

This manuscript has been previously reviewed at another Nature Research journal. This document only contains reviewer comments and rebuttal letters for versions considered at Communications Physics.

REVIEWERS' COMMENTS:

Reviewer #1 (Remarks to the Author):

In this work, the authors devise a new device-independent randomness generation protocol based on the instrumental scenario, which is commonly studied in causal inference. The instrumental scenario has received some attention within the foundations of quantum theory community since it provides a simpler test of non-classicality than in a Bell test. However, unlike in a Bell test, this scenario allows for some communication between experimental operations: one party, Alice, makes a measurement, and the outcome directly determines another party's, Bob's, measurement choice. The idea that connects the two scenarios is that if statistics were compatible with a classical common cause explanation or classical instrumental explanation, then if an adversary had access to the latent variables of a device, then everything is perfectly predictable. If one shows incompatibility with these classical explanations then there are no latent variables describing the statistics in the first place.

I think this work merits publication and opens new and interesting avenues of research. For one thing, a lot of research in device-independent quantum information bases security on monogamy. The intuition being that if statistics are close to the maximal violation of some inequality then the underlying state is pure and thus uncorrelated from anything else. Such an intuition is reinforced by the fact that the operations in a Bell test are just local measurements on an entangled state. However, it's possible that this work highlights such intuition isn't necessary for a device-independent protocol. One just needs some notion of "statistical monogamy" that the observed correlations are near the extrema of the set of allowed correlations, thus prohibiting a large amount of correlation with an adversary. Furthermore the authors extend the recently-developed techniques of entropy accumulation in new directions, which is interesting in and of itself.

Overall I recommend publication of this work.

One thing I think the authors could highlight is that the causal assumptions that Alice's measurement doesn't directly affect B's system could be argued more practically. Let me expand on this. In normal device-independent quantum information, one can impose the condition that devices do not communicate by having space like separation, or more reasonably by putting shielding around the devices, and then possibly discarding the device. It's my feeling that the causal assumptions of the current work can be imposed by shielding Alice's device to prevent any unwanted communication from Alice's device to Bob's, and then the only influence is the direct influence of the outcome b to Bob's choice y . This seems as natural as the assumptions in vanilla device independence. Perhaps the authors could emphasise this point in their work?

Minor comment: the authors use "such X" when they should be using "such a X". For example, "such framework" should be "such a framework"

Editors Comment: we have further contacted the reviewer to explicitly comment on the remaining concerns of the original Reviewer #2 at Nature Communications and they confirmed that the issue with the NPA hierarchy has now been resolved.

Point-by-point response to the Reviewers

Reviewer #1 (Remarks to the Author):

“In this work, the authors devise a new device-independent randomness generation protocol based on the instrumental scenario, which is commonly studied in causal inference. The instrumental scenario has received some attention within the foundations of quantum theory community since it provides a simpler test of non-classicality than in a Bell test. However, unlike in a Bell test, this scenario allows for some communication between experimental operations: one party, Alice, makes a measurement, and the outcome directly determines another party’s, Bob’s, measurement choice. The idea that connects the two scenarios is that if statistics were compatible with a classical common cause explanation or classical instrumental explanation, then if an adversary had access to the latent variables of a device, then everything is perfectly predictable. If one shows incompatibility with these classical explanations, then there are no latent variables describing the statistics in the first place. I think this work merits publication and opens new and interesting avenues of research. For one thing, a lot of research in device-independent quantum information bases security on monogamy. The intuition being that if statistics are close to the maximal violation of some inequality then the underlying state is pure and thus uncorrelated from anything else. Such an intuition is reinforced by the fact that the operations in a Bell test are just local measurements on an entangled state. However, it’s possible that this work highlights such intuition isn’t necessary for a device-independent protocol. One just needs some notion of “statistical monogamy” that the observed correlations are near the extrema of the set of allowed correlations, thus prohibiting a large amount of correlation with an adversary. Furthermore the authors extend the recently-developed techniques of entropy accumulation in new directions, which is interesting in and of itself. Overall I recommend publication of this work.”

We thank the Reviewer for the positive assessment of our work and for recommending its publication on *Communications Physics*.

“One thing I think the authors could highlight is that the causal assumptions that Alice’s measurement doesn’t directly affect B’s system could be argued more practically. Let me expand on this. In normal device-independent quantum information, one can impose the condition that devices do not communicate by having space like separation, or more reasonably by putting shielding around the devices, and then possibly discarding the device. It’s my feeling that the causal assumptions of the current work can be imposed by shielding Alice’s device to prevent any unwanted communication from Alice’s device to Bob’s, and then the only influence is the direct influence of the outcome b to Bob’s choice y . This seems as natural as the assumptions in vanilla device independence. Perhaps the authors could emphasise this point in their work?”

In order to emphasise the point raised by the Reviewer, we added the following sentence in the *Introduction*:

“In practical applications, this premise can be enforced, by shielding A’s measurement station, in order to allow only for the communication of its outcome bit to B and prevent any other unwanted communication.”

“Minor comment: the authors use “such X” when they should be using “such a X”. For example, “such framework” should be “such a framework”

The reported typos were corrected.