Erratum: Fundamental limitations on the device-independent quantum conference key agreement [Phys. Rev. A 105, 022604 (2022)]

Karol Horodecki, Marek Winczewski, and Siddhartha Das

(Received 12 January 2023; published 16 February 2023)

DOI: 10.1103/PhysRevA.107.029902

We recently learned that the bound presented in Sec. IV of our paper is redundant. This fact motivated us, apart from describing which parts should be disregarded (see below), to also revise some of the text. It is important to note that there is no change with respect to the results and proofs of the original version of our paper. We describe below essential changes.

We have learned that the two measures of multipartite entanglement–multipartite squashed entanglement $E_{\rm sq}$ and its dual $\tilde{E}_{\rm sq}$ in our paper are, in fact, equal to each other. The equality follows from Theorem 7 in Ref. [1]. Precisely the two definitions given in our paper below are equivalent [1].

Definition 4 [from Ref. [23] (of the original paper)]. "For an N-partite state $\rho_{A_1,\dots,A_N}$,

$$E^q_{\rm sq}\left(\rho_{A_1,\dots,A_N}\right) := \inf_{\sigma} I(A_1{:}A_2{:}\dots{:}A_N|E)_\sigma, \tag{20}$$

where the infimum is taken over states $\sigma_{A_1,\dots,A_N E}$ that are extensions of $\rho_{A_1,\dots,A_N}$, i.e., $\mathrm{Tr}_E[\sigma_{A_1,\dots,A_N E}] = \rho_{A_1,\dots,A_N}$."
and

Definition 7. "For an N-partite state $\rho_{A_1,\dots,A_N}$,

$$\widetilde{E}_{\rm sq}(\rho_{N(A)}) := \inf D_N(\sigma_{N(A)E}), \tag{49}$$

where the infimum is taken over states $\sigma_{N(A)E}$ that are extensions of $\rho_{N(A)}$, i.e., $\mathrm{Tr}_E[\sigma_{N(A)E}] = \rho_{N(A)}$."

Here,

$$I(A_1{:}\dots{:}{:}_N|E)_\rho = \sum_{i=1}^{N} S(A_i|E)_\rho - S(A_1,\dots,A_N|E)_\rho.$$

and

$$\begin{aligned} D_N(\rho_{N(A)E}) := {} & I(A_1{:}A_2\cdots A_N|E)_{\rho_{N(A)E}} + I(A_2{:}A_3\cdots A_N|A_1E)_{\rho_{N(A)E}} + I(A_3 : A_4\cdots A_N|A_1A_2E)_{\rho_{N(A)E}} \\ & + \cdots + I(A_{N-1}{:}A_N|A_1\cdots A_{N-2}E)_{\rho_{N(A)E}}. \end{aligned}$$

In turn, our upper bounds on the device-independent (DI) key based on the dual measure given in Theorem 5 and Corollary 3 in Sec. IV of the paper equals the multipartite reduced c-squashed entanglement bounds given in Theorems 2 and Corollary 2 in Sec. III of our paper, respectively. For this reason, any reference to the dual function, including these in the discussion section, should be skipped in reading. As a result, Fig. 2 also should not contain the plot of a dual bound, which appeared to be not equal to the c-squashed due to lack of optimization. Figure 2 should look like Fig. 2 here.

We have also noted typographical errors that could make unclear Eq. (68) and text around it. The new text reflects the numerics that was actually performed in our paper, hence, the modification presented below does not affect the plot given in Fig. 2 there. It was

$$\begin{aligned} \text{``}P^{\rm attack}_\nu(a,b_1,b_2,f|020) &= \Lambda_{E\to F}\, P^{\rm CC}_\nu(a,b_1,b_2,e|020) \\ &= (1-\nu)^3 P_{\rm GHZ}(a,b_1,b_2|x,y_1,y_2)\delta_{e,?} + [1-(1-\nu)^3]P^{\rm L}_\nu(a,b_1,b_2|x,y_1,y_2) \\ &\quad \times \delta_{e,(a,b_1,b_2)}[\delta_{a,b,c}\delta_{f,a} + (1-\delta_{a,b,c})\delta_{f,?}], \end{aligned} \tag{68}$$

where $\delta_{a,b,c}$ is 1 if all three indices have the same value and 0 otherwise. The above attack strategy is, therefore, a direct three-partite generalization of strategy proposed in Ref. [17]. The eavesdropper aims to be correlated only with the events $(a,b_1,b_2) = (0,0,0)$ or $(a,b_1,b_2) = (1,1,1)$, which mimic outputs of the honest strategy of the Greenberger- Horne-Zeilinger (GHZ) state. By applying the above attack strategy, we are ready to plot an upper bound on the reduced cc-squashed entanglement Corollary 2."

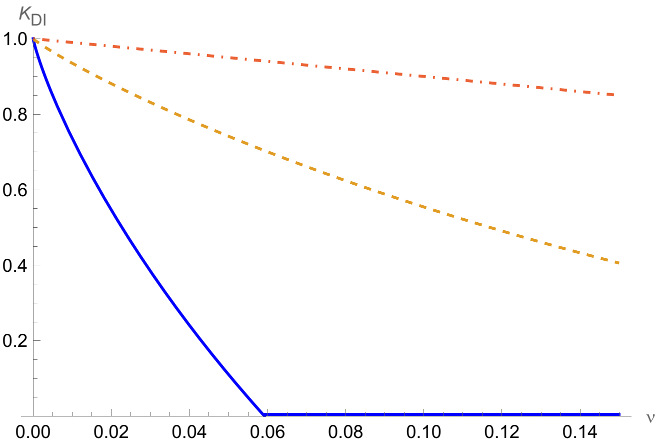

FIG. 2. Plot of upper and lower bounds on the device-independent conference key agreement (DI-CKA) of Ref. [2]. The yellow dashed line represents an upper bound (not fully optimized) on the upper bound $\frac{1}{N-1}I[N(A)\downarrow E]$ from Eq. (39) with the attack strategy in Eq. (68). The red dashed-dot curve is the trivial upper bound obtained in Corollary 5 via the relative entropy of entanglement bound $(1-\nu)$. The blue solid line represents the lower bound from Ref. [2].

It should be now as follows:

$$\text{“}P_\nu^{\text{attack}}(a,b_1,b_2,f|020)=\Lambda_{E\to F}\,P_\nu^{\text{CC}}(a,b_1,b_2,e|020)$$
$$=(1-\nu)^3P_{\text{GHZ}}(a,b_1,b_2|020)\delta_{f,?}+[1-(1-\nu)^3]P_\nu^{\text{L}}(a,b_1,b_2|020)\big[\delta_{a,b_1,b_2}\delta_{f,a}+\big(1-\delta_{a,b_1,b_2}\big)\delta_{f,?}\big], \tag{68}$$

where δ_{a,b_1,b_2} is 1 if all three indices have the same value and 0 otherwise. The above attack strategy is, therefore, a direct three-partite generalization of strategy proposed in Ref. [3]. The eavesdropper aims to be correlated only with the events $(a,b_1,b_2)=(0,0,0)$ or $(a,b_1,b_2)=(1,1,1)$, whenever they originate from the local behavior P_ν^{L}, and maps all other events to $f=?$. By applying the above attack strategy, we are ready to plot an upper bound on the reduced c-squashed entanglement shown in Corollary 2. The latter bound is a multipartite version of the intrinsic information [4,5], used first for the bipartite case in Ref. [6] against a nonsignaling adversary (see in this context Refs. [7–9]). Here, the strategy of Eve to process her classical variable E to F is based on Ref. [3] as shown above.”

Proposition 3 originally read as follows:

Proposition 3. “For any N-partite quantum behavior $(\rho_{N(A)},\mathcal{M})$ there is

$$K_{\text{DI,dev}}^{\text{iid}}(\rho_{N(A)},\mathcal{M})\leqslant\min\Big\{\min_{\mathcal{P}}K_{\text{DI,dev}}^{\text{iid}}(\rho_{\mathcal{P}(N(A))})\min_{\mathcal{P}}\inf_{(\sigma_{\mathcal{P}(N(A))},\mathcal{L})=(\rho_{\mathcal{P}(M(A))},\mathcal{M})}K_{DD}(\sigma_{\mathcal{P}(N(A))})\Big\}, \tag{72}$$

where $\mathcal{P}$ is any nontrivial partition of the set of systems $A_1,\dots,A_N$.”

It should now be as follows (sign × exhanged for the comma and without a bracket]):

Proposition 3. “For any N-partite quantum behavior $(\rho_{N(A)},\mathcal{M})$ there is

$$K_{\text{DI,dev}}^{\text{iid}}(\rho_{N(A)},\mathcal{M})\leqslant\min\Big\{\min_{\mathcal{P}}K_{\text{DI,dev}}^{\text{iid}}(\rho_{\mathcal{P}(N(A))}),\min_{\mathcal{P}}\inf_{\{\sigma_{\mathcal{P}(N(A))},\mathcal{L}\}=\{\rho_{\mathcal{P}(M(A))},\mathcal{M}\}}K_{DD}(\sigma_{\mathcal{P}(N(A))})\Big\}, \tag{72}$$

where $\mathcal{P}$ is any nontrivial partition of the set of systems $A_1,\dots,A_N$.”

The errors listed here, and corrected typographical errors, do not affect the results and proofs in our paper. An updated version has been made available [10].

S.D. acknowledges M. E. Shirokov for pointing out that the dual bound is redundant.

[1] N. Davis, M. E. Shirokov, and M. M. Wilde, Energy-constrained two-way assisted private and quantum capacities of quantum channels, Phys. Rev. A **97**, 062310 (2018).

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

[3] M. Farkas, M. Balanzó-Juandó, K. Łukanowski, J. Kołodyński, and A. Acín, Bell Nonlocality Is Not Sufficient for the Security of Standard Device-Independent Quantum Key Distribution Protocols, Phys. Rev. Lett. **127**, 050503 (2021).

[4] U. Maurer and S. Wolf, The intrinsic conditional mutual information and perfect secrecy, in *Proc. 1997 IEEE Symposium on Information Theory (Abstracts)* (1997), p. 88.

[5] U. Maurer and S. Wolf, Unconditionally secure key agreement and the intrinsic conditional information, IEEE Trans. Info. Theor. **45**, 499 (1999).

[6] A. Acín, S. Massar, and S. Pironio, Efficient quantum key distribution secure against no-signalling eavesdroppers, New J. Phys. **8**, 126 (2006).

[7] M. Winczewski, T. Das, and K. Horodecki, Limitations on a device-independent key secure against a nonsignaling adversary via squashed nonlocality, Phys. Rev. A **106**, 052612 (2022).

[8] E. Kaur, M. M. Wilde, and A. Winter, Fundamental limits on key rates in device-independent quantum key distribution, New J. Phys. **22**, 023039 (2020).

[9] A. Philip, E. Kaur, P. Bierhorst, and M. M. Wilde, Multipartite intrinsic non-locality and device-independent conference key agreement, Quantum **7**, 898 (2023).

[10] K. Horodecki, M. Winczewski, and S. Das, Fundamental limitations on the device-independent quantum conference key agreement, arXiv:2111.02467.