High-speed device-independent quantum key distribution against collective attacks

Qiang Zhang (qiangzh@ustc.edu.cn)  
University of Science and Technology of China  
https://orcid.org/0000-0003-3482-3091

Wen-Zhao Liu  
University of Science and Technology of China

Yu-Zhe Zhang  
University of Science and Technology of China

Yi-Zheng Zhen  
University of Science and Technology of China

Ming-Han Li  
University of Science and Technology of China

Yang Liu  
University of Science and Technology of China

Jingyun Fan  
Southern University of Science and Technology  
https://orcid.org/0000-0003-4516-8870

Feihu Xu  
University of Science and Technology of China  
https://orcid.org/0000-0002-1643-225X

Jian-Wei Pan  
Shanghai Branch, National Laboratory for Physical Sciences at Microscale and Department of Modern Physics, University of Science and Technology of China  
https://orcid.org/0000-0002-6100-5142

Physical Sciences - Article

Keywords: quantum key distribution, collective attacks, photonic setup

Posted Date: October 27th, 2021

DOI: https://doi.org/10.21203/rs.3.rs-957419/v1

License: This work is licensed under a Creative Commons Attribution 4.0 International License.  
Read Full License
High-speed device-independent quantum key distribution against collective attacks

Wen-Zhao Liu¹,²,³,†, Yu-Zhe Zhang¹,²,³, Yi-Zheng Zhen¹,²,³, Ming-Han Li¹,²,³, Yang Liu¹,²,³, Jingyun Fan⁴, Feihu Xu¹,²,³, Qiang Zhang¹,²,³, and Jian-Wei Pan¹,²,³

¹Hefei National Laboratory for Physical Sciences at Microscale and Department of Modern Physics, University of Science and Technology of China, Hefei 230026, P. R. China.
²Shanghai Branch, CAS Center for Excellence and Synergetic Innovation Center in Quantum Information and Quantum Physics, University of Science and Technology of China, Shanghai 201315, P. R. China.
³Shanghai Research Center for Quantum Sciences, Shanghai 201315, P. R. China.
⁴Shenzhen Institute for Quantum Science and Engineering and Department of Physics, Southern University of Science and Technology, Shenzhen, 518055, P. R. China

†These authors contributed equally

The security of quantum key distribution (QKD)¹,² usually relies on that the users’s devices are well characterized according to the security models made in the security proofs³. In contrast, device-independent QKD⁴–¹¹ — an entanglement-based protocol² — permits the security even without any knowledge of the underlying devices. Despite its beauty in theory, device-independent QKD is elusive to realize with current technology. This is because a faithful realization requires a high-quality violation of Bell inequality without the fair-sampling assumption¹²,¹³. Particularly, in a photonic realization, a rather high detection efficiency is needed where the threshold values depend on the security proofs⁷–¹¹; this efficiency is far
beyond the current reach\textsuperscript{12–24}. Here, both theoretical and experimental innovations yield the realization of device-independent QKD based on a photonic setup. On the theory side, to relax the threshold efficiency for practical device-independent QKD, we exploit the random post-selection\textsuperscript{25} combined with adding noise\textsuperscript{26} for preprocessing, and compute the entropy with complete nonlocal correlations\textsuperscript{27}. On the experiment side, we develop a high-quality polarization-entangled photonic source and achieve state-of-the-art (heralded) detection efficiency of 87.49\%, which outperforms previous experiments\textsuperscript{12–24} and satisfies the threshold efficiency for the first time. Together, we demonstrate device-independent QKD at a secret key rate of 466 bits/s over 20 m standard fiber in the asymptotic limit against collective attacks. Besides, we show the feasibility of generating secret keys at a fiber length of 220 meters. Importantly, our photonic implementation can generate entangled photons at a high rate and in the telecom wavelength, which is desirable for high-speed key generation over long distances. The results not only prove the feasibility of device-independent QKD with realistic devices, but also push the security of communication to an unprecedented level.

\textit{Introduction. —} Quantum key distribution (QKD)\textsuperscript{1,2} allows two distant users to share a secret key with information-theoretical security\textsuperscript{3}. The security of QKD usually relies on the assumption that the devices are trusted and well-characterized\textsuperscript{28–30}. In practice, however, the imperfections in realistic devices may introduce potential backdoors or side channels\textsuperscript{31,32}. Measurement-device-independent QKD\textsuperscript{33,34} (see also an efficient version\textsuperscript{35}) was proposed to remove the side channels in measurement settings, but its state-preparation devices have to be precisely calibrated. Notably, device-independent QKD\textsuperscript{4–7} relaxes conventional security assumption on the devices. With mini-
mal assumptions satisfied \cite{7}, e.g., the devices have no memory between trials \cite{36,37} and the classical processing units are trusted, the security of device-independent QKD can be guaranteed based solely on the violation of a Bell inequality.

Device-independent QKD is not an easy task with current technology. A realization typically requires that a Bell inequality is violated in a loophole-free fashion \cite{38,39}. A key problem in the photonic implementation is the limited detection efficiency, e.g., the emitted photons in experiments may not be detected due to the losses in the transmission or the imperfect detectors. Although researchers have closed the detection loopholes in recent experiments with efficiency $\eta \sim 80\%$ \cite{12–24}, a much higher efficiency, e.g., $\eta > 90\%$, is normally required for the purpose of device-independent QKD \cite{7–11}. Despite recent theory progress \cite{26,27,40–46}, a practical implementation of device-independent QKD remains elusive.

Here we report the first experimental realization of device-independent QKD with entangled photons, thanks to the significant advancements at both theoretical and experimental sides. On the theoretical side, we propose a protocol to greatly enhance the loss tolerance in the practical case of device imperfections which requires a single-photon system efficiency of about 86\%, and provide a security proof against collective attacks (see the Supplementary Information for details). The basic idea of our protocol is to extract secret keys in the post-selected strings of outcomes \cite{25,47} and then add the noise \cite{26} to the survived raw keys, where the lower bound of quantum conditional entropy can be computed based on the framework in ref. \cite{27}. On the experimental side, we achieve a single-photon system efficiency of greater than 87\% which surpasses the values reported in previous
loophole-free Bell test experiments with photons \textsuperscript{12–24} (see Table 2). Combining the experimental and theoretical advances, we present a proof-of-principle experimental demonstration of device-independent QKD over standard fiber distances up to 220 meters.

\textit{Protocol.} Our protocol is constructed based on a Bell test. As shown in Fig. 1, a pair of entangled photons are shared between Alice and Bob. We consider the scenario that Alice’s measurement has binary input \(x \in \{1, 2\}\) and binary outcome \(a\) and Bob’s measurement has triple input \(y \in \{1, 2, 3\}\) and binary outcome \(b\), where \(a, b = 0(1)\) if the respective detector does (not) register an event, i.e. “click” (or “no-click”). We denote the probability of joint measurement with outcomes \((a, b)\) conditioning upon the measurement inputs \((x, y)\) as \(P(a, b|x, y)\).

Modified after Ref. \textsuperscript{7}, our device-independent QKD protocol is readily to be implemented in the state-of-art quantum optical experiments with the addition of new features, which are briefly summarized here (see the Supplementary Information for details). Consider \(N\)–rounds of Bell test experiment described in Fig. 1, we randomly select a round of experiment whose measurement inputs are \((\bar{x}, \bar{y}) = (1, 3)\) as “key-generation rounds” and use the unselected rounds of experiments as “test rounds” to test nonlocal correlation. For the selected “key-generation rounds” of experiments, Alice and Bob each randomly and independently keep (or discard) a round of experiment with probability \(p\) (or \(1 - p\)) if the respective measurement outcome is a “non-click” and keep a round of experiment if the respective outcome is a “click”. After this post-selection procedure, both Alice and Bob announce the discarded rounds using an authenticated public channel. Those “key-generation rounds” of experiments which are not kept by Alice and Bob simultaneously are
discarded. Then, Alice further performs a noisy preprocessing. She generates the noisy raw keys \( \hat{a}_x \) by flipping each of her survived key bits independently with probability \( p_N \). The protocol is then proceeded with an error correction step that allows Bob to infer Alice’s new (noisy) raw key. The final secret key can be obtained after the privacy amplification. We compile an experimental procedure of our protocol which is listed in Table 1.

Figure 1: An illustration of the device-independent QKD protocol. Alice and Bob share a pair of entangled photons potentially controlled by Eve (\( \rho_{ABE} \)). Alice performs a measurement to her share with binary input \( x \in \{1, 2\} \) and binary output \( a \in \{0, 1\} \). Bob performs a measurement to his share with triple input \( y \in \{1, 2, 3\} \) and binary output \( b \in \{0, 1\} \).

We remark that the random post selection can effectively remove the no-detection events that contain little correlations but high errors, which can effectively reduce the information cost of error correction\(^25\). The noisy preprocessing can decrease the correlation between Alice and Eve by mixing the probability distributions with randomness\(^26\). These two additional processing steps can effectively facilitate the enhancement of loss tolerance (See the Supplementary Information for details).

**Key rate from the preprocessed events.** We consider the collective attack model\(^7\) where the devices behave in an independent and identically distributed (i.i.d.) manner and the devices are memoryless\(^36,37\) at each step of the protocol. For the process of random post-selection, let \( p_\alpha = 1 \cdot \delta_{\alpha, 0} + p \cdot \delta_{\alpha, 1} \) such that a given event \((a, b)\) can be kept with probability \( \omega_{ab} = p_a \cdot p_b \).

Suppose that for a given “key-generation round”, the probability that it can be kept is \( p_{\nu_\nu} = \)
Table 1: The device-independent QKD protocol with preprocessing.

**Assumptions** We focus on collective attacks and assume that the devices are memoryless and behave identically and independently at each step of the protocol.

**Distribution** A source, potentially controlled by Eve, distributes entangled photons to Alice and Bob.

**Measurements** Alice and Bob randomly choose measurement settings $x \in \{1, 2\}$ and $y \in \{1, 2, 3\}$ to measure their own part, respectively.

**Form the raw keys** They use a fraction of strings corresponding to $(\bar{x}, \bar{y}) = (1, 3)$ as the “key-generation round” to generate the raw keys, while all the other strings are used as the “test round” to characterize the nonlocal correlations.

**Random post-selection** For the “key-generation round”, Alice and Bob each randomly and independently discards the non-click bits with probability $1 - p$, while they keep all the click bits.

**Noisy preprocessing** Alice generates the noisy raw keys $\hat{a}_x$ by flipping each of her survived key bits independently with probability $p_N$.

**Error correction and Privacy amplification** A secret key is distilled asymptotically via a one-way error correction protocol and a privacy amplification procedure.
\[ \sum_{a,b \in V} \omega_{ab} P(a, b | x, y), \]

where \( \mathcal{V}_p \) represents the set of post-selected events. In the limit of infinite data size, for a given set of bipartite correlations \( \{ P(a, b | x, y) \} \) that character the devices, the secret key rate \( r \) with optimal error correction can be lower-bounded by the Devetak-Winter rate \(^{48} \)

\[
 r \geq p_{V_p} \left[ H(\hat{A}_x | E, \mathcal{V}_p) - H(\hat{A}_x | B_y, \mathcal{V}_p) \right], \quad (1)
\]

where \( H(\hat{A}_x | E, \mathcal{V}_p) \) is the single-run conditional von Neumann entropy that quantifies the strength of the correlations between Alice and Eve. We here use \( \hat{A}_x \) represent the final key bits of Alice after the step of random post-selection and noisy preprocessing. \( H(\hat{A}_x | B_y, \mathcal{V}_p) \) is the single-run cost of one-way error correction from Alice to Bob. \( p_{V_p} \) represents survived probability of the single-run pair of key bits. We adopt the method in Ref. \(^{27} \) to show that the single-run conditional von Neumann entropy \( H(\hat{A}_x | E, \mathcal{V}_p) \) can be bounded by a converging sequence of optimizations that can be subsequently computed using the NPA hierarchy \(^{49} \) (see the Supplementary Information for details). Note that for the test round, Alice and Bob keep all the outcomes without any post-selection such that the Bell test is done without detection loopholes \(^{47} \).

**Experiment.** — A schematic of the experiment is depicted in Fig. 2 which consists of three modules. Pairs of polarization-entangled photons at the wavelength of 1560 nm are generated probabilistically via the spontaneous parametric downconversion process in the central module (a). The pairs of photons are sent to two side modules (b), where Alice and Bob perform correlated detections to generate secret keys. The single-photon detection efficiency is respectively determined to be 87.16 ± 0.22\% and 87.82 ± 0.21\% for Alice and Bob (see the Supplementary Information for details), which significantly surpass the record values in previous loophole-free Bell tests with photons \(^{14–24} \) (see Table 2). Furthermore, the values also surpass the efficiency threshold of 86.2\%
Figure 2: **Schematic of the experiment.** a Entanglement Source, Creation of pairs of entangled photons: Light pulses of 10 ns are injected at a repetition pulse rate of 2 MHz into a periodically poled potassium titanyl phosphate (PPKTP) crystal in a Sagnac loop to generate polarization-entangled photon pairs. The two photons of an entangled pair at 1560 nm travel in opposite directions to two sites Alice and Bob, where they are subject to polarization projection measurements. We place the PPKTP at a small angle with the light path. This will not significantly affect the upper limit of efficiency that the system could achieve, but it could effectively reduce the reflection of the 1560 nm photons on the inner surface of the PPKTP crystal when the devices are not perfect. These enhancements lead that the non-maximally entangled state generated in our experiment has a better fidelity $99.52 \pm 0.15\%$ as compared to our previous work $^{20,22,23}$. b Alice and Bob, single-photon polarization measurement: In the measurement sites, Alice (Bob) uses a HWP to project the single photon into pre-determined measurement bases. After being collected into the fiber, the single photons transmit through a certain length of fiber and then are detected by a superconducting nanowire single-photon detector (SNSPD) operating at 1K. HWP – half-wave plate; QWP – quarter-wave plate; DM – dichroic mirror; PBS – polarizing beam splitter.
Table 2: Efficiencies in existing photonic experiments of *loophole-free* Bell tests and related applications. The efficiencies in the table are averaged over Alice’s and Bob’s global detection efficiency. (QRNG: quantum random number generation)

| Label | Experiment       | Year | Type      | Efficiency |
|-------|------------------|------|-----------|------------|
| (1)   | Shalm *et al.*   | 2015 | Bell test | 75.15%     |
| (2)   | Giustina *et al.*| 2015 | Bell test | 77.40%     |
| (3)   | Liu *et al.*     | 2018 | QRNG      | 79.40%     |
| (4)   | Shen *et al.*    | 2018 | QRNG      | 82.33%     |
| (5)   | Bierhorst *et al.* | 2018 | QRNG      | 75.50%     |
| (6)   | Liu *et al.*     | 2018 | QRNG      | 78.65%     |
| (7)   | Li *et al.*      | 2018 | Bell test | 78.75%     |
| (8)   | Zhang *et al.*   | 2020 | QRNG      | 76.00%     |
| (9)   | Shalm *et al.*   | 2021 | QRNG      | 76.30%     |
| (10)  | Li *et al.*      | 2021 | QRNG      | 81.35%     |
| (11)  | Liu *et al.*     | 2021 | QRNG      | 84.10%     |
| (12)  | This work        | 2021 | QKD       | 87.49%     |
for device-independent key generation in a realistic scenario.

According to the numerical studies, we prepare a non-maximally two-photon entangled state \( \cos(20.0^\circ)|HV\rangle + \sin(20.0^\circ)|VH\rangle \) and set the measurement settings to \( \{-88.22^\circ, 54.29^\circ\} \) and \( \{9.75^\circ, 21.45^\circ, -1.07^\circ\} \) respectively for \( x \in \{1, 2\} \) and \( y \in \{1, 2, 3\} \) to optimize the probability of key generation, where the values presented in degree are angles of half-wave plates in the polarization measurements by Alice and Bob (Fig. 2). We experimentally measure a two-photon state fidelity of \( 99.52 \pm 0.15\% \) with respect to the ideal state and achieve a CHSH game winning probability of \( 0.7559 \), both substantially improving over previous results \(^{16,17,20,22,23}\) (see the Supplementary Information for details). We repeat the experiment at a rate of \( 2 \times 10^6 \) rounds per second.

In this proof-of-principle experimental demonstration, we place Alice and Bob in the same lab with a distance of 20 meters (mainly the fiber length). We have adopted the shielding assumption \(^{22,50}\) to prohibit unnecessary communications between relevant events taking place in three modules and between these events and adversaries. We alternate the measurement settings instead of randomization to reduce experimental complexity.

We conduct \( 2.4 \times 10^8 \) rounds of experiment for each of the six combinations of measurement settings \((x, y)\) and perform data analysis following the protocol. With optimized parameters \( p_N = 0.13 \) and \( p = 0.96 \), we obtain \( H(\hat{A}_x|E, \mathcal{V}_p) = 0.560206 \) and \( H(\hat{A}_x|B, \mathcal{V}_p) = 0.559953 \). (see the Supplementary Information for details). Finally, according the asymptotic key rate in Eq. (1), 55,920 bits of secret keys are expected to be distilled after error correction and privacy amplifica-
tion. This corresponds to $2.33 \times 10^{-4}$ bit per round or 466 bits per second. Furthermore, we show the feasibility to successfully generate secret keys at a fiber length of 220 meters by conducting the same rounds of experiments, for which we re-optimize the experiment over $p_N$ and $p$. These results are shown in Tab. 3. This shows the loss tolerance of our system to conduct device-independent QKD at longer distances over telecom fiber.

Table 3: The secret key rate as a function of the fiber distance between Alice and Bob. We test the device-independent QKD protocol by adding different length of fibers.

| Fiber length/m | Key rate/bit·s$^{-1}$ | $p_N$ | $p$ |
|----------------|-----------------------|-------|-----|
| 20             | 466                   | 0.13  | 0.96|
| 80             | 107.4                 | 0.17  | 0.94|
| 220            | 2.6                   | 0.49  | 0.99|

**Conclusion.** — In conclusion, we have reported an experimental realization of device-independent QKD against collective attacks with a photonic setup. Our photonic implementation can generate entangled photons at a high rate and in the telecom wavelength, which is desirable for the practical applications. This photonic platform can be naturally combined with quantum memory and quantum repeaters to form a quantum internet. In future, by using the framework of entropy accumulation theorem $^{51}$, our protocol and security analysis can be extended to the consideration of finite-key effects $^{11}$. Overall, the successful implementation of device-independent QKD paves the way for the further realizations and applications of quantum communication and quantum information processing in a device-independence manner.
Note added. When we are completing the manuscript, we notice two concurrent proof-of-concept device-independent QKD experiments based on trapped ions and trapped atoms. In contrast to those systems, our photonic implementation can generate entangled photons at a high rate in the telecom wavelength, which is suitable for high-speed key generation over long-haul optical fiber networks.

Acknowledgements We thank Peter Brown, Roger Colbeck, Charles Lim, Nicolas Sangouard, Jean-Daniel Bancal, Yanbao Zhang, Xingjian Zhang for enlightening discussions. This work was supported by the National Key Research and Development (R&D) Plan of China (2018YFB0504300,2020YFA0309701), the National Natural Science Foundation of China (617714438,62031024), the Anhui Initiative in Quantum Information Technologies, the Chinese Academy of Sciences and the Key-Area Research and Development Program of Guangdong Province (2020B0303010001, 2019ZT08X324).

Author contributions J.F., F.X., Q.Z. and J.-W.P. conceived the research. Y.L., J.F., Q.Z. and J.-W.P. designed the experiment. W.-Z.L., M.-H.L. and Y.L. designed and implemented the entangled photon pair source. W.-Z.L. designed the data acquisition software. Y. Zhang, Y. Zhen and F.X. developed the theory. Y. Zhang, Y. Zhen, W.-Z.L. and F.X. performed the protocol analysis, numerical modelling and randomness extraction. All authors contributed to the experimental realization, data analysis and manuscript preparation.

Competing interests The authors declare no competing interests.
References

1. Bennett, C. H. & Brassard, G. Quantum cryptography: Public key distribution and coin tossing. In *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing*, 175–179 (Bangalore, India, 1984).

2. Ekert, A. K. Quantum cryptography based on bell’s theorem. *Phys. Rev. Lett.* **67**, 661–663 (1991). URL https://link.aps.org/doi/10.1103/PhysRevLett.67.661.

3. Xu, F., Ma, X., Zhang, Q., Lo, H.-K. & Pan, J.-W. Secure quantum key distribution with realistic devices. *Reviews of Modern Physics* **92**, 025002 (2020).

4. Mayers, D. & Yao, A. Quantum cryptography with imperfect apparatus. In *Proceedings of the 39th Annual Symposium on Foundations of Computer Science, FOCS ’98*, 503– (IEEE Computer Society, Washington, DC, USA, 1998). URL http://dl.acm.org/citation.cfm?id=795664.796390.

5. Barrett, J., Hardy, L. & Kent, A. No signaling and quantum key distribution. *Phys. Rev. Lett.* **95**, 010503 (2005). URL https://link.aps.org/doi/10.1103/PhysRevLett.95.010503.

6. Acín, A. *et al.* Device-independent security of quantum cryptography against collective attacks. *Phys. Rev. Lett.* **98**, 230501 (2007). URL https://link.aps.org/doi/10.1103/PhysRevLett.98.230501.
7. Pironio, S. et al. Device-independent quantum key distribution secure against collective attacks. *New J. Phys.* **11**, 045021 (2009). URL http://stacks.iop.org/1367-2630/11/i=4/a=045021.

8. Masanes, L., Pironio, S. & Acín, A. Secure device-independent quantum key distribution with causally independent measurement devices. *Nat. Commn.* **2**, 238 (2011). URL https://doi.org/10.1038/ncomms1244.

9. Reichardt, B. W., Unger, F. & Vazirani, U. Classical command of quantum systems. *Nature* **496**, 456 (2013). URL https://doi.org/10.1038/nature12035.

10. Vazirani, U. & Vidick, T. Fully device-independent quantum key distribution. *Phys. Rev. Lett.* **113**, 140501 (2014). URL https://link.aps.org/doi/10.1103/PhysRevLett.113.140501.

11. Arnon-Friedman, R., Dupuis, F., Fawzi, O., Renner, R. & Vidick, T. Practical device-independent quantum cryptography via entropy accumulation. *Nat. Commn.* **9**, 459 (2018). URL https://doi.org/10.1038/s41467-017-02307-4.

12. Giustina, M. et al. Bell violation using entangled photons without the fair-sampling assumption. *Nature* **497**, 227–230 (2013).

13. Christensen, B. G. et al. Detection-loophole-free test of quantum nonlocality, and applications. *Physical review letters* **111**, 130406 (2013).
14. Shalm, L. K. et al.  Strong loophole-free test of local realism. *Phys. Rev. Lett.* **115**, 250402 (2015). URL https://link.aps.org/doi/10.1103/PhysRevLett.115.250402.

15. Giustina, M. et al.  Significant-loophole-free test of bell’s theorem with entangled photons. *Phys. Rev. Lett.* **115**, 250401 (2015). URL https://link.aps.org/doi/10.1103/PhysRevLett.115.250401.

16. Li, M.-H. et al.  Test of local realism into the past without detection and locality loopholes. *Physical review letters* **121**, 080404 (2018).

17. Liu, Y. et al.  High-speed device-independent quantum random number generation without a detection loophole. *Physical review letters* **120**, 010503 (2018).

18. Shen, L. et al.  Randomness extraction from bell violation with continuous parametric down-conversion. *Physical review letters* **121**, 150402 (2018).

19. Bierhorst, P. et al.  Experimentally generated randomness certified by the impossibility of superluminal signals. *Nature* **556**, 223–226 (2018).

20. Liu, Y. et al.  Device-independent quantum random-number generation. *Nature* **562**, 548 (2018). URL https://doi.org/10.1038/s41586-018-0559-3.

21. Zhang, Y. et al.  Experimental low-latency device-independent quantum randomness. *Physical Review Letters* **124**, 010505 (2020).
22. Liu, W.-Z. et al. Device-independent randomness expansion against quantum side information. *Nature Physics* **17**, 448–451 (2021).

23. Li, M.-H. et al. Experimental realization of device-independent quantum randomness expansion. *Phys. Rev. Lett.* **126**, 050503 (2021). URL https://link.aps.org/doi/10.1103/PhysRevLett.126.050503.

24. Shalm, L. K. et al. Device-independent randomness expansion with entangled photons. *Nature Physics* **17**, 452–456 (2021).

25. Xu, F., Zhang, Y.-Z., Zhang, Q. & Pan, J.-W. Device-independent quantum key distribution with random post selection. *to be submitted* (2021).

26. Ho, M. et al. Noisy preprocessing facilitates a photonic realization of device-independent quantum key distribution. *Physical Review Letters* **124**, 230502 (2020).

27. Brown, P., Fawzi, H. & Fawzi, O. Device-independent lower bounds on the conditional von neumann entropy (2021). arXiv:2106.13692.

28. Lo, H. K. & Chau, H. F. Unconditional security of quantum key distribution over arbitrarily long distances. *Science* **283**, 2050 (1999). URL http://science.sciencemag.org/content/283/5410/2050.

29. Shor, P. W. & Preskill, J. Simple proof of security of the bb84 quantum key distribution protocol. *Phys. Rev. Lett.* **85**, 441–444 (2000). URL https://link.aps.org/doi/10.1103/PhysRevLett.85.441.
30. Renner, R. Security of quantum key distribution. *Int. J. Quantum Inf.* **06**, 1–127 (2008). URL https://doi.org/10.1142/S0219749908003256.

31. Xu, F., Qi, B. & Lo, H.-K. Experimental demonstration of phase-remapping attack in a practical quantum key distribution system. *New. J. Phys.* **12**, 113026 (2010). URL http://stacks.iop.org/1367-2630/12/i=11/a=113026.

32. Lydersen, L. *et al.* Hacking commercial quantum cryptography systems by tailored bright illumination. *Nat. Photon.* **4**, 686–689 (2010).

33. Lo, H.-K., Curty, M. & Qi, B. Measurement-device-independent quantum key distribution. *Phys. Rev. Lett.* **108**, 130503 (2012). URL https://link.aps.org/doi/10.1103/PhysRevLett.108.130503.

34. Braunstein, S. L. & Pirandola, S. Side-channel-free quantum key distribution. *Phys. Rev. Lett.* **108**, 130502 (2012). URL https://link.aps.org/doi/10.1103/PhysRevLett.108.130502.

35. Lucamarini, M., Yuan, Z., Dynes, J. & Shields, A. Overcoming the rate–distance limit of quantum key distribution without quantum repeaters. *Nature* **557**, 400 (2018). URL https://doi.org/10.1038/s41586-018-0066-6.

36. Barrett, J., Colbeck, R. & Kent, A. Memory attacks on device-independent quantum cryptography. *Phys. Rev. Lett.* **110**, 010503 (2013). URL https://link.aps.org/doi/10.1103/PhysRevLett.110.010503.
37. Curty, M. & Lo, H.-K. Foiling covert channels and malicious classical post-processing units in quantum key distribution. *Npj Quantum Inf.* **5**, 14 (2019). URL https://doi.org/10.1038/s41534-019-0131-5.

38. Hensen, B. *et al.* Loophole-free bell inequality violation using electron spins separated by 1.3 kilometres. *Nature* **526**, 682 (2015). URL https://doi.org/10.1038/nature15759.

39. Rosenfeld, W. *et al.* Event-ready bell test using entangled atoms simultaneously closing detection and locality loopholes. *Phys. Rev. Lett.* **119**, 010402 (2017). URL https://link.aps.org/doi/10.1103/PhysRevLett.119.010402.

40. Ma, X. & Lütkenhaus, N. Improved data post-processing in quantum key distribution and application to loss thresholds in device independent qkd. *Quantum Information & Computation* **12**, 203–214 (2012).

41. Tan, E. Y.-Z., Lim, C. C.-W. & Renner, R. Advantage distillation for device-independent quantum key distribution. *Physical Review Letters* **124**, 020502 (2020).

42. Woodhead, E., Acín, A. & Pironio, S. Device-independent quantum key distribution with asymmetric chsh inequalities. *Quantum* **5**, 443 (2021).

43. Sekatski, P. *et al.* Device-independent quantum key distribution from generalized chsh inequalities. *Quantum* **5**, 444 (2021).
44. Gonzales-Ureta, J. R., Predojević, A. & Cabello, A. Device-independent quantum key distribution based on bell inequalities with more than two inputs and two outputs. *Physical Review A* **103**, 052436 (2021).

45. Brown, P., Fawzi, H. & Fawzi, O. Computing conditional entropies for quantum correlations. *Nature communications* **12**, 1–12 (2021).

46. Schwonnek, R. *et al.* Device-independent quantum key distribution with random key basis. *Nature communications* **12**, 1–8 (2021).

47. de la Torre, G., Bancal, J.-D., Pironio, S., Scarani, V. *et al.* Randomness in post-selected events. *New Journal of Physics* **18**, 035007 (2016).

48. Igor, D. & Andreas, W. Distillation of secret key and entanglement from quantum states. *Proc. R. Soc. Lond. A* **461**, 207–235 (2005). URL https://doi.org/10.1098/rspa.2004.1372.

49. Navascués, M., Pironio, S. & Acín, A. Bounding the set of quantum correlations. *Phys. Rev. Lett.* **98**, 010401 (2007). URL https://link.aps.org/doi/10.1103/PhysRevLett.98.010401.

50. Pironio, S. *et al.* Random numbers certified by bell’s theorem. *Nature* **464**, 1021 (2010). URL https://doi.org/10.1038/nature09008.

51. Dupuis, F., Fawzi, O. & Renner, R. Entropy accumulation. *Communications in Mathematical Physics* **379**, 867–913 (2020).
52. Nadlinger, D. P. et al. Device-independent quantum key distribution (2021). arXiv:2109.14600.

53. Zhang, W. et al. Experimental device-independent quantum key distribution between distant users (2021). arXiv:2110.00575.
Figures

Figure 1

An illustration of the device-independent QKD protocol.

Figure 2
Schematic of the experiment.

Supplementary Files

This is a list of supplementary files associated with this preprint. Click to download.

- SupplementaryV3.pdf