No-signaling quantum key distribution: solution by linear programming

Won-Young Hwang · Joonwoo Bae · Nathan Killoran

Received: 11 May 2013 / Accepted: 5 November 2014 / Published online: 2 December 2014
© Springer Science+Business Media New York 2014

Abstract We outline a straightforward approach for obtaining a secret key rate using only no-signaling constraints and linear programming. Assuming an individual attack, we consider all possible joint probabilities. Initially, we study only the case where Eve has binary outcomes, and we impose constraints due to the no-signaling principle and given measurement outcomes. Within the remaining space of joint probabilities, by using linear programming, we get bound on the probability of Eve correctly guessing Bob’s bit. We then make use of an inequality that relates this guessing probability to the mutual information between Bob and a more general Eve, who is not binary-restricted. Putting our computed bound together with the Csiszár–Körner formula, we obtain a positive key generation rate. The optimal value of this rate agrees with known results, but was calculated in a more straightforward way, offering the potential of generalization to different scenarios.
Keywords  No-signaling principle · Quantum key distribution · Linear programming

1 Introduction

A nonlocal realistic model, the de Broglie-Bohm theory, is not only consistent with quantum theory but also coherently describes measurement processes including wavefunction collapse [1]. This raises a question whether all realistic models must be nonlocal to be consistent with quantum theory, which led to the discovery of Bell’s inequality [2,3].

Recently, the nonlocality involved with Bell’s inequality and entanglement has entered a new phase of its development. It turned out that entanglement is a concrete physical resource for information processing [4]. In the same context, interestingly, it was found that with nonlocal correlations we can generate a cryptographic key, a private random shared sequence, whose security relies on only the no-signaling principle [5–7]. For this, no quantum theory is used for the security analysis. However, the only currently available way to realize nonlocal correlations is by using quantum entanglement. So these protocols are called no-signaling quantum key distribution (QKD). Remarkably, what is used to show security in no-signaling QKD is only the outcomes of measurements. As long as the outcomes satisfy a certain condition, security is provided, no matter how the outcomes are generated. Thus, no-signaling QKD has device-independent security. To satisfy the security condition, detector efficiency must be much higher than what is currently achievable. On the other hand, there is another main type of QKD’s [8–10] which does not rely on nonlocality for its security.

In Refs. [6,7], the security of no-signaling QKD against individual attacks has been analyzed in a novel way, exploiting the intrinsic structure of no-signaling probabilities [11,12]. In particular, by fixing the size of the input and output alphabets that are used to generate a secret key between the legitimate parties, a finite set of extremal points are distinguished. Information about the no-signaling polytope structure leads to huge simplifications in the security analysis. In Ref. [13], security against individual attacks was shown using the insight that no-signaling and nonlocal probabilities are generally monogamous. Indeed, a monogamy relation that is valid for no-signaling probabilities is explicitly employed to show the security. This approach can be applied even if the eavesdropper’s alphabet is not binary [13,14].

In this paper, we present a security analysis of no-signaling QKD protocols by numerically optimizing no-signaling probabilities. This explicitly shows that direct optimization over no-signaling probabilities can be used as the main theoretical tool to prove security. Specifically, we consider a protocol proposed by Acin, Massar, Pironio (AMP) [7,15] as a simple example. To motivate the advantage of our approach, we note that the method in Refs. [6,7] relies on the specific structure of certain no-signaling polytopes shown in Refs. [11,12]. However, it seems that the generalization to larger alphabets or higher dimensions is much harder to analyze; see for instance Ref. [16]. Nevertheless, since our approach relies only on basic mathematical tools, we expect that in principle it can also be applicable to other cases (though the computational load may become heavier).

This paper is organized as follows. First, we consider Eve’s (an eavesdropper’s) guessing probability about Bob’s (a receiver’s) bit. That is, we consider the case that
Eve’s outcomes are binary. Within the remaining space of joint probabilities, we maximize \( P_E \), the probability that Eve correctly guesses Bob’s bit, by linear programming. Then, we derive a bound on the mutual information between Bob and a general Eve (whose number of outcomes is now unrestricted), \( I_{BE} \). A key generation rate \( K \) is obtained by using the Csiszár–Körner formula [17]. In our case, \( K = I_{AB} - I_{BE} \), where \( I_{AB} \) is the mutual information between Alice (a sender) and Bob.

2 Main contents

2.1 AMP protocol

Two users, Alice and Bob, attempt to distribute a Bell state, \( |\phi^+\rangle = (1/\sqrt{2})(|0\rangle_A|0\rangle_B + |1\rangle_A|1\rangle_B) \), where \( A \) and \( B \) denote Alice and Bob, respectively, and \( |0\rangle \) and \( |1\rangle \) compose an orthonormal basis of a quantum bit (qubit). To mimic a realistic case with channel noise, we assume the Bell state was transformed to a Werner state

\[
\rho = p|\phi^+\rangle\langle\phi^+| + (1 - p)\frac{I}{4},
\]

where \( 0 \leq p \leq 1 \). (If the maximally entangled state, or the Bell state, is based on bosonic codes like coherent states or photons then noise may be due to attenuation also, and if atomic or other maximally entangled states are considered then bit flip noise may take place.) Although we use the Werner state to model potential data, our method does not rely on this. The assumption that the state is the Werner state is not necessary for security. As explained above, security is provided as long as the outcomes satisfy a certain condition, no matter how the outcomes are generated. For each copy of the distributed state, Alice chooses the value of an index \( x \) among 0, 1, and 2 with probabilities \( q \), \((1 - q)/2\), and \((1 - q)/2\), respectively. Then, she performs a measurement \( M_x \) on her qubit. \( M_0 \) is a measurement composed of two projectors \(|+\rangle\langle+| \) and \(|-\rangle\langle-| \) where \(|\pm\rangle = (1/\sqrt{2})(|0\rangle \pm |1\rangle)\). \( M_1 \) is measurement composed of \(|\pi/4\rangle\langle\pi/4| \) and \(|5\pi/4\rangle\langle5\pi/4| \) and \( M_2 \) is a one composed of \(|-\pi/4\rangle\langle-\pi/4| \) and \(|-5\pi/4\rangle\langle-5\pi/4| \). Here, \(|\phi\rangle = (1/\sqrt{2})(|0\rangle + e^{i\phi}|1\rangle)\) is a state obtained by rotating counterclockwise the state \(|+\rangle \) around the \( z \)-axis by an angle \( \phi \). Here, in the case of polarization, \( M_0 \) is polarization measurement in an axis and \( M_1 \) and \( M_2 \) are those in an axis which is counterclockwise rotated one from the original axis by an angle \( \pi/8 \) and \(-\pi/8 \), respectively. Bob also chooses a value of his index \( y \) for each copy, either 0 or 1, with probabilities \( q' \) and \( 1 - q' \), respectively. Then, he performs a measurement \( N_y \) on his qubit. Here, \( N_0 = M_0 \) and \( N_1 \) is a measurement composed of \(|\pi/2\rangle\langle\pi/2| \) and \(|3\pi/2\rangle\langle3\pi/2| \). The measurements can be physically realized by polarization measurement of photons. The Werner state can be prepared in photonic systems via a down-conversion process.

Next, both Alice and Bob publicly announce their values \( x \) and \( y \) for each copy. Measurement outcomes in the case \( x = y = 0 \) are kept and used to generate the key. Outcomes from other cases are publicly announced to estimate Eve’s information. Alice and Bob choose \( q \) and \( q' \) close to 1 so that almost events are in the case \( x = y = 0 \). This does not affect the security in the asymptotic case we consider.
2.2 Constraints on the probability distributions

We assume an individual attack in which Eve follows the same procedure for each instance. For each choice of measurements $x$ and $y$ by Alice and Bob, there is a joint probability for measurement outcomes $a, b, e$ for Alice, Bob, and Eve, respectively. The joint probability for $a, b, e$, conditioned on measurements $x$ and $y$ is denoted by $P(a, b, e|x, y)$. Here, $a$ and $b$ are binary variables according to the protocol. The number of Eve’s outcomes $e$ should be arbitrary in principle. However, for now, we consider the case that Eve’s outcome is binary. We do this because we are interested in the guessing probability, and Eve’s final guess has to be binary to match Bob’s alphabet.

Let us write constraints for the joint probabilities. First, they satisfy normalization

$$\sum_{a, b, e} P(a, b, e|x, y) = 1$$ (2)

for each $x, y$. Let us denote the marginal distribution for Alice and Bob, $\sum_e P(a, b, e|x, y)$, by $P(a, b, \triangle|x, y)$.

The marginal distributions corresponding to the state in Eq. (1) should be consistent with the measurement outcomes. For the measurement basis choice $(x = 0, y = 0)$, we have

$$P(0, 0, \triangle|0, 0) = P(1, 1, \triangle|0, 0) = \frac{p}{2} + \frac{1 - p}{4},$$

$$P(0, 1, \triangle|0, 0) = P(1, 0, \triangle|0, 0) = \frac{1 - p}{4}. (3)$$

For $(x = 0, y = 1)$, where there is no correlation,

$$P(a, b, \triangle|0, 1) = \frac{1}{4}$$ (4)

for each $a$ and $b$. For $(x = 1, y = 0)$, $(x = 1, y = 1)$, and $(x = 2, y = 0)$,

$$P(0, 0, \triangle|x, y) = P(1, 1, \triangle|x, y)$$

$$= 0.854 \frac{p}{2} + \frac{1 - p}{4} \equiv \alpha$$

$$P(0, 1, \triangle|x, y) = P(1, 0, \triangle|x, y)$$

$$= 0.146 \frac{p}{2} + \frac{1 - p}{4} \equiv \beta, (5)$$

where the two numerical values, 0.854 and 0.146, are obtained from measurement outcomes for the Bell state. For $(x = 2, y = 1)$,

$$P(0, 0, \triangle|2, 1) = P(1, 1, \triangle|2, 1) = \beta$$

$$P(0, 1, \triangle|2, 1) = P(1, 0, \triangle|2, 1) = \alpha. (6)$$
Now, we consider no-signaling conditions. Because the marginal distribution for Alice and Eve must be independent of Bob’s basis choice, we have

\[ P(a, \triangle, e|x, 0) = P(a, \triangle, e|x, 1) \]  

for each \( x \). Here, we use a notation for marginal distributions analogous to the previous one. Similarly,

\[ P(\triangle, b, e|0, y) = P(\triangle, b, e|1, y) = P(\triangle, b, e|2, y) \]

for each \( y \). Another no-signaling constraint is that Eve’s marginal distribution is independent of the basis choices of Alice and Bob,

\[ P(\triangle, \triangle, e|x, y) = P(\triangle, \triangle, e|0, 0) \]

for each \( x, y \).

2.3 Maximizing guessing probability \( P_E \)

Here, we maximize the guessing probability, \( P_E \), for a binary-restricted Eve within these constraints (2)–(9) by linear programming.

For visual convenience, \( P(a, b, e|x, y) \) are denoted as:

\[
\begin{align*}
P(a, b, e|0, 0) &= x_{abe}, & P(a, b, e|0, 1) &= y_{abe}, \\
P(a, b, e|1, 0) &= z_{abe}, & P(a, b, e|1, 1) &= u_{abe}, \\
P(a, b, e|2, 0) &= v_{abe}, & P(a, b, e|2, 1) &= w_{abe}.
\end{align*}
\]

(10)

We regard \( a_{be} \) as a binary number, for example, \( P(1, 0, 1|0, 0) = x_{101} = x_5 \).

Now, let us rewrite the constraints regarding measurement outcomes. For Eqs. (3) and (4), we have, respectively,

\[
\begin{align*}
x_0 + x_1 &= x_6 + x_7 = \frac{p}{2} + \frac{1-p}{4}, \\
x_2 + x_3 &= x_4 + x_5 = \frac{1-p}{4},
\end{align*}
\]

(11)

and

\[
\begin{align*}
y_0 + y_1 &= y_2 + y_3 = y_4 + y_5 = y_6 + y_7 = \frac{1}{4}.
\end{align*}
\]

(12)

For Eq. (5), we have

\[
\begin{align*}
A_0 + A_1 &= A_6 + A_7 = \alpha, \\
A_2 + A_3 &= A_4 + A_5 = \beta,
\end{align*}
\]

(13)
where $A = z, u, v$. For Eq. (6), we have

\[
\begin{align*}
w_0 + w_1 &= w_6 + w_7 = \beta \\
w_2 + w_3 &= w_4 + w_5 = \alpha.
\end{align*}
\]  

(14)

We can see that Eqs. (11)–(14) make the normalization in Eq. (2) satisfied. Thus, the normalization condition is redundant and can be removed.

The no-signaling condition in Eq. (7) can be expressed as

\[
\begin{align*}
x_i + x_{i+2} &= y_i + y_{i+2}, \\
z_i + z_{i+2} &= u_i + u_{i+2}, \\
v_i + v_{i+2} &= w_i + w_{i+2},
\end{align*}
\]

(15)

where $i = 0, 1, 4, 5$. We can see that, by Eqs. (11)–(14), the case when $i = 0, 4$ implies the case when $1, 5$, respectively. Thus, the latter cases can be removed. The no-signaling condition in Eq. (8) can be expressed as

\[
\begin{align*}
x_j + x_{j+4} &= z_j + y_{j+4}, \\
z_j + z_{j+4} &= v_j + v_{j+4}, \\
y_j + y_{j+4} &= u_j + u_{j+4}, \\
u_j + u_{j+4} &= w_j + w_{j+4},
\end{align*}
\]

(16)

where $j = 0, 1, 2, 3$. We can also see that, by Eqs. (11)–(14), the case when $j = 0, 2$ implies the case when $j = 1, 3$, respectively. Thus, the latter cases are redundant and can be removed. We can verify that Eqs. (A6) and (A7) [or equivalently, Eqs. (7) and (8)] lead to Eq. (9), which can thus be removed. As a result, we can remove all variables $B_i$ where $B = x, y, z, u, v, w$ and $i$ is an odd number.

Therefore, by non-negativity of each quantity, the space in which we optimize $I_{BE}(2)$ is as follows:

\[
\begin{align*}
0 &\leq x_k \leq \frac{p}{2} + \frac{1 - p}{4}, \quad 0 \leq x_l \leq \frac{1 - p}{4},
\end{align*}
\]

(17)

where $k = 0, 6$ and $l = 2, 4$,

\[
0 \leq y_j \leq \frac{1}{4},
\]

(18)

where $j = 0, 2, 4, 6$, and

\[
\begin{align*}
0 &\leq A_k \leq \alpha, \quad 0 \leq A_l \leq \beta, \\
0 &\leq w_k \leq \beta, \quad 0 \leq w_l \leq \alpha,
\end{align*}
\]

(19)

where $A = z, u, v$ and $k = 0, 6$ and $l = 2, 4$. The constraints are those that remain in Eqs. (15) and (16) after removing odd numbered variables.
Because the key is generated only from the results where \( x = y = 0 \), we need to consider the joint distribution \( P(\Delta, b, e|0, 0) \equiv R(b, e) \). Now, the guessing probability

\[
P_E = R(0, 0) + R(1, 1) = x_0 + x_4 + x_3 + x_7
= (x_0 + x_4) - (x_2 + x_6) + \frac{1}{2},
\]

where Eqs. (10) and (11) are used.

To maximize the guessing probability, we use linear programming [18]. First, we note that the constraints (17)–(19) define a convex set. We define \( C \in [0, \frac{1}{2}] \times [0, \frac{1}{2}] \) as the projection of this set onto the \((a, b)\)-plane where \( a \equiv x_0 + x_4 \) and \( b \equiv x_2 + x_6 \). We notice that \( C \) is convex and is symmetric under transformations \((a, b) \leftrightarrow (b, a)\) and \((a, b) \leftrightarrow (\frac{1}{2} - a, \frac{1}{2} - b)\). In our case, the linear function \( P_E \) can be directly optimized using linear programming. Specifically, for fixed value of the noise parameter \( p \), we perform the following optimization:

\[
P_E^{\text{max}} = \max_{(a, b) \in C} P_E(a, b) \quad \text{subject to} \quad P_E(a, b) \in C.
\]

2.4 Maximizing \( I_{BE} \)

Now, we obtain a bound on the mutual information, \( I_{BE} \), from the guessing probability \( P_E \). There is a simple relation for the problem [13]: Let us consider a marginal distribution for Bob and Eve, \( R(i, j) \). Here, Eve is not binary-restricted \((i = 0, 1 \text{ and } j = 0, 1, 2, \ldots)\). Consider conditional probabilities \( P(0|j) \) and \( P(1|j) \) due to the joint probability \( R(i, j) \). The joint probabilities can be written as \( R(i, j) = P(i|j)P(j) \), where \( P(j) = \sum_i R(i, j) \) is a marginal distribution for Eve. The mutual information is

\[
I_{BE} = H(i) - H(i|j)
= H(i) - \sum_j H[P(0|j)]P(j),
\]

where the binary entropy function \( H[q] \equiv -[q \log_2 q + (1 - q) \log_2 (1 - q)] \) has been introduced. Let \( P_E(j) \) be Eve’s probability to guess Bob’s outcome correctly, when her outcome is \( j \). However, we can observe that \( P_E(j) = \max\{P(0|j), P(1|j)\} \). Because \( H[P(0|j)] = H[P(1|j)] = H[P_E(j)] \) here, we have

\[
I_{BE} = H(i) - \sum_j H[P_E(j)]P(j),
\]

The (average) guessing probability is \( P_E = \sum_j P_E(j)P(j) \). However, for a fixed \( P_E \), the smallest value of the quantity \( \sum_j H[P_E(j)]P(j) \) is obtained when each \( P_E(j) \) take either 1/2 or 1, by the concavity of the binary entropy as discussed in
Fig. 1 Mutual informations depending on the noise parameter $p$. Positive key is possible in the region where $I_{BE}$ is smaller than $I_{AB}$ (dashed line).

Ref. [13]. For example, for $P_E = 0.8$ what minimizes $\sum_j H[P_E(j)]P(j)$ is that $R(0, 0) = 0.2, R(0, 1) = 0.15, R(1, 1) = 0.15, R(0, 2) = 0.15, R(1, 2) = 0.15,$ and $R(1, 3) = 0.2$. Here, $P_E(0) = P_E(3) = 1$ and $P_E(1) = P_E(2) = 0.5$. Now, let $r$ denote the sum of all $P(j)$ with $P_E(j) = 0.5$. In the example, the $r$ value is 0.6. Because $\sum_j H[P_E(j)]P(j) \geq r$ and $P_E = 1 - (r/2)$, we have

$$\sum_j H[P_E(j)]P(j) \geq r = 2(1 - P_E).$$

(24)

Now, we obtain

$$I_{BE} = H(i) - \sum_j H[P_E(j)]P(j) \leq 1 - 2(1 - P_E) = 2P_E - 1,$$

(25)

where the constraint $H(i) = 1$ is used. Therefore, we get

$$I_{BE} \leq 2P_E - 1.$$

(26)

Using the relation (26) and the maximal guessing probability obtained by linear programming, we can get a bound on $I_{BE}$ as shown in Fig. 1. Then, by the Csiszár–Körner formula [17], we can get a lower bound on the key generation rate $K = I_{AB} - I_{BE}$. As we can see, in the regime $p < \frac{1}{\sqrt{2}}$ where the Werner state admits a local realistic model, Eve has full information about Bob, namely $P_E = 1$, so there can be no secret key. However, in the regime where $\frac{1}{\sqrt{2}} \leq p \leq 1$, Eve’s information is restricted. When $p = 1, I_{BE} = 2 - \sqrt{2} \simeq 0.586$ and $I_{AB}$ is equal to 1, giving maximal $K = 0.414$. The region where we have nonzero $K$ is $0.9038 \leq p \leq 1$. The
key generation rate we obtained is the same as optimal rate found in Eq. (8) in Ref. [6]. A sudden change in the first derivative of the curve can be observed in Fig. 1. One may think this strange. However, the sudden change occurs at the point where the Werner state switches from separable to entangled. Were we to directly evaluate an entanglement measure on this state, we would see similar behavior when crossing the border of the set of separable states.

The relation (26) is only valid for the binary case. Thus, in the case when Alice and Bob’s information carriers are not binary, the relation will not apply. In such a situation, our general framework could still be used, but relation (26) would need to be generalized.

3 Conclusion

We outlined a straightforward approach for obtaining a secret key rate using only no-signaling constraints and linear programming. Assuming an individual attack, we considered all possible joint probabilities. We initially examined the case where Eve has binary outcomes. We imposed constraints due to the no-signaling principle and given measurement outcomes. Within the remaining space of joint probabilities, by using linear programming, we optimized the guessing probability between Bob and Eve. We then presented an inequality that relates the guessing probability to the mutual information between Bob and a general Eve who is not binary-restricted. Using the bound and the Csiszár–Körner formula [17], we lower bounded the final key generation rate. The optimal value of the key generation rate, obtained in the noiseless case $p = 1$, exactly matches the result from Ref. [6]. However, our approach does not require any specific knowledge of the no-signaling polytopes, instead relying on linear programming techniques to optimize the relevant quantities. Thus, our approach holds promise for application to other protocols, where the structure of the no-signaling polytopes cannot be determined analytically.

Acknowledgments This study was supported by Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education, Science and Technology (2010-0007208), and by National Research Foundation and Ministry of Education, Singapore, and the people programme (Marie Curie Actions) of the European Union’s Seventh Framework Programme (FP7/2007-2013) under REA grant agreement N.609305. NK acknowledges the Ontario Graduate Scholarship program for support.

References

1. Bohm, D., Hiley, B.: The Undivided Universe. Routledge, London (1993), introduced in Ref. [2]
2. Bell, J.S.: Speakable and Unspeakable in Quantum Mechanics. Cambridge University Press, Cambridge (1987)
3. Bell, J.S.: Physics 1, 195 (1964), reprinted in Ref. [2]
4. Nielsen, M.A., Chuang, I.L.: Quantum Computation and Quantum Information. Cambridge Univ. Press, Cambridge (2000)
5. Barrett, J., Hardy, L., Kent, A.: No signaling and quantum key distribution. Phys. Rev. Lett. 95, 010503 (2005)
6. Acín, A., Gisin, N., Masanes, L.: From Bell’s theorem to secure quantum key distribution. Phys. Rev. Lett. 97, 010503 (2006)
7. Acín, A., Massar, S., Pironio, S.: Efficient quantum key distribution secure against no-signalling eavesdroppers. New J. Phys. 8, 126 (2006)
8. Bennett, C.H., Brassard, G.: Proceedings of the IEEE International Conference on Computers, Systems, and Signal Processing, Bangalore, p. 175. IEEE, New York (1984)
9. Huttner, B., Imoto, N., Gisin, N., Mor, T.: Quantum cryptography with coherent states. Phys. Rev. A 51, 1863 (1995)
10. Mishra, M.K., et al.: Bipartite coherent-state quantum key distribution with strong reference pulse. Quantum Inf. Process. 12, 907 (2013)
11. Barrett, J., Linden, N., Massar, S., Pironio, S., Popescu, S., Roberts, D.: Nonlocal correlations as an information-theoretic resource. Phys. Rev. A 71, 022101 (2005)
12. Jones, N.S., Masanes, L.: Interconversion of nonlocal correlations. Phys. Rev. A 72, 052312 (2005)
13. Pawlowski, M.: Security proof for cryptographic protocols based only on the monogamy of Bell’s inequality violations. Phys. Rev. A 85, 046302 (2012)
14. Hwang, W.-Y., Gittsovich, O.: Security proof for cryptographic protocols based only on the monogamy of Bell’s inequality violations. Phys. Rev. A 85, 046301 (2012)
15. With respect to physical implementation, the protocol is almost the same as the Ekert protocol [16]. However, because security is analyzed with a different, though related, point of view, we give a new name
16. Pironio, S., Bancal, J.-D., Scarani, V.: Extremal correlations of the tripartite no-signaling polytope. J. Phys. A Math. Theor. 44, 065303 (2011)
17. Csiszár, I., Körner, J.: Broadcast channels with confidential messages. IEEE Trans. Inf. Theory 24, 339 (1978)
18. Gass, S.: Linear Programming: Methods And Applications. Dover Publications, Mineola (2010)