New Journal of Physics
The open access journal at the forefront of physics

Deutsche Physikalische Gesellschaft DPG
IOP Institute of Physics

Published in partnership with: Deutsche Physikalische Gesellschaft and the Institute of Physics

CrossMark

OPEN ACCESS

RECEIVED
20 June 2022

REVISED
4 November 2022

ACCEPTED FOR PUBLICATION
16 November 2022

PUBLISHED
28 November 2022

PAPER

Upper bound on device-independent quantum key distribution with two way classical postprocessing under individual attack

Yu-Zhe Zhang, Yi-Zheng Zhen and Feihu Xu*

Hefei National Laboratory for Physical Sciences at Microscale and School of Physical Sciences, University of Science and Technology of China, Hefei 230026, People's Republic of China

* Author to whom any correspondence should be addressed.

E-mail: feihuxu@ustc.edu.cn

Keywords: quantum information, device independent, quantum key distribution

Abstract

Device-independent quantum key distribution (DI-QKD) can guarantee the security even with untrusted devices. Unfortunately, conventional DI-QKD protocols can tolerate low noises only and require high detection efficiencies to achieve positive key rates. To improve the noise robustness, one promising solution is implementing the two-way classical postprocessing, which has the advantage of reducing the bit errors. In this paper, we study the DI-QKD with B-step two-way classical postprocessing under individual attacks. We adopt the tool of convex combination attack, i.e. an optimal individual attack, to upper bound the Devetak-Winter key rate. We show that, by using the B-step procedure, our protocol can tolerate detection efficiencies as low as 81.0% and depolarising noise of 0.799, which is better than the thresholds for the protocol with one-way error correction. This result can serve as the lower bounds on the critical noise and detection efficiency for the scenarios under general attacks. Our work justifies the advantage of two-way classical postprocessing for DI-QKD, thus offering a step towards its applications.

1. Introduction

Quantum key distribution (QKD) promise information-theoretical security for communication based on the laws of quantum physics [28]. Device-independent QKD (DI-QKD) [1, 10, 18], the security of which is based on the violation of a Bell inequality [8], allows the users to realize QKD even without the trust on the quantum devices. Device-independent security relies on the fact that more a quantum state is nonlocal, less an eavesdropper can correlated with the state. In DI-QKD, no assumptions on the dimensions of quantum systems or the internal working of the quantum devices are made. The security assumption only requires a trusted random number generator and two secure physical locations for Alice and Bob to guarantee that no unwanted information can leak to the outside [22].

Several theoretical efforts have advanced the developments of DI-QKD for different scenarios [3, 6, 13, 17, 22, 24–27, 29]. Benefited from the theoretical progresses in reducing the required efficiency and enhancing the tolerance on noise, three concurrent proof-of-concept DI-QKD experiments have been carried out, based on trapped ions [19], trapped atoms [30] and photonic setup [14], respectively. However, in practice, the realistic DI-QKD systems both suffer from the noise and require sufficiently large detection efficiency to achieve a positive key.

One possible solution to improve the noise robustness for experimental realisation is the two-way classical postprocessing [4, 12, 16]. In traditional QKD, the main advantage of the two-way classical postprocessing is reducing the bit error rates to a certain amount, e.g. less than a noise threshold, such that a secret key can be distilled asymptotically via a one-way classical postprocessing protocol. In the case of DI-QKD, the protocol with advantage distillation [26] has been shown to be particularly useful under the assumption of collective attacks.

In this paper, by using the convex combination (CC) attack [11] which is an optimal individual attack, we develop a technique for upper bounding the asymptotic Devetak-Winter key rate [9] of DI-QKD protocols with two-way classical postprocessing. Different from the advantage distillation [26], we consider the B-step protocol proposed in [12, 16], where Alice and Bob perform the xor operation locally on their two bits and then retain one bit or discard both dependent on the xor result. We use a local deterministic model to characterize the local and non-local part of correlations in the CC attack, which quantifies Eve's ability to learn the output of Alice measurement. Applying the B-step procedure, we show that our protocol can potentially decrease the required minimal detection efficiency and the maximal allowed depolarising noise. Particularly, the key rate upper bound is positive if the detection efficiency is larger than 81.0% or if the depolarising noise coefficient is larger than 0.799, which outperforms the standard one-way classical postprocessing protocol [22].

Notice that since the probability of the local correlation being shared in the CC attack can be maximized by using a linear programming, it can provide a direct method to upper-bound the key rates and predict the zero-key regions of DI-QKD [15]. Therefore, our analysis can serve as the lower bounds on the critical noise and detection efficiency when considering the DI-QKD with B-step protocol under the cases of collective or coherent attacks. We expect that the CC attack [11] can be an efficient tool to bound the secret key rate for general DI-QKD protocols.

2. Protocol description

Formally, in a general DI-QKD protocol, two parties, Alice and Bob, have access to a bipartite quantum state ρ_{AB}. The protocol consists of N rounds. In each round, Alice chooses a measurement labelled by $x \in \{1, 2\}$ and Bob chooses a measurement labelled by $y \in \{1, 2, 3\}$ to measure their own part of state ρ_{AB} respectively. Without loss of generality, we assume that each of Alice's (Bob's) measurements has 2 possible outcomes $a \in \{0, 1\}$ ($b \in \{0, 1\}$). Denoting the positive-operator-valued-measures associated with Alice's and Bob's measurements by $A_{a|x}$ and $B_{b|y}$. Then, the joint distribution of Alice's and Bob's outputs with respective to measurement settings can be described by:

$$P_{AB}(a, b|x, y) = \mathrm{Tr}\left[\rho_{AB}(A_{a|x} \otimes B_{b|y})\right]. \tag{1}$$

The protocol we consider here requests that Alice and Bob use a fraction of rounds corresponding to the measurement bases $(\bar{x}, \bar{y}) = (2, 3)$ as the key generation rounds and the rest as the test rounds to test the non-local correlation. We also focus on cases where the key-generating measurements have symmetrised outcomes, in the sense that $P_{AB}(0, 1|\bar{x}, \bar{y}) = P_{AB}(1, 0|\bar{x}, \bar{y}) = \xi/2$ and $P_{AB}(0, 0|\bar{x}, \bar{y}) = P_{AB}(1, 1|\bar{x}, \bar{y}) = (1-\xi)/2$ for some $\xi \leqslant 1/2$ (if $\xi \geqslant 1/2$, one can simply let Bob flip his bits). The symmetrised outcomes can always be achieved via a symmetrisation step, where Alice generates a uniformly random bit T in each round and publicly sends it to Bob, with both of them flipping their measurement outcome values if and only if $T = 1$.

Before distilling the key, our protocol will further introduce a B-step procedure [12, 16]. In the traditional QKD, the B step has been found useful in increasing the tolerance to the quantum bit errors. Here, we discuss the application of this method in DI-QKD. Alice and Bob first randomly permute all their raw keys $A_{\bar{x}}$ and $B_{\bar{y}}$. Then, Alice and Bob apply an XOR operation between two pair bits (a_1, b_1) and (a_2, b_2), and obtain the results $\mu_A = a_1 \oplus a_2$ and $\mu_B = b_1 \oplus b_2$. They compare the results μ_A, μ_B via two-way classical communication. If $\mu_A \neq \mu_B$, Alice and Bob discard the two pairs (a_1, b_1) and (a_2, b_2); otherwise, they keep one pair bits.

After the two-way classical postprocessing, Alice and Bob have reached an agreement on the rounds which are accepted to generate raw keys. They then follow the standard one-way error-correction and privacy amplification procedure, which allows one to employ the Deveteck-Winter rate [9] to generate secure keys.

In order to upper-bound the key rate, we apply the CC attack [11] to the DI-QKD protocols introduced above. In CC attack, Eve knows the form of the state ρ_{AB} and the measurements $\{A_{a|x}\}$, $\{B_{b|y}\}$, such that she can make use of these knowledge to distribute the quantum correlations to Alice and Bob in each round. In particular, Eve distributes local deterministic correlations $p^{L}_{AB}(a, b|x, y)$ with overall probability q^{L}, and she distributes a nonlocal quantum correlation $p^{NL}_{AB}(a, b|x, y)$ with probability $1 - q^{L}$. Eventually, the observed correlation of Alice and Bob takes the form:

$$P_{AB}(a, b|x, y) = q^{L} \cdot p^{L}_{AB}(a, b|x, y) + \left(1 - q^{L}\right) \cdot p^{NL}_{AB}(a, b|x, y). \tag{2}$$

Since Alice and Bob will announce their inputs (x, y) for every round, Eve knows the outcomes $e = (a, b)$ in all rounds in which she distributes a local correlation $p^{L}_{AB}(a, b|x, y)$. For the rounds where Eve distributes a nonlocal correlation, we suppose that Eve has no information about Alice's and Bob's outcomes, i.e. $e = ?$. Finally, Alice, Bob and Eve share a distribution which reads:

$$P_{ABE}(a, b, e|x, y) = q^L \cdot p^L_{AB}(a, b|x, y) \cdot \delta_{e,(a,b)} + \left(1 - q^L\right) \cdot p^{NL}_{AB}(a, b|x, y) \cdot \delta_{e,?}, \tag{3}$$

where δ is the Kronecker delta.

3. Local deterministic model of $P^L(a, b|x, y)$

In this subsection, we are going to find the maximum of q^L among all possible decompositions [5, 23] of the form equation (2). This quantity, denoted $q^L_{\max}$, defines the local content of the distribution $P(a, b|x, y)$. The local model $p^L_{AB}(a, b|x, y)$ is chosen as follows. Let $\lambda = (a_1, a_2; b_1, b_2, b_3)$ define an assignment: of outputs a_x and b_y for each of the inputs $x = 1, 2$ and $y = 1, 2, 3$. Let d_λ denote the corresponding deterministic behavior [7]:

$$d_\lambda(a, b|x, y) = \begin{cases} 1, \text{ if } a = a_x \text{ and } b = b_y, \\ 0, \text{ otherwise.} \end{cases} \tag{4}$$

There are 2^5 possible output assignments and therefore 2^5 such local deterministic behaviors. Then, a local behavior $p^L_{AB}(a, b|x, y)$ can be written as a CC of these deterministic points,

$$p^L_{AB}(a, b|x, y) = \sum_\lambda q_\lambda d_\lambda(a, b|x, y), \tag{5}$$

with $q_\lambda \geqslant 0$ and $\sum_\lambda q_\lambda = 1$. For the non-local model $p^{NL}_{AB}(a, b|x, y)$, we restrict it to be quantum [7, 20, 21],

$$p^{NL}_{AB}(a, b|x, y) \in \mathcal{Q}. \tag{6}$$

To find the maximal $q^L_{\max}$, let us define probabilities $\widetilde{p}^L_{AB}(a, b|x, y) = q^L \times p^L_{AB}(a, b|x, y)$, $\widetilde{p}^{NL}_{AB}(a, b|x, y) = (1 - q^L) \times p^L_{AB}(a, b|x, y)$ and $\widetilde{q}_\lambda = q^L q_\lambda$. It can be verified that:

$$q^L = \sum_{a,b} \widetilde{p}^L_{AB}(a, b|x, y) = \sum_\lambda \widetilde{q}_\lambda \quad \text{for any } x, y. \tag{7}$$

Therefore, the linear program reads:

$$\begin{aligned} \max_{\widetilde{q}_\lambda, \widetilde{p}^{NL}_{AB}} \quad & \sum_{a,b} \widetilde{p}^L_{AB}(a, b|\bar{x}, \bar{y}) \\ s.t. \quad & \widetilde{p}^L_{AB}(a, b|x, y) + \widetilde{p}^{NL}_{AB}(a, b|x, y) = P_{AB}(a, b|x, y) \\ & \widetilde{p}^{NL}_{AB}(a, b|x, y) \in \mathcal{Q}. \end{aligned} \tag{8}$$

Using the Navascués-Pironio-Acín (NPA) hierarchy [7, 20, 21], we can obtain the local content of $P_{AB}(a, b|x, y)$ in a device-independent way. We denote the k_{th} level by $\mathcal{Q}_k$. Since the NPA hierarchy forms a sequence of outer approximations to the set of quantum correlations, $\mathcal{Q} \subseteq \mathcal{Q}_1 \subseteq \cdots \subseteq \mathcal{Q}_k$, the relaxed local part provides a upper bound on the true local part, i.e, $q^L_{\max} \leqslant q^L_{\max}(k)$.

As a quick example, we consider the local content $q^L_{\max}$ for different detection efficiency $\eta \in [0, 1]$ of the following case: the source generates a maximally entangled state $|\psi_{AB}\rangle = (|00\rangle + |11\rangle)/\sqrt{2}$ and the measurements are $A_1 = (\sigma_z + \sigma_x)/\sqrt{2}$, $A_2 = B_3 = (\sigma_z - \sigma_x)/\sqrt{2}$, $B_1 = \sigma_z$ and $B_2 = \sigma_x$, such that the CHSH inequality is maximally violated. Note that for a loophole-free Bell test with inefficient detectors, one has to take into account all measurement outcomes produced by the devices to close the detection loopholes. A simple strategy is that Alice and Bob view their no-detection outcomes as a '1' outcome [1, 22]. The result is shown in figure 1. Numerical bounds are computed at a NPA relaxation level $k = 2, 3$. It could be seen that, taking $k = 2$ is enough to tightly bound the quantum set [2, 20, 21]. When the detection efficiency is less than 0.828, the local content $q^L_{\max}$ is equal to 1, which means that the correlation $P_{AB}(a, b|x, y)$ between Alice and Bob is local such that Eve will learn all the information about the outcomes of Alice and Bob.

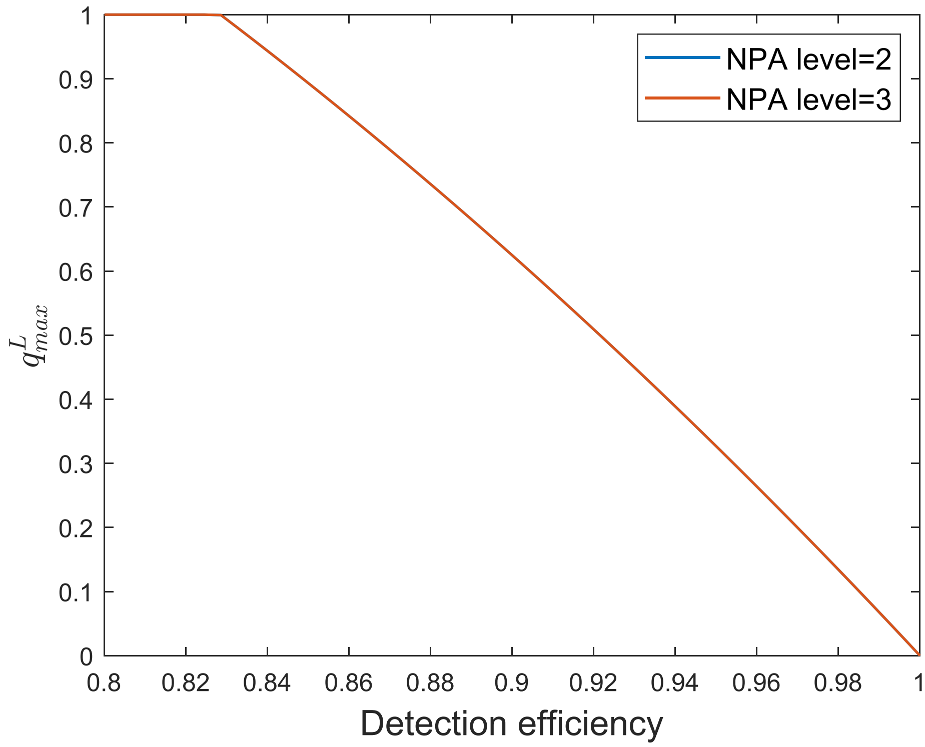

Figure 1. The local content q^L_{max} as a function of detection efficiency. The quantum correlation is given by a maximally entangled state and by qubit measurements that give the maximal violation of the CHSH inequality. When $\eta < 0.828$, $q^L_{\max} = 1$. Numerical bounds are computed at a NPA relaxation level $k = 2, 3$.

4. Key rate based on B-step

Let us note first that within the CC attack, in the non-local rounds which happen with probability $q^{NL}_{\min} = 1 - q^L_{\max}$, Eve distributes a non-local correlation with entries p^{NL}_{ab}, shared by Alice and Bob. In contrast, whenever she distributes a local correlation with probability equal to the local weight q^L, she perfectly knows the outcome of Alice and Bob. Hence, denoting by p^L_{ab} the resulting correlation within the local rounds, the overall tripartite correlation (in the key generation rounds) reads:

$$P_{ABE}(a,b,e|\bar{x},\bar{y}) = q^L_{\max} \cdot \begin{pmatrix} p^L_{00}\delta_{e,00} & p^L_{01}\delta_{e,01} \\ p^L_{10}\delta_{e,10} & p^L_{11}\delta_{e,11} \end{pmatrix} + q^{NL}_{\min} \cdot \begin{pmatrix} p^{NL}_{00} & p^{NL}_{01} \\ p^{NL}_{10} & p^{NL}_{11} \end{pmatrix} \delta_{e,?}, \tag{9}$$

where the random variable of Eve, e, consists of two bits (one for Alice and one for Bob) and an extra outcome '?' represents her lack of knowledge.

Now, we consider the above correlation after the B-step procedure. Let (a_s, b_s) denote outcomes of the survived round and (a_d, b_d) denote outcomes of the discarded round. It is obvious that if both of the two selected rounds come from the local part, Eve will learn all the information about the survived round. If the survived round is from the nonlocal part while the discarded part from the local part, or vice versa, Eve will learn that $e = a_d$ and $a_s = \mu \oplus e$ such that all the information about the survived round will be leaked. Therefore, the only secure situation is that both of the two selected rounds come from the non-local part. This makes Eve has no information about the survived round, i.e. $a_s = \mu \oplus ? = ?$. Denote the case where the two selected rounds are form the non-local part as '??'. Then, the correlation after the B-step procedure conditioned on a non-local correlation, i.e. $P_{AB}(a, b|E = ??, x, y)$ (un-normalized), can be written as:

$$\frac{(1-q^L_{max})^2}{2} \cdot \begin{pmatrix} p^{NL}_{00} \cdot (1-\xi^{NL}) & p^{NL}_{01} \cdot \xi^{NL} \\ p^{NL}_{10} \cdot \xi^{NL} & p^{NL}_{11} \cdot (1-\xi^{NL}) \end{pmatrix}. \tag{10}$$

Here, ξ^{NL} is the QBER for the non-local part and $\xi^{NL} = p^{NL}_{01} + p^{NL}_{10}$.

Tracing out Bob, we then obtain the desired marginal distribution $P_{AE}(a|E = ??, x, y)$ (un-normalized) shared by Alice and Eve after the B-step:

$$\frac{(1-q^L_{max})^2}{2} \cdot \begin{pmatrix} p^{NL}_{00} \cdot (1-\xi^{NL}) + p^{NL}_{01} \cdot \xi^{NL} \\ p^{NL}_{10} \cdot \xi^{NL} + p^{NL}_{11} \cdot (1-\xi^{NL}) \end{pmatrix}. \tag{11}$$

Hence, the desired entropy of Alice's outcomes conditioned on Eve, $H(A|E=??,\text{accept})$, is fully defined only by the case when Eve distributes a non-local correlation, and reads:

$$\frac{(1-q^L_{\max})^2}{2}\cdot\left[(1-\xi^{NL})^2+\xi^{NL^2}\right]\cdot h\left(\frac{p^{NL}_{00}\cdot(1-\xi^{NL})+p^{NL}_{01}\cdot\xi^{NL}}{(1-\xi^{NL})^2+\xi^{NL^2}}\right). \tag{12}$$

Thus, the final bound on the Devetak-Winter key rate [9] is given by:

$$r\leqslant H(A|E=??,\text{accept})-H(A|B,\text{accept}), \tag{13}$$

where $H(A|B,\text{accept})$ is the cost of one-way error correction, and can be written as:

$$\frac{1}{2}\left[(1-\xi)^2+\xi^2\right]h\left(\frac{\xi^2}{(1-\xi)^2+\xi^2}\right), \tag{14}$$

where the term $\frac{1}{2}[(1-\xi)^2+\xi^2]$ represents the fraction of rounds that are kept after post-selection.

The advantage by applying B-step is the quantum bit error rate ξ can be significantly reduced, and a net increase in the key generation may occur. As a comparison, for the protocol without B-step, the final bound on the key rate can be obtained directly form equation (9). By tracing out Bob in equation (9), the correlation shared between Alice and Eve can be represented by:

$$P_{AE}(a,e|\bar{x},\bar{y})=q^L_{\max}\cdot\begin{pmatrix}(p^L_{00}+p^L_{00})\delta_{e,0}\\(p^L_{10}+p^L_{11})\delta_{e,1}\end{pmatrix}+q^{NL}_{\min}\cdot\begin{pmatrix}p^{NL}_{00}+p^{NL}_{01}\\p^{NL}_{10}+p^{NL}_{11}\end{pmatrix}\delta_{e,?}, \tag{15}$$

such that the conditional entropy $H(A|E)$ is given by:

$$H(A|E)=q^{NL}_{\min}h\left(p^{NL}_{00}+p^{NL}_{01}\right), \tag{16}$$

and the final upper bounded key rate without B-step is:

$$r\leqslant q^{NL}_{\min}h\left(p^{NL}_{00}+p^{NL}_{01}\right)-h(\xi). \tag{17}$$

5. Simulation

In the simulation, we first focus on the threshold efficiency of the detection devices. We here consider the state is a non-maximally entangled state $|\psi(\theta)\rangle=\cos(\theta)|00\rangle+\sin(\theta)|11\rangle$, where $\theta\in[0,\pi/2]$. For simplicity, we restrict measurements to be projective within the x–z plane of the Bloch-sphere, i.e. measurements in the form of $\Pi(\phi)=\cos(\phi)\sigma_z+\sin(\phi)\sigma_x$, where $\phi\in[-\pi,\pi]$, and denote Alice and Bob's measurements by:

$$A_{0|x}=\frac{I+\Pi(\phi_x)}{2}\eta, A_{1|x}=\frac{I-\Pi(\phi_x)}{2}\eta+(1-\eta)\cdot I, \tag{18}$$

$$B_{0|y}=\frac{I+\Pi(\phi_y)}{2}\eta, B_{1|y}=\frac{I-\Pi(\phi_y)}{2}\eta+(1-\eta)\cdot I.$$

With the above notations, Alice and Bob's joint probability can be expressed as $P_{AB}(a,b|x,y)=\mathrm{Tr}[|\psi(\theta)\rangle\langle\psi(\theta)|(A_{a|x}\otimes B_{b|y})]$.

We numerically compare the protocol with and without the B-steps and the results are shown in figure 2. In the simulation, the key rate upper bounds are computed with NPA level 2. We find that when using the protocol with B-step, a positive key rate upper bound is obtained when the detection efficiency is larger than 81%. In contrast, without the B-step, the key rate upper bound is positive only if detection efficiency is larger than $\eta=90.7\%$.

We also consider a depolarising noise model for the noisy qubit state:

$$\rho_{AB}=V\cdot|\psi(\theta)\rangle\langle\psi(\theta)|+(1-V)\cdot\frac{I}{4}. \tag{19}$$

We find that the protocol with B-step could tolerate the depolarising noise of $V\geqslant 0.799$, while without B-step, the protocol only tolerates $V\geqslant 0.83$, as shown in figure 3.

In appendix, we consider another decomposition of the observed distribution $P_{AB}(a,b|x,y)$ where the nonlocal part $p^{NL}_{AB}(a,b|x,y)$ is chosen by varying $\eta\to 1$ and $V\to 1$. This decomposition means that if the

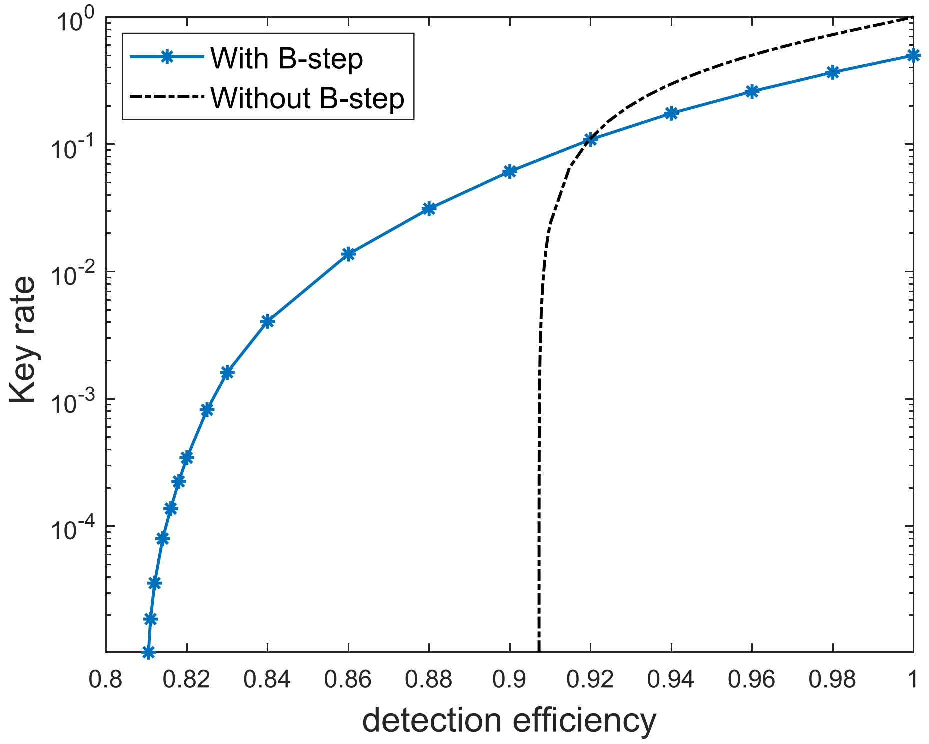

Figure 2. Upper bounded key rate as a function of detection efficiency, where the blue solid curve stand for the protocols with B-step and the black dashed curve is the protocol without B-step.

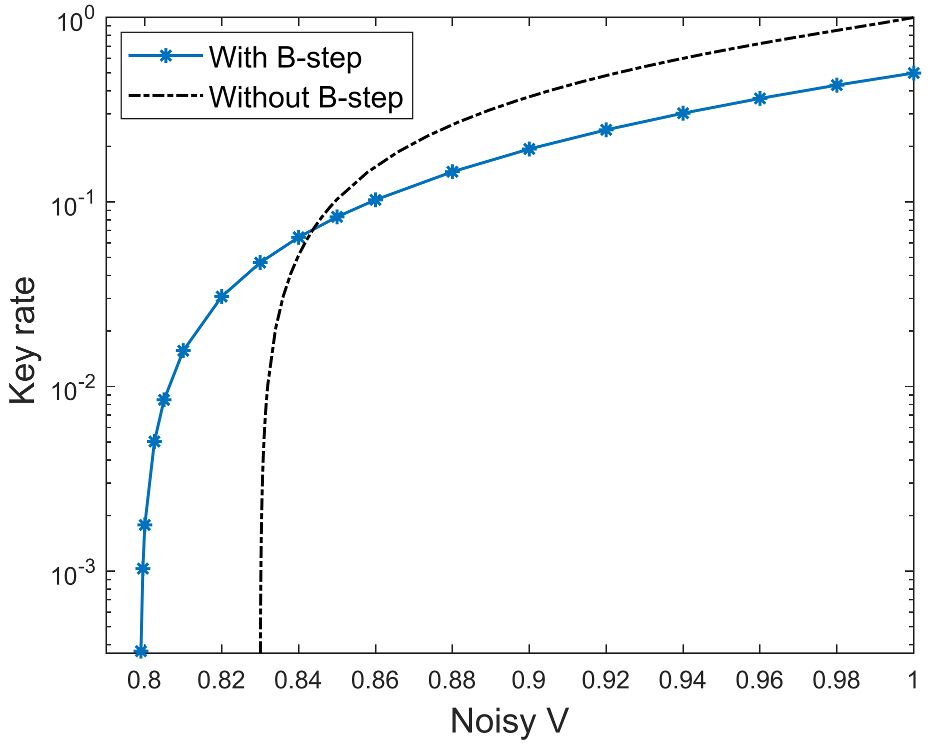

Figure 3. Upper bounded key rate as a function of the depolarising noisy V, where the blue solid curve and black dashed curve stand for protocols with or without B-step, respectively.

devices are noiseless, Eve will not learn any information of the outcomes. By using this kind of decomposition, we find that the critical detection efficiency in this case is around 68.3% (see appendix for details).

6. Conclusion and discussion

In this paper, we have upper bounded the DI-QKD with two-way communication. We select the B-step protocol where the survived events have lower errors compared with the standard protocol. Our security analysis uses the framework of CC attack where Eve randomly distributes a local or nonlocal correlation to Alice and Bob. By using an alternative decomposition of the observed quantum correlation, one could directly restrict the conditional entropy $H(A|E)$. Finally, a significant reduction of the threshold detection efficiency and depolarising noisy is achieved if we focus on the CC attack models, which implies the potential advantage of the B-step processing in DI-QKD. In general, one can apply the B-step procedure two or more times to obtain a better noise tolerance. Whether the advantage by applying more B steps such that the protocol tolerates the most noises remains to be explored. Moreover, as the B-step procedure costs half of the keys that Alice and Bob have had at hands, more B-step procedures will significantly lower the overall key rate. Finally, we remark that our techniques can be applied to other DI-QKD protocols, such as the protocols with noisy preprocessing [13] or random postselection [29], to find out the limited detection efficiency or depolarising noisy for positive keys.

Note that the CC attack belongs to the class of individual attacks, thus it permits an upper bound on the key rate of the protocol under general attacks [15]. To obtain a tight lower bound, one needs to consider the collective attacks [26] and the coherent attacks. Particularly, in the general non-i.i.d. attacks, namely the coherent attacks [3, 27], the raw keys, $r^n = r_1, r_2, \ldots, r_n$, is produced by an non-i.i.d. process. Then, each r_i may depend not only on i_{th} round of the protocol but also on everything that happened in previous rounds. For the protocol with two way communication [12, 16, 26], Alice and Bob have to randomly keep one of the selected two pairs of outcomes. Consequently, Eve might potentially learn more information of the survived rounds from the discarded ones. It is foreseen that the security analysis against coherent attacks is more challenging. Nonetheless, we recently noticed that there had been important theory developments towards this direction [31].

Note added. A recent work that uses the CC attack to bound general DI-QKD protocols by Karol Łukanowski *et al* will appear soon [15].

Data availability statement

All data that support the findings of this study are included within the article (and any supplementary files).

Acknowledgments

We thank Jan Kołodyński, Karol Łukanowski, and Máté Farkas for the motivation on the subject and the helpful discussions. This work was supported by National Natural Science Foundation of China (62031024, 12005091), National Key Research and Development Program of China (2020YFA0309700), and Shanghai Academic/Technology Research Leader (21XD1403800). F X acknowledges the support from the Tencent Foundation.

Appendix

In this section, we will consider a new decomposition of the observed distribution $P_{AB}(a,b|x,y)$ where the nonlocal part $p_{AB}^{NL}(a,b|x,y)$ is chosen by varying $\eta \to 1$ and $V \to 1$. To be specific, we denote Alice and Bob's measurements by:

$$\hat{A}_{0|x} = \frac{I + \Pi(\phi_x)}{2}, \hat{A}_{1|x} = \frac{I - \Pi(\phi_x)}{2} \tag{A.1}$$

$$\hat{B}_{0|y} = \frac{I + \Pi(\phi_y)}{2}, \hat{B}_{1|y} = \frac{I - \Pi(\phi_y)}{2}.$$

Then the nonlocal part is expressed as:

$$p_{AB}^{NL}(a,b|x,y) = \mathrm{Tr}[|\psi(\theta)\rangle\langle\psi(\theta)|(\hat{A}_{a|x} \otimes \hat{B}_{b|y})]. \tag{A.2}$$

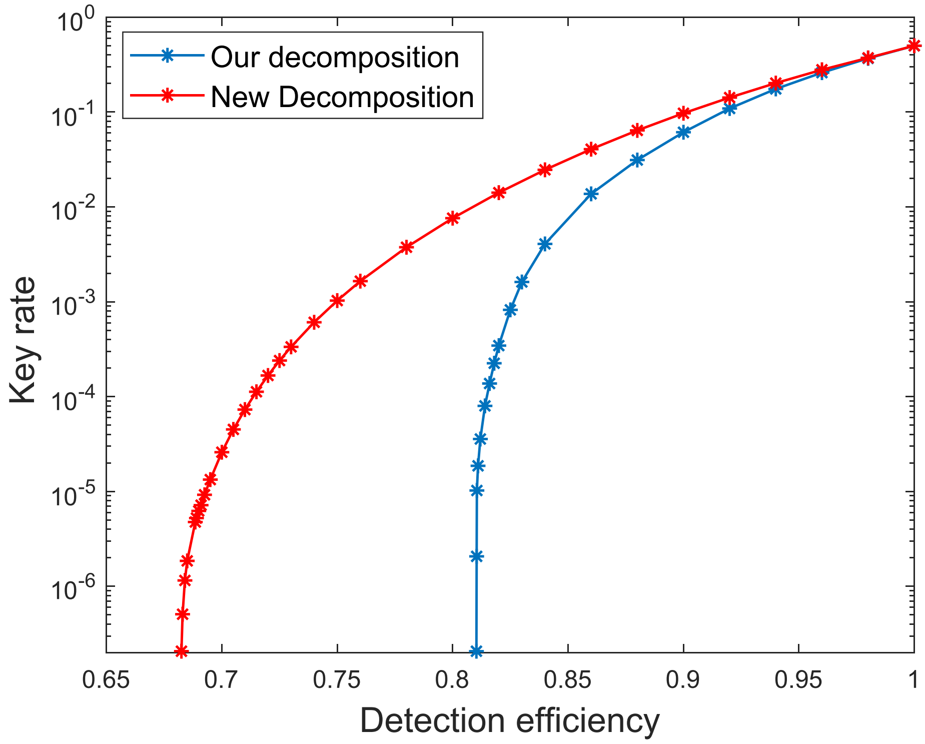

Figure A1. Upper bounded key rate as a function of detection efficiency η, where the blue solid curve stand for the decomposition used in the main text and the red solid curve is the protocol where the nonlocal part is chosen by varying $\eta \to 1$.

In order to find the maximal $q^L_{\max}$, we have the following linear program:

$$\max_{q_\lambda} \quad q \tag{A.3}$$

$$s.t. \quad q \cdot p^L_{AB} + (1-q) \cdot p^{NL}_{AB} = P_{AB}$$

$$p^L_{AB} = \sum_\lambda q_\lambda d_\lambda$$

$$0 \leqslant q_\lambda \leqslant 1, \sum_\lambda q_\lambda = 1,$$

where the first constraint is to enforce Eve to distribute on average the observed correlation $P_{AB}(a,b|x,y)$, while the other constraints ensure $\{q_\lambda\}$ to constitute a valid probability vector.

As figure A1 shows, by optimizing all the parameters, we find that this new decomposition provides a critical detection efficiency of 68.3%. In fact, this improvement comes from relaxing the ability of Eve. Noted that when considering the non-maximally entangled state $|\psi(\theta)\rangle = \cos(\theta)|00\rangle + \sin(\theta)|11\rangle$, it was proven the local content of the non-maximally entangled state is [5, 23]:

$$q^L_{max}(|\psi(\theta)\rangle) = 1 - \cos 2\theta. \tag{A.4}$$

Therefore, in this new decomposition, Eve could still use some local correction to simulate the nonlocal part $p^{NL}_{AB}(a,b|x,y)$.

ORCID iDs

Yu-Zhe Zhang https://orcid.org/0000-0003-1070-6560
Feihu Xu https://orcid.org/0000-0002-1643-225X

References

[1] Acín A, Brunner N, Gisin N, Massar S, Pironio S and Scarani V 2007 Device-independent security of quantum cryptography against collective attacks *Phys. Rev. Lett.* **98** 230501

[2] Acín A, Pironio S, Vértesi T and Wittek P 2016 Optimal randomness certification from one entangled bit *Phys. Rev.* A **93** 040102

[3] Arnon-Friedman R, Dupuis Fedéric, Fawzi O, Renner R and Vidick T 2018 Practical device-independent quantum cryptography via entropy accumulation *Nat. Commun.* **9** 459

[4] Bae J and Antonio A 2007 Key distillation from quantum channels using two-way communication protocols *Phys. Rev.* A **75** 012334

[5] Branciard C, Gisin N and Scarani V 2010 Local content of bipartite qubit correlations *Phys. Rev.* A **81** 022103

[6] Brown P, Fawzi H and Fawzi O 2021 Device-independent lower bounds on the conditional von Neumann entropy (arXiv:2106.13692)

[7] Brunner N, Cavalcanti D, Pironio S, Scarani V and Wehner S 2014 Bell nonlocality *Rev. Mod. Phys.* **86** 419–78

[8] Clauser J F, Horne M A, Shimony A and Holt R A 1969 Proposed experiment to test local hidden-variable theories *Phys. Rev. Lett.* **23** 880–4

[9] Devetak I and Winter A 2005 Distillation of secret key and entanglement from quantum states *Proc. R. Soc.* A **461** 207–35

[10] Ekert A K 1991 Quantum cryptography based on Bell's theorem *Phys. Rev. Lett.* **67** 661–3

[11] Farkas Mé, Balanzó-Juandó M, Łukanowski K, Kołodyński J and Acín A 2021 Bell nonlocality is not sufficient for the security of standard device-independent quantum key distribution protocols *Phys. Rev. Lett.* **127** 050503

[12] Gottesman D and Hoi-Kwong L 2003 Proof of security of quantum key distribution with two-way classical communications *IEEE Trans. Inf. Theory* **49** 457–75

[13] Ho M, Sekatski P, Ernest Y-Z Renner T, R, Bancal J-D and Sangouard N 2020 Noisy preprocessing facilitates a photonic realization of device-independent quantum key distribution *Phys. Rev. Lett.* **124** 230502

[14] Liu W-Z, Zhang Y-Z, Zhen Y-Z, Ming-Han Li, Liu Y, Fan J, Feihu X, Zhang Q and Pan J-W 2022 Toward a photonic demonstration of device-independent quantum key distribution *Phys. Rev. Lett.* **129** 050502

[15] Łukanowski K, Balanzó-Juandó M, Farkas Mé, Acín A, and Kołodyński J 2022 Upper bounds on key rates in device-independent quantum key distribution based on convex-combination attacks (arXiv:2206.06245)

[16] Ma X, Fung C H F, Dupuis Féric, Chen K, Tamaki K and Lo H-K 2006 Decoy-state quantum key distribution with two-way classical postprocessing *Phys. Rev.* A **74** 032330

[17] Masanes Lis, Pironio S and Acín A 2011 Secure device-independent quantum key distribution with causally independent measurement devices *Nat. Commun.* **2** 238

[18] Mayers D and Yao A 1998 Quantum cryptography with imperfect apparatus *Proc. 39th Annual Symp. Foundations of Computer Science* p 503

[19] Nadlinger D P *et al* 2022 Experimental quantum key distribution certified by Bell's theorem *Nature* **607** 682–6

[20] Navascués M, Pironio S and Antonio A 2007 Bounding the set of quantum correlations *Phys. Rev. Lett.* **98** 010401

[21] Navascués M, Pironio S and Acín A 2008 A convergent hierarchy of semidefinite programs characterizing the set of quantum correlations *New J. Phys.* **10** 073013

[22] Pironio S, Acín A, Brunner N, Gisin N, Massar S and Scarani V 2009 Device-independent quantum key distribution secure against collective attacks *New J. Phys.* **11** 045021

[23] Portmann S, Branciard C and Gisin N 2012 Local content of all pure two-qubit states *Phys. Rev.* A **86** 012104

[24] Reichardt B W, Unger F and Vazirani U 2013 Classical command of quantum systems *Nature* **496** 456–60

[25] Schwonnek Re, Goh K T, Primaatmaja I W, Tan E Y-Z, Wolf R, Scarani V and Lim C C-W 2021 Device-independent quantum key distribution with random key basis *Nat. Commun.* **12** 2880

[26] Tan E Y-Z, Lim C C-W and Renner R 2020 Advantage distillation for device-independent quantum key distribution *Phys. Rev. Lett.* **124** 020502

[27] Umesh V and Vidick T 2014 Fully device-independent quantum key distribution *Phys. Rev. Lett.* **113** 140501

[28] Xu F, Xiongfeng M, Zhang Q, Hoi-Kwong L and Pan J-W 2020 Secure quantum key distribution with realistic devices *Rev. Mod. Phys.* **92** 025002

[29] Xu F, Zhang Y-Z, Zhang Q and Pan J-W 2022 Device-independent quantum key distribution with random postselection *Phys. Rev. Lett.* **128** 110506

[30] Zhang W *et al* 2022 A device-independent quantum key distribution system for distant users *Nature* **607** 687–91

[31] Zhang X, Zeng P, Tian Y, Hoi-Kwong L and Xiongfeng M 2021 Quantum complementarity approach to device-independent security (arXiv:2111.13855)