2\varepsilon\frac{(|00\rangle\langle 00| + |11\rangle\langle 11|)}{4} + 2\varepsilon\frac{(|01\rangle\langle 01||10\rangle\langle 10|)}{4} \\
&= (\tfrac{\gamma_1}{2} - \tfrac{\gamma_2}{2})|\psi^+\rangle\langle\psi^+| + 2\varepsilon\tfrac{\mathbb{I}}{4} \\
&= (1 - 2\varepsilon)|\psi^+\rangle\langle\psi^+| + 2\varepsilon\tfrac{\mathbb{I}}{4}.
\end{aligned} \tag{3}$$

In order to simplify the last step we make use of the additional constraint on the eigenvalues, i.e., $\gamma_3 = \varepsilon - \gamma_2$ which it has been shown to yield $\gamma_1 = 1 - 3/2\varepsilon$ and $\gamma_i = \varepsilon/2$ for $i = \{2, 3, 4\}$. This corresponds to a security threshold of 6.8% when evaluated for the above state. The states $|\phi^\pm\rangle$ give perfect correlations in the z-basis, $|\psi^\pm\rangle$ give perfect anticorrelations in the x-basis where the probabilities $\sum_i \gamma_i = 1$. As we highlighted that in the original security proof [8] for the BB84 protocol, in order to improve this security threshold, a conditioning on the random variable, i.e., $W = X \otimes Y$ was performed. The random variable contains all the information about the error positions. However, in our derivation we express Eve's information about the raw key $I_E(\underline{\varepsilon})$ as a function of the error positions which appears to be more elegant.

In this protocol, the third basis is conjugate to the others. Since γ_3 and γ_4 bring perfect anticorrelations which is equivalent to the quantum bit-error-rate (QBER) in the z-basis then

$$\varepsilon_z = \gamma_3 + \gamma_4.$$

The constraints on the eigenvalues yield the error rates in the other bases such that

$$\gamma_2 = \varepsilon_x - \gamma_4,$$

and

$$\gamma_3 = \varepsilon_y - \gamma_2.$$

Eve's information can be calculated by using the Holevo bound which states that

$$I_E = S(\rho_E) - \tfrac{1}{2}S(\rho_{E|0}) - \tfrac{1}{2}S(\rho_{E|1}). \tag{4}$$

The entropy of the state after the purification of Eve, ρ_{AB} becomes

$$S(\rho_E) = S(\rho_{AB}) = H(\{\gamma_1, \gamma_2, \gamma_3, \gamma_4\}) \equiv H(\underline{\gamma}), \tag{5}$$

where H is the Shannon entropy. A purification $|\psi\rangle_{ABE} = \sum_i \sqrt{\gamma_i}|\phi_i\rangle_{AB}|e_i\rangle_E$ was used to calculate $\rho_{E|b}$, by using a change of notation for the Bell states, and $\langle e_i|e_j\rangle = \delta_{ij}$ where e_i and e_j are two orthonormal basis, we trace out Bob and then project Alice on $|+z\rangle$ for $b = 0$ and on $|-z\rangle$ for $b = 1$. Since there is no preference in this attack, because both values are equiprobable then

$$S(\rho_{E|0}) = S(\rho_{E|1}) = h(\varepsilon_z). \tag{6}$$

By substituting the relationship in Equation (4) and using Equation (5) we get

$$I_E(\underline{\gamma}) = H(\underline{\gamma}) - h(\varepsilon_z). \tag{7}$$

Using the above constraints we arrive at

$$\varepsilon_x - \varepsilon_y = \gamma_4 - \gamma_3.$$

We add this constraint to ε_z in order to eliminate γ_3 we get

$$\varepsilon_x - \varepsilon_y + \varepsilon_z = 2\gamma_4.$$

After dividing each term by ε_z we get

$$\frac{1 + (\varepsilon_x - \varepsilon_y)/\varepsilon_z}{2} = \gamma_4/\varepsilon_z.$$

Starting from the sum of probabilities ($\sum_i \gamma_i = 1$), we can express γ_1 in terms of the other constraints,

$$\begin{aligned}\gamma_1 &= 1 - (\gamma_2 + \gamma_3 + \gamma_4)\\ &= 1 - (\varepsilon_x + \varepsilon_y + \varepsilon_z)/2.\end{aligned} \tag{8}$$

However, in this proof, the error positions are still employed. Instead of conditioning on the random variable in order to increase the security threshold, the Eve's information about the raw key, $I_E(\underline{\varepsilon})$ is used in this derivation. If no error occurred, we obtain $h\left(\frac{\gamma_1}{1-\varepsilon_z}\right)$ and if an error occurred we obtain $h\left(\frac{\gamma_4}{\varepsilon_z}\right)$. By averaging over the four subsystems we obtain

$$I_E(\underline{\varepsilon}) = \varepsilon_z h\left(\frac{1 + (\varepsilon_x - \varepsilon_y)/\varepsilon_z}{2}\right) + (1 - \varepsilon_z) h\left(\frac{1 - (\varepsilon_x + \varepsilon_y + \varepsilon_z)/2}{1 - \varepsilon_z}\right). \tag{9}$$

Using the assumption for the depolarizing channel, where we use, $\varepsilon_x = \varepsilon_y = \varepsilon_z = \varepsilon$, then $I_E(\underline{\varepsilon})$

$$I_E(\underline{\varepsilon}) = \varepsilon + (1 - \varepsilon) h\left(\frac{1 - 3\varepsilon/2}{1 - \varepsilon}\right).$$

Using $r = 1 - h(\varepsilon) - I_E(\underline{\varepsilon})$ to find the secret fraction (one-way postprocessing, no preprocessing and perfect error correction) and then equating it to zero so that we can obtain the value for ε we arrive at

$$\varepsilon + h(\varepsilon) + (1 - \varepsilon) h\left(\frac{1 - 3\varepsilon/2}{1 - \varepsilon}\right) = 1. \tag{10}$$

Solving this equation gives us the lower bound on the bit error rate for the six state scheme using one-way classical post-processing. Thus, the bound on the bit error rate becomes $\varepsilon \approx 0.1261$.

3. Conclusion

We have derived the upper bounds to the accessible information for the six-state protocol without using the technique of conditioning on the random variable and we arrived at the same QBER. This value shows the limit to which the channel should be considered to be secure for the safe generation of a secret key. Above this value, the channel is insecure and the parties abort the protocol.

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

[2] Renner R, Gisin N and Kraus B 2005 *Physical Review A* **72** 12332

[3] Shadman Z, Kampermann H, Meyer T and Bruss D 2008 *Arxiv preprint arXiv:0804.0587*

[4] Bruß D and Macchiavello C 2002 *Phys. Rev. Lett.* **88**(12) 127901 URL `http://link.aps.org/doi/10.1103/PhysRevLett.88.127901`

[5] Lo H 2001 *Arxiv preprint quant-ph/0102138*

[6] Kraus B, Gisin N and Renner R 2005 *Phys. Rev. Lett.* **95** 080501

[7] Gottesman D and Lo H 2003 *Information Theory, IEEE Transactions on* **49** 457–475 ISSN 0018-9448

[8] Christandl M, Renner R and Ekert A 2004 *Arxiv preprint quant-ph/0402131*

[9] Bruß D 1998 *Phys. Rev. Lett.* **81** 3018–3021

[10] Bennett C, Brassard G *et al.* 1984 *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing* vol 175 (Bangalore, India)