Author Correction

Long-range QKD without trusted nodes is not possible with current technology (npj Quantum Information, (2022), 8, 1, (108), 10.1038/s41534-022-00613-4)

Huttner, Bruno; Alléaume, Romain; Diamanti, Eleni; Fröwis, Florian; Grangier, Philippe; Hübel, Hannes; Martin, Vicente; Slater, Joshua A.; Tittel, Wolfgang; More Authors

DOI
10.1038/s41534-022-00660-x

Publication date
2022

Document Version
Final published version

Published in
NPJ Quantum Information

AUTHOR CORRECTION OPEN

Check for updates

Author Correction: Long-range QKD without trusted nodes is not possible with current technology

Bruno Huttner, Romain Alléaume, Eleni Diamanti, Florian Fröwis, Philippe Grangier, Hannes Hübel, Vicente Martin, Andreas Poppe, Joshua A. Slater, Tim Spiller, Wolfgang Tittel, Benoit Tranier, Adrian Wonfor and Hugo Zbinden

npj Quantum Information (2022)8:143 ; https://doi.org/10.1038/s41534-022-00660-x

Correction to: *npj Quantum Information* https://doi.org/10.1038/s41534-022-00613-4, published online 9 September 2022

The original version of this Article contained errors in the Competing interests statement and Table 1 and incorrectly omitted the Acknowledgements section.

The original Competing interests statement reported no competing interests for the authors; this has been corrected to "B.H. and F.F. are employees of ID Quantique, Geneva and ID Quantique Europe, Vienna, respectively, which have competing interests with Arqit in developing quantum communication technologies. B.T. is an employee of Thales Alenia Space, a joint Venture which invests in satellite quantum communications. B.H. is the inventor of several patents, both pending and accepted, in the field of space QKD. The authors declare that there are no other competing interests".

The original Table 1 omitted the captions. Table 1 captions read:

The different steps of the protocol are described below, each item corresponding to the numbered row in the Table.

1. Alice prepares a series of quantum states, according to BB84 polarisation protocol. For each state, she chooses both the bit value and the corresponding basis. She sends the states to Bob over a quantum channel (arrow with diagonal stripes).
2. Many states are lost in the transmission. Bob tells Alice, which states have been lost (X in the table). He uses the classical discussion channel (white arrow). Alice and Bob discard all the corresponding states. The resulting series of bits is the raw key.
3. Alice tells Bob, over the classical discussion channel, which bases she used. Bob notes the cases when he and Alice used different bases (X in the table), but does not tell Alice. The remaining bits represent the sifted key for Bob. Alice cannot know, which of the states were received by Bob in the correct basis.
4. to 6. Alice and Carol follow the same protocol with a new series of states.
7. Alice performs an XOR of the two raw keys she exchanged with Bob and with Carol and sends the result to Carol, over the classical discussion channel.
8. Bob sends directly to Carol, which bits he received in the wrong basis and should not be used (X in the table). He uses a confidential classical channel, "which cannot be eavesdropped by Alice" (black arrow).
9. Carol notes the wrong bits in the XORed key.
10. Carol makes an XOR of the two sifted keys, and sends to Bob, which bits should not be used (X in the table). She also uses the same confidential classical channel, "which cannot be eavesdropped by Alice".
11. Bob and Carol now share a common sifted key, unknown to Alice. They can process it in the standard way (error estimation, error correction, privacy amplification) to finally get a shared secret key. The main hypothesis of the protocol is that Bob and Carol share a confidential classical channel, which cannot be eavesdropped by Alice.

The correct Acknowledgements read: B.H., R.A., E.D., F.F., P.G., H.H., V.M., A.P., J.A.S., A.W. and H.Z. acknowledge support from the H2020-funded research project OPENQKD, Grant agreement contract number 857156, https://openqkd.eu/.

This has now been corrected in both the PDF and HTML versions of the Article.

Published online: 12 December 2022