Reply to "comment on 'Fully device-independent conference key agreement'"

Ribeiro, Jérémy; Murta, Gláucia; Wehner, Stephanie

DOI
10.1103/PhysRevA.100.026302

Publication date
2019

Document Version
Final published version

Published in
Physical Review A

Citation (APA)
Ribeiro, J., Murta, G., & Wehner, S. (2019). Reply to "comment on 'Fully device-independent conference key agreement'". *Physical Review A*, *100*(2), Article 026302. https://doi.org/10.1103/PhysRevA.100.026302

Reply to "Comment on 'Fully device-independent conference key agreement'"

Jérémy Ribeiro, Gláucia Murta,* and Stephanie Wehner
QuTech, Delft University of Technology, Lorentzweg 1, NL-2628 CJ Delft, Netherlands

(Received 3 July 2019; published 26 August 2019)

In this Reply we correct a mistake that we made in the correctness proofs of our protocol. Specifically, the Bell inequality we used ensures security but does not allow us to produce a key. In this Reply we explain and correct this mistake by adjusting the Bell inequality we used in the proof. Incidentally, this correction leads to slightly better asymptotic key rates. Importantly, *none* of the conclusions of the article are affected.

DOI: 10.1103/PhysRevA.100.026302

I. THE ISSUE

In this Reply, we address the concerns raised in the Comment [1] and correct the mistake in the proof of our protocol [2]. In our article we presented a protocol for device-independent conference key agreement (CKA) between N parties, Alice, Bob$_1, \ldots,$ Bob$_{N-1}$, using an N-partite Greenberger-Horne-Zeilinger (GHZ) state $[(|0\rangle^{\otimes N} + |1\rangle^{\otimes N})/\sqrt{2}]$. The protocol, aiming to be secure in the device-independent settings, relies on a statistical Bell test. In particular, in our article we presented the N-partite Mermin-Ardehali-Belinskii-Klyshko (MABK) inequality. However, using this inequality with the GHZ state leads to a protocol that is secure but does not produce a key. The intuition for that is the following.

(i) In order to ensure security, the protocol requires that the state and the measurement are such that they can achieve a sufficiently high violation of the MABK inequality. To do so using the GHZ state, Alice's observables A_0 and A_1 need to be in the XY plane of the Bloch sphere.

(ii) In order to generate a key that is correlated with those of the Bobs, Alice needs to have at least one of her observables (either A_0 or A_1) that is equal to the Pauli Z operator.

The two above conditions for A_0 and A_1 cannot simultaneously be true.

Moreover, even if there is no noise in the protocol, if Alice measures the GHZ state with a measurement in the XY plane, her outcomes will be completely uncorrelated with Bobs' outcomes. Therefore, no key can be produced, even though violation of the MABK inequality ensures that Alice's outcomes have high entropy conditioned on Eve. As a consequence, the protocol of the article will abort at almost every honest execution, and hence, no key is produced. Of course, one could consider measuring the GHZ state in a basis in between the Z basis and the XY plane. However, this would, at best, lead to a very low key rate, and it would, at worst, not be sufficient to get any key at all, causing the protocol to always abort.

The new inequality [the parity–Clauser-Horne-Shimony-Holt (CHSH) inequality] we introduce in the next section is such that a violation can be achieved by measuring in the Z basis, which ensures that entropy conditioned on Eve in Alice's measurement outcomes in the Z basis is high. Furthermore, when all the parties measure the GHZ state in the Z basis, they should get the same outcome (in the noiseless scenario), which allows for the production of a shared bit string (the key). If a small amount of noise is present, the errors it induces can be corrected by an error correction procedure, as already presented in the protocol in [2].

Remark 1. We point out that the lower bound we derived in [2] on the smoothed min-entropy as a function of the MABK violation is correct [see Eq. (5) of that article] and can therefore be considered a result of independent interest. It is, however, not sufficient to produce a secure key between Alice and the Bobs, as it says nothing about the correlations between Alice and the Bobs.

II. THE SOLUTION

To solve the problem, we choose to replace the MABK inequality by a new N-partite inequality, which we will call the parity-CHSH inequality and which is closely related to the well-known CHSH inequality. Note that the MABK we used in [2] is also closely related to the CHSH inequality but in a slightly different way.

The CHSH inequality can be formulated as a bound on the winning probability of the following bipartite game. Let Alice and Bob be the two players in this game, called the CHSH game. At the beginning of the game, they are both asked a uniformly random binary question, $x \in \{0, 1\}$ and $y \in \{0, 1\}$, respectively. They then have to answer bits a and b, respectively. They win the game if and only if

$$a + b = xy \bmod 2.$$

No communication is allowed between Alice and Bob during the game. They can, however, agree on any strategy before the start of the game. The CHSH inequality states that by using a classical strategy (a nonquantum strategy),[1] Alice and Bob's

*Present address: Institut für Theoretische Physik III, Heinrich-Heine-Universität Düsseldorf, Universitätsstraße 1, D-40225 Düsseldorf, Germany.

[1] Strategies that can be modeled with local hidden variables.

winning probability must satisfy the following:

$$P_{\text{win}}^{\text{CHSH}} \leqslant \frac{3}{4}. \tag{1}$$

Our new parity-CHSH inequality extends the CHSH inequality to N parties as follows. Let Alice, $\text{Bob}_1, \ldots, \text{Bob}_{N-1}$ be the N players of the following game (the parity-CHSH game). Alice and Bob_1 are asked uniformly random binary questions $x \in \{0, 1\}$ and $y \in \{0, 1\}$ respectively. The other Bobs are each asked a fixed question, e.g., always equal to 1. Alice will answer bit a, and $\forall\, i \in \{1, \ldots, N-1\}$, Bob_i answers bit b_i. We denote by $\bar{b} := \bigoplus_{2 \leqslant i \leqslant N-1} b_i$ the parity of all the answers of $\text{Bob}_2, \ldots, \text{Bob}_{N-1}$. The players win if and only if

$$a + b_1 = x(y + \bar{b}) \bmod 2.$$

As for the CHSH inequality, classical strategies for the parity-CHSH game must satisfy

$$P_{\text{win}}^{\text{Parity}-\text{CHSH}} \leqslant \frac{3}{4}. \tag{2}$$

Remark 2. Note that if we condition on $\bar{b} = 0$, the game is essentially the CHSH game. When conditioned on $\bar{b} = 1$, the parity-CHSH game reduces to a game equivalent to the CHSH up to relabeling the question y. We will use this to later prove that the function $\hat{f}$ defined in Eq. (3) lower bounds some entropy of interest.

Interestingly, for both the CHSH and parity-CHSH games, if the players use a quantum strategy, e.g., by sharing an entangled state before the beginning of the game and then measuring it, they can violate the above inequality, meaning that their winning probability can be higher than 3/4. In fact, quantum mechanics can lead to a winning probability up to $\approx$0.85 for both games. The GHZ state allows us to reach the maximum winning probability achievable by quantum mechanics for the parity-CHSH game. Importantly, this can be done with Alice's observables being $A_0 = Z$ and $A_1 = X$.

We can then use this new inequality to prove the security of our protocol. The only changes that need to be made in [2] is replacing the MABK inequality by the parity-CHSH and, accordingly, modifying the so-called min-tradeoff function [see Eq. (10)]. This corresponds to modifying step 2 in Sec. II of [2]. Let ${A'}_1^i$ be Alice's measurement outcomes, X_1^i and ${Y_{(1,\ldots,N-1)}}_1^i$ respectively encode the bases that Alice and the Bobs have used for their measurements until round i, T_1^i encodes which of the rounds in rounds 1 to i are test rounds, and E is a quantum resister held by Eve (see Protocol 1 of [2]). The min-tradeoff function is a function that lower bounds the von Neumann entropy $H := H({A'}_1^i | X_1^i {Y_{1,\ldots,N-1}}_1^i T_1^i {A'}_1^{i-1} E)$ as a function of the winning probability of the Bell game we consider, which in our case will be the parity-CHSH game. Then Eq. (10) of [2] has to be replaced by

$$\hat{f}(p_w) := \left(1 - \frac{\mu}{2}\right)\left\{1 - h\left[\frac{1}{2} + \frac{1}{2}\sqrt{(4p_w - 2)^2 - 1}\right]\right\}, \tag{3}$$

where p_w is shorthand notation for $P_{\text{win}}^{\text{Parity}-\text{CHSH}}$.

To see why $\hat{f}$ lower bounds H we follow the same reasoning as in [2], simply adapting the proof to the use of the parity-CHSH inequality [see the Appendix of [2] between Eqs. (A50) and (A60)].

We first notice that since $\Pr(X_i = 0) = (1 - \frac{\mu}{2})$,

$$\begin{aligned} H = &\left(1 - \frac{\mu}{2}\right) H\left(A'_i | X_1^{i-1} {Y_{(1,\ldots,N-1)}}_1^i {A'}_1^{i-1} T_1^i E, X_i = 0\right) \\ &+ \frac{\mu}{2} \underbrace{H\left(A'_i | X_1^{i-1} {Y_{(1,\ldots,N-1)}}_1^i {A'}_1^{i-1} T_1^i E, X_i = 1\right)}_{\geqslant 0} \\ \geqslant &\left(1 - \frac{\mu}{2}\right) H\left(A'_i | X_1^{i-1} {Y_{(1,\ldots,N-1)}}_1^i {A'}_1^{i-1} T_1^i E, X_i = 0\right). \end{aligned}$$

The above inequality holds since A'_i is a classical register. Conditioned on $X_i = 0$, A'_i is independent of ${Y_{(1,\ldots,N-1)}}_i$ and of T_i, and in the following, R denotes the registers $X_1^{i-1} {Y_{(1,\ldots,N-1)}}_1^{i-1} {A'}_1^{i-1} T_1^{i-1} E$ so that

$$H\left(A'_i | X_1^{i-1} {Y_{(1,\ldots,N-1)}}_1^i {A'}_1^{i-1} T_1^i E\, X_i = 0\right) = H(A'_i | R\, X_i = 0).$$

It remains to lower bound $H(A'_i | R, X_i = 0)$. We first lower bound it by

$$H(A'_i | R\, X_i = 0) \geqslant H(A'_i | R, X_i = 0, \bar{b}),$$

where $\bar{b}$ is the register that contains the parity bit of the outcome of $\text{Bob}_2, \ldots, \text{Bob}_{N-1}$. We can then expand the von Neumann entropy as

$$\begin{aligned} H(A'_i | R\, X_i = 0, \bar{b}) = &\; p_{\bar{b}=0} H(A'_i | R, X_i = 0, \bar{b} = 0) \\ &+ p_{\bar{b}=1} H(A'_i | R, X_i = 0, \bar{b} = 1). \end{aligned}$$

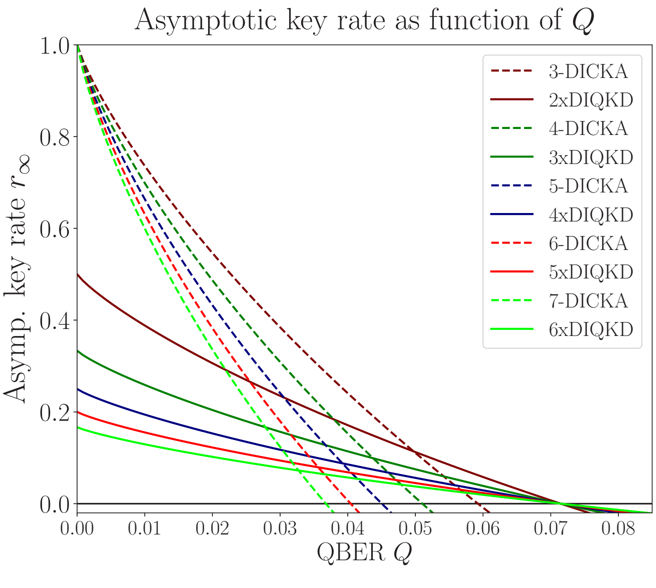

FIG. 1. Asymptotic key rate for N-DICKA (dashed lines) and for the distribution of a secret key between N parties through $(N-1)$-DIQKD protocols (solid lines), when each qubit experiences independent bit errors measured at a bit error rate (QBER) Q. For both types of protocols and from top to bottom, the lines correspond to the number of parties $N = \{3, 4, 5, 6, 7\}$. We observe that for the low-noise regime it is advantageous to use device-independent conference key agreement (DICKA) instead of $(N-1) \times$ DIQKD (DIQKD = device-independent quantum key distribution). In general, the comparison between the two methods depends on the cost and noisiness of producing GHZ states over pairwise Einstein-Podolsky-Rosen pairs.

From Ref. [3] we have that $(1-\frac{\mu}{2})H(A_i'|R,X_i=0,\bar{b}=0)\geqslant\hat{f}(p_{w|\bar{b}=0})$ and $(1-\frac{\mu}{2})H(A_i'|R,X_i=0,\,\bar{b}=1)\geqslant\hat{f}(p_{w|\bar{b}=1})$. Indeed, from Remark 2 we have that conditioned on $\bar{b}=0$, the parity-CHSH game is simply a CHSH game; therefore, $p_{w|\bar{b}=0}$ is equal to $P_{\rm win}^{\rm CHSH}$ when evaluated on the state shared between Alice and Bob$_1$ conditioned on $\bar{b}=0$. Moreover, Ref. [3] precisely lower bounds $(1-\frac{\mu}{2})H(A_i'|RX_i=0,\,\bar{b}=0)$ by $\hat{f}(P_{\rm win}^{\rm CHSH})$. The same reasoning holds for $\bar{b}=1$.

As a consequence,

$$\left(1-\frac{\mu}{2}\right)H(A_i'|RX_i=0,\,\bar{b}) \geqslant p_{\bar{b}=0}\hat{f}(p_{w|\bar{b}=0})+p_{\bar{b}=1}\hat{f}(p_{w|\bar{b}=1}).$$

By convexity of the function $\hat{f}$, we get

$$\left(1-\frac{\mu}{2}\right)H(A_i'|RX_i=0,\,\bar{b}) \geqslant \hat{f}(p_{\bar{b}=0}p_{w|\bar{b}=0}+p_{\bar{b}=1}\hat{p}_{w|\bar{b}=1})=\hat{f}(p_w),$$

and therefore, $H\geqslant\hat{f}(p_w)$. ■

III. HOW DOES THIS AFFECT OUR RESULTS?

The claims of our article [2] remain essentially unchanged.

(i) Our main theorem, Theorem 1, is still valid: One needs to use only the new expression for $\hat{f}$ given in Eq. (3) of this Reply.

(ii) The protocol is essentially unchanged. The only modifications we have to make are small adaptations regarding the use of the parity-CHSH inequality:

(a) Step 1(c) of Protocol 1 becomes “If $T_i=0$ Alice and the Bobs choose $(X_i,Y_{(1,\dots,N-1),i})=(0,2,0,\dots,0)$ and if $T_i=1$, Alice chooses $X_i\in_R\{0,1\}$ uniformly at random, Bob$_1$ chooses $Y_{(1),i}\in_R\{0,1\}$ uniformly at random, and Bob$_2,\dots,$ Bob$_{N-1}$ choose $(Y_{(2,\dots,N-1),i})=(1,\dots,1)$.”

(b) Step 4 of Protocol 1 becomes “If $T_i=1$, Alice uses A_i' and her guess on $B'_{(1,\dots,N-1),i}$ to set $C_i=1$ if they have won the N-partite parity-CHSH game and to set $C_i=0$ if they have lost it. If $T_i=0$, she sets $C_i=\perp$. She aborts if $\sum_i C_i<\delta\cdot\sum_i T_i$, where $\delta\in]p_{\rm min},p_{\rm max}[$.”

In particular we see from the first modification that using the parity-CHSH game, Bob$_1$ is now the only player who needs to use three settings for his measurement device: $Y_{(2),i}\in\{0,1,2\}$. All the other players need to use only two settings.

(iii) The asymptotic key rate is slightly improved compared to that in [2]. This is because the parity-CHSH inequality is somehow easier to violate than the MABK inequality. Figure 1 of [2] then has to be replaced by Fig. 1 of this Reply. The global behavior of the key rates remains the same. The asymptotic key rate as a function of the quantum bit error rate(QBER) is now given by

$$r_{N-\text{CKA},\infty}=1-h\left[\frac{1}{2}+\frac{1}{2}\sqrt{16\left(\frac{\sqrt{1-2Q}^{N}}{2\sqrt{2}}+\frac{(1-2Q)\left(1-\sqrt{1-2Q}^{N-2}\right)}{8\sqrt{2}}\right)^{2}-1}\right]-h(Q). \tag{4}$$

ACKNOWLEDGMENT

We would like to thank T. Holz, D. Miller, H. Kampermann, and Dr. Bruß, who pointed out this mistake.

[1] T. Holz, D. Miller, H. Kampermann, and D. Bruß, Comment on “Fully device-independent conference key agreement,” Phys. Rev. A **100**, 026301 (2019).

[2] J. Ribeiro, G. Murta, and S. Wehner, Fully device-independent conference key agreement, Phys. Rev. A **97**, 022307 (2018).

[3] A. Acín, N. Brunner, N. Gisin, S. Massar, S. Pironio, and V. Scarani, Device-Independent Security of Quantum Cryptography against Collective Attacks, Phys. Rev. Lett. **98**, 230501 (2007).