Reply to "Comment on 'Device-independent entanglement-based Bennett 1992 protocol' "

Giuseppe Vallone,[1,*] Giovanni Di Giuseppe,[2] Paolo Mataloni,[3] Paolo Villoresi,[1] and Marco Lucamarini[4,†]
[1]*Department of Information Engineering, University of Padova, I-35131 Padova, Italy*
[2]*Scuola di Scienze e Tecnologie, Divisione di Fisica, I-62032 Camerino (MC), Italy*
[3]*Dipartimento di Fisica, Università Sapienza di Roma, I-00185 Roma, Italy*
[4]*Toshiba Research Europe Ltd, 208 Cambridge Science Park, Cambridge CB4 0GZ, United Kingdom*
(Received 11 April 2016; published 27 June 2016)

Our paper [Phys. Rev. A **86**, 032325 (2012)], setting forth a previously unknown connection between the Bennett 1992 protocol and a Bell inequality, has recently received a Comment [Phys. Rev. A **93**, 066303 (2016)] about a possible flaw in its potential device-independent (DI) implementation. We point the authors of the Comment to prior works showing that what they assume to be specific to our protocol's DI implementation is actually a standard assumption in DI quantum key distribution. Therefore there is no need to revise any of the conclusions drawn in Lucamarini *et al.* [Phys. Rev. A **86**, 032325 (2012)].

DOI: 10.1103/PhysRevA.93.066304

In Ref. [1], we described a somewhat surprising connection between the long-standing prepare-and-measure (PM) Bennett 1992 (B92) protocol [2] for quantum key distribution (QKD) and the Clauser-Horne (CH) type of Bell inequality [3]. The main advantage of our result is that it allows for overcoming the PM nature of the B92, making it suitable for an entanglement-based implementation where the source of the entangled photons is owned by the adversary, Eve. Previous security proofs of the B92 [4,5] had to assume that the photons were prepared by a legitimate transmitter, Alice, making the protocol intrinsically PM. Our work removed this constraint, thus broadening the applicability of the B92. A proof-of-principle experiment of the protocol, called Lucamarini-Vallone-Gianani-Mataloni-Di Giuseppe (LVGMD), was in fact provided in Ref. [6].

The connection with the CH inequality allowed us to prove the security of the entanglement-based B92 protocol using the mathematical tools introduced in Ref. [7], which do not require a detailed characterization of the devices used in a QKD implementation. Here, it is worth noticing that "no detailed characterization of devices" is not equivalent to "no assumption is needed to prove the security of DI-QKD." There are still assumptions in DI-QKD [8–11]. Typically, no assumption is needed on the dimension of the Hilbert space of the quantum signals sent to the measuring devices or about the exact calibration of the measuring devices. The standard assumptions in DI-QKD can be read for instance in Ref. [11] and are the following:

(1) secure locations,
(2) trusted random number generators,
(3) trusted classical devices,
(4) authenticated classical channel between Alice and Bob,
(5) quantum physics is correct.

In some cases [12], the last assumption can be replaced by the no-signaling condition. Within the above-listed assumptions, the users can turn the quantum information into classical and process it without risk of being observed by Eve.

Assumption 1 corresponds to the fact that the legitimate users sit within secure perimeters that are not penetrable by the eavesdropper, i.e., no unwanted information can leak to the outside. Assumption 3 is related to the functioning of classical measuring devices used to store, process, and communicate the classical data (e.g., memories and computing devices) generated by their quantum apparatuses. If they were controlled by Eve, this would lead to a catastrophic violation of the quantum-enabled DI security [13] as also noted by the authors of Ref. [14].

Assumption 2 is a perhaps less widely known assumption in DI-QKD: The random number generators (RNGs) used by the legitimate parties, Alice and Bob, have to be within the above-mentioned secure perimeters, outside Eve's reach. They are assumed to work properly and generate a string of random numbers uniformly distributed. For a general DI-QKD protocol, this is clearly stated, e.g., in Ref. [15]. There it is shown that removing such an assumption from a DI protocol clearly affects its secure key rate: by using the words of Ref. [15] "the bad quality of randomness used there has a big impact on the security."

More specifically for our case, the same assumption is explicitly mentioned on p. 2, column 2, paragraph 1, line 7 of Ref. [7], which is the work employed in the security proof of Ref. [1]: "the inputs x and y are chosen uniformly at random" (x and y are the basis settings for Alice and Bob, respectively). Finally, the same assumption appears in the recently performed loophole-free Bell tests [16–18], which represent the prerequisite of any DI-QKD setup. In those experiments, great care was taken to guarantee that the RNGs were unbiased and independent of Eve's action [19].

After having clarified the above points, let us come to the criticism of our work contained in Ref. [14]. In our view, the Comment actually targets two works, i.e., Refs. [1,6] with the following two points:

(1) The RNG owned by Bob in the entanglement-based B92 [1] can be biased. This can affect the protocol's secure key rate, so the protocol is not DI.

(2) The experiment performed in Ref. [6] is not loophole free, so it does not represent a DI implementation of the protocol in Ref. [1].

From our preliminary clarifications, the inconsistency of the above criticism should be apparent. The comment in point (1) could be addressed against most of the existing DI-QKD

*vallone@dei.unipd.it
†marco.lucamarini@crl.toshiba.co.uk

protocol even those based on the BB84 protocol [20]. The possible bias of the RNG is not automatically included in any DI scenario, and a specific analysis is required to analyze this problem [15]. Point (2) is quite shallow. In science, it is perfectly legitimate and customary to perform proof-of-concept experiments under reasonable assumptions. In the case of Ref. [6], a proof-of-principle experiment as written in the title, the fair sampling assumption was enforced as in all the Bell inequality tests performed so far with the exception of the already cited works [16–18].

In conclusion, we argue that the argument contained in the Comment [14] is trivial since it is well known that for the DI-QKD protocol the quality of randomness in the basis choice has an effect on the security. Then, the Comment [14] does not invalidate our LVGMD protocol [1] since we assumed unbiased RNG as performed in most DI-QKD protocols. We agree that a loophole-free Bell violation must be obtained to guarantee the security of the key in the protocol introduced in Ref. [1], but this applies to any DI-QKD protocol: Indeed random basis choices are required to close the freedom-of-choice loophole in a Bell test.

A better result, not contained in Ref. [14], would be the quantitative estimation of the effect of the bias in the key security in the LVGMD protocol, similar to what was performed in Ref. [15] for the the DI-QKD protocol based on the Collins-Gisin-Linden- Massar-Popescu inequality [21] (a generalization of the well-known Clauser-Horne-Shimony-Holt inequality [22]). We leave this investigation for future research.

[1] M. Lucamarini, G. Vallone, I. Gianani, P. Mataloni, and G. Di Giuseppe, Phys. Rev. A **86**, 032325 (2012).

[2] C. H. Bennett, Phys. Rev. Lett. **68**, 3121 (1992).

[3] J. F. Clauser and M. A. Horne, Phys. Rev. D **10**, 526 (1974).

[4] K. Tamaki, M. Koashi, and N. Imoto, Phys. Rev. Lett. **90**, 167904 (2003).

[5] K. Tamaki and N. Lütkenhaus, Phys. Rev. A **69**, 032316 (2004).

[6] G. Vallone, A. Dall'Arche, M. Tomasin, and P. Villoresi, New J. Phys. **16**, 063064 (2014).

[7] Ll. Masanes, S. Pironio, and A. Acín, Nat. Commun. **2**, 238 (2011).

[8] A. Acín, N. Brunner, N. Gisin, S. Massar, S. Pironio, and V. Scarani, Phys. Rev. Lett. **98**, 230501 (2007).

[9] D. Mayers and A. Yao, Quantum Inform. Comput. **4**, 273 (2004).

[10] A. Acín, N. Gisin, and L. Masanes, Phys. Rev. Lett. **97**, 120405 (2006).

[11] S. Pironio, A. Acín, N. Brunner, N. Gisin, S. Massar, and V. Scarani, New J. Phys. **11**, 045021 (2009).

[12] J. Barrett, L. Hardy, and A. Kent, Phys. Rev. Lett. **95**, 010503 (2005).

[13] I. Gerhardt, Q. Liu, A. Lamas-Linares, J. Skaar, V. Scarani, V. Makarov, and C. Kurtsiefer, Phys. Rev. Lett. **107**, 170404 (2011).

[14] Y. Tan and Q. Cai, Phys. Rev. A **93**, 066303 (2016).

[15] M. Huber and M. Pawłowski, Phys. Rev. A **88**, 032309 (2013).

[16] B. Hensen *et al.*, Nature (London) **526**, 682 (2015).

[17] M. Giustina, M. A. M. Versteegh, S. Wengerowsky, J. Handsteiner, A. Hochrainer, K. Phelan, F. Steinlechner, J. Kofler, J.Å. Larsson, C. Abellán, W. Amaya, V. Pruneri, M. W. Mitchell, J. Beyer, T. Gerrits, A. E. Lita, L. K. Shalm, S. W. Nam, T. Scheidl, R. Ursin, B. Wittmann, and A. Zeilinger, Phys. Rev. Lett. **115**, 250401 (2015).

[18] K. Shalm *et al.*, Phys. Rev. Lett. **115**, 250402 (2015).

[19] C. Abellán, W. Amaya, D. Mitrani, V. Pruneri, and M. W. Mitchell, Phys. Rev. Lett. **115**, 250403 (2015).

[20] C. H. Bennett and G. Brassard, in *Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing* (IEEE, New York, 1984), p. 175.

[21] D. Collins, N. Gisin, N. Linden, S. Massar, and S. Popescu, Phys. Rev. Lett. **88**, 040404 (2002).

[22] J. F. Clauser, M. A. Horne, A. Shimony, and R. A. Holt, Phys. Rev. Lett. **23**, 880 (1969).