nature COMMUNICATIONS

ARTICLE

Received 13 May 2014 | Accepted 9 Mar 2015 | Published 23 Apr 2015

DOI: 10.1038/ncomms7908

Limitations on quantum key repeaters

Stefan Bäuml[1,2], Matthias Christandl[3], Karol Horodecki[4,5] & Andreas Winter[1,2,6]

A major application of quantum communication is the distribution of entangled particles for use in quantum key distribution. Owing to noise in the communication line, quantum key distribution is, in practice, limited to a distance of a few hundred kilometres, and can only be extended to longer distances by use of a quantum repeater, a device that performs entanglement distillation and quantum teleportation. The existence of noisy entangled states that are undistillable but nevertheless useful for quantum key distribution raises the question of the feasibility of a quantum key repeater, which would work beyond the limits of entanglement distillation, hence possibly tolerating higher noise levels than existing protocols. Here we exhibit fundamental limits on such a device in the form of bounds on the rate at which it may extract secure key. As a consequence, we give examples of states suitable for quantum key distribution but unsuitable for the most general quantum key repeater protocol.

[1] Department of Mathematics, University of Bristol, Bristol BS8 1TW, UK. [2] Fisica Teòrica: Informació i Fenòmens Quàntics, Universitat Autònoma de Barcelona, ES-08193 Bellaterra (Barcelona), Spain. [3] Department of Mathematical Sciences, University of Copenhagen, Universitetsparken 5, 2100 Copenhagen, Denmark. [4] Institute of Informatics, University of Gdańsk, 80-952 Gdańsk, Poland. [5] National Quantum Information Centre of Gdańsk, 81-824 Sopot, Poland. [6] ICREA—Institució Catalana de Recerca i Estudis Avançats, ES-08010 Barcelona, Spain. Correspondence and requests for materials should be addressed to S.B. (email: stefan.baeuml@bristol.ac.uk).

© 2015 Macmillan Publishers Limited. All rights reserved.

When a signal is passed from a sender to a receiver, it inevitably degrades due to the noise present in any realistic communication channel, for example, a cable or free space. The degradation of the signal is typically exponential in the length of the communication line. When the signal is classical, degradation can be counteracted by the use of an amplifier that measures the degraded signal and, depending on a threshold, replaces it by a stronger signal. When the signal is quantum mechanical (for example, encoded in non-orthogonal polarizations of a single photon), such an amplifier cannot work anymore, since the measurement inevitably disturbs the signal[1], and, more generally, since quantum mechanical signals cannot be cloned[2]. Sending a quantum signal, however, is the basis of quantum key distribution (QKD), a method to distribute a cryptographic key, which can later be used for perfectly secure communication between sender and receiver[3]. The degradation of sent quantum signals therefore seems to place a fundamental limit on the distance at which secure communication is possible thereby severely limiting its applicability in the internet[4–6].

A way around this limitation is the use of entanglement-based QKD schemes[7,8] in conjunction with a so-called quantum repeater[9,10]. This amounts to distributing n Einstein–Podolsky–Rosen (EPR) pairs between Alice and Charlie (an untrusted telecom provider) and between Bob and Charlie. Imperfections due to noise in the transmission are compensated by distillation, yielding $\approx E_D \times n$ perfect EPR pairs. Here E_D denotes the distillable entanglement of the imperfect EPR pair, that is, the optimal rate at which perfect EPR pairs can be distilled from imperfect ones. The EPR pairs between Charlie and Bob are then used to teleport the state of Charlie's other particles to Bob. This process, known as entanglement swapping, results in EPR pairs between Alice and Bob[11] (see Fig. 1). When Alice and Bob make appropriate measurements on these EPR pairs, they obtain a sequence of secret key bits, that is, an identical but random sequence of bits that is uncorrelated with the rest of the universe (including Charlie's systems), enabling secure communication. The described scheme with one intermediate station effectively doubles the distance over which QKD can be carried out. This abstract view of the quantum repeater will be sufficient for our purpose. The full proposal of a quantum repeater in fact allows to efficiently extend the distance arbitrarily even if the local operations are subject to a limited amount of noise[9]. The implementation of quantum repeaters is therefore one of the focal points of experimental quantum information science[10].

Owing to the tight connection between the distillation of EPR pairs and QKD[12,13], it came as a surprise that there are bound entangled states (that is, entangled states with vanishing distillable entanglement) from which the secret key can be obtained[14]. With the help of a quantum repeater as described above, however, the secret key contained in such states cannot be extended to larger distances, as the states do not allow for the distillation of EPR pairs. This raises the question of whether there may be other ways to extend the secret key to arbitrary distances than by entanglement distillation and swapping, other quantum key repeaters.

In this work, we introduce and formally define the concept of a quantum key repeater. We then study the associated quantum key repeater rate. It is always at least as large as the rate that can be obtained in a quantum repeater protocol and we raise the question whether it could be larger (and in particular non-zero for bound entangled states). Our main results consist of upper bounds on this quantity which we use to show that there are quantum states with extreme behaviour—state with a large key rate but with a negligible quantum key repeater rate. We thus demonstrate the fundamental limitations on quantum key repeaters.

Results

The quantum key repeater rate. We analyse the quantum key repeater rate $K_{A\leftrightarrow C\leftrightarrow B}$ at which a protocol—only using local operations and classical communication (LOCC)—is able to extract private bits between Alice and Bob from entangled states, which each of them shares with Charlie (see Fig. 2). See Supplementary Note 1 for a formal definition of the key repeater rate. By a private bit, we mean an entangled state containing a unit of privacy paralleling the EPR pair as a unit of entanglement[14,15]. Mathematically, private bits are entangled states of the form

$$\gamma_{AA'BB'} = \frac{1}{2}\begin{bmatrix} \sqrt{XX^\dagger} & 0 & 0 & X \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ X^\dagger & 0 & 0 & \sqrt{X^\dagger X} \end{bmatrix}, \qquad (1)$$

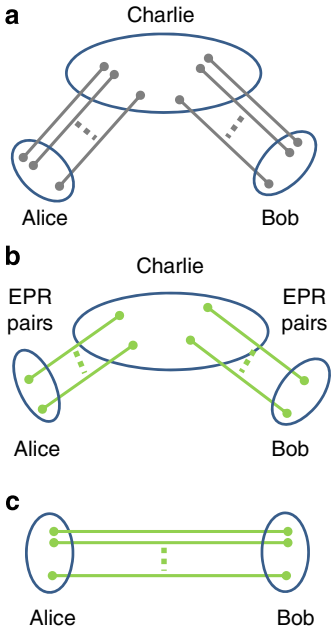

Figure 1 | Quantum repeater. (**a**) Alice and Charlie—and similarly Charlie and Bob—distil EPR pairs from noisy states (grey). (**b**) Charlie uses the EPR pairs (green) he shares with Bob to teleport his part of the states he shares with Alice to Bob. (**c**) Alice and Bob share EPR pairs.

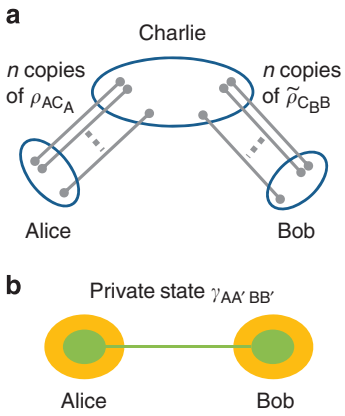

Figure 2 | Quantum key repeater. (**a**) Multiple copies of noisy states ρ and $\tilde{\rho}$, shared by Alice and Charlie and by Charlie and Bob, respectively, are transformed by means of LOCC into (**b**) a private state γ (green-yellow) between Alice and Bob.

© 2015 Macmillan Publishers Limited. All rights reserved.

where A and B are qubits that contain the key bits, corresponding to the rows and columns in the matrix. The AB subsystem is called the key part. A′ and B′ are each a d-dimensional systems, forming the so-called shield part. X is a d^2-by-d^2 matrix with $\|X\|_1 = 1$ (see also Fig. 3). $\gamma_{AA'BB'}$ can also be presented in the form $U|\Psi\rangle\langle\Psi|_{AB} \otimes \sigma_{A'B'} U^\dagger$, where $\sigma_{A'B'}$ is some state, $|\Psi\rangle = \frac{1}{\sqrt{2}}|00+11\rangle$ and $U = |00\rangle\langle 00|_{AB} \otimes U_0 + |11\rangle\langle 11|_{AB} \otimes U_1$, where U_0 and U_1 are unitaries acting on $\sigma_{A'B'}$. This operation is called twisting. It is now easy to see that the bit that Alice and Bob obtain when they measure A and B in the computation basis is a key bit, that is, it is random and secure, that is product with a purification of γ held by the eavesdropper. The relation between X and $\sigma_{A'B'}$ is given by $X = U_0 \sigma_{A'B'} U_1^\dagger$.

Note that just as the definition of the distillable key[14,16], the definition of the quantum key repeater rate is information-theoretic in nature. The role of Charlie here merits special attention. While he participates in the LOCC protocol like Alice and Bob do, he is not a 'trusted party'; indeed, at the end of the protocol, Alice and Bob wish to obtain private bits, whose privacy is not compromised even if at that point Charlie passes all his remaining information to the eavesdropper. We also note that well-known techniques from quantum information theory[17,18] allow to conclude that the obtained rate of private bits can be made unconditionally secure[19–21]. In the following, we will describe our main results, which demonstrate that the performance of quantum key repeaters beyond the use of entanglement distillation is severely limited.

Some private states cannot be swapped. Our first result takes as its starting point the observation that there are private bits that are almost indistinguishable from separable states by LOCC[22]. To see this, consider the state

$$\tilde{\gamma}_{AA'BB'} = \frac{1}{2}\begin{bmatrix} \sqrt{XX^\dagger} & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & \sqrt{X^\dagger X} \end{bmatrix}, \qquad (2)$$

which is obtained from γ, when Alice and Bob measure the key part of their state in the computational basis. An example is given by the choice $X = \frac{1}{d\sqrt{d}} \sum_{ij} u_{ij} |i\rangle\langle j| \otimes |j\rangle\langle i|$, where the u_{ij} are the entries in the quantum Fourier transform in dimension d. For this choice of X, $\tilde{\gamma}$ is separable. The distinguishability under LOCC operations is measured in the norm $\|\gamma - \tilde{\gamma}\|_{LOCC}$, which is bounded by the distinguishability under global maps preserving the positivity under the partial transpose $\|\gamma - \tilde{\gamma}\|_{PPT}$ (ref. 23). This can further be bounded by $\|\gamma^\Gamma - \tilde{\gamma}^\Gamma\|_1$, which is easily calculated as $\|X^\Gamma\|_1 = \frac{1}{\sqrt{d}+1}$. Γ indicates the partial transpose, that is, the transpose of one of the systems[24].

Suppose now that a quantum repeater protocol applied to two copies of the latter state, shared by Alice and Charlie and Bob and Charlie, respectively, successfully outputs a private bit between Alice and Bob. This could be regarded as the privacy analogue to entanglement swapping. Then, if Alice and Bob joined their labs, they could distinguish this resulting state from a separable state, as separable states are well distinguishable from private states by a global measurement[14]. This implies an LOCC procedure for Alice and Bob (jointly) and Charlie to distinguish the initial private bits $\gamma \otimes \gamma$ from separable states: first run the quantum key repeater protocol and then perform the measurement. This, however, is in contradiction to the property that the private state γ (and hence $\gamma \otimes \gamma$) is almost indistinguishable from separable states under LOCC. In conclusion, this shows that such private bits cannot be successfully extended to a private bit between Alice and Bob by any LOCC protocol acting on single copies (see Supplementary Note 2).

Bounding the quantum key repeater rate. Although intuitive, the above argument only bounds the repeated key obtained from a single copy of input states. The language of entanglement measures allows us to formulate this argument asymptotically as a rigorous distinguishability bound on the rate $K_{A\leftrightarrow C\leftrightarrow B}$ for general states ρ and $\tilde{\rho}$:

$$K_{A\leftrightarrow C\leftrightarrow B}\left(\rho_{AC_A} \otimes \tilde{\rho}_{C_B B}\right) \leq D^{\infty}_{C\leftrightarrow AB}\left(\rho_{AC_A} \otimes \tilde{\rho}_{C_B B}\right), \qquad (3)$$

where the right-hand side is the regularized LOCC-restricted relative entropy distance to the closest separable state[25]: $D^{\infty}_{C\leftrightarrow AB}(\rho) = \lim_{n\mapsto\infty} \frac{1}{n} D_{C\leftrightarrow AB}(\rho^{\otimes n})$, where $D_{C\leftrightarrow AB}(\rho) = \inf_\sigma \sup_M D(M(\rho)\|M(\sigma))$ with the minimization over separable states σ, the maximization over measurements implementable by LOCC with respect to the C:AB partition and D the relative entropy distance. The proof is given in Supplementary Note 3.

Arguably, it is difficult, if not impossible, to compute this expression. But noting that this bound is invariant under partial transposition of the C system, we can easily upper bound the

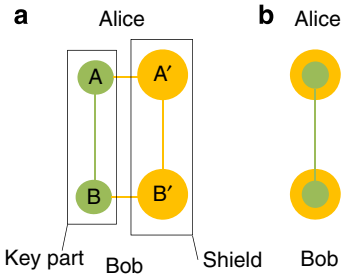

Figure 3 | The private state $\gamma_{AA'BB'}$. (**a**) Bipartite state with four subsystems A, A′, B and B′. The subsystems AB form the 'key part' (green) which, due to the 'shield part' A′B′ (yellow), is secure against an eavesdropper. (**b**) Icon of a private bit.

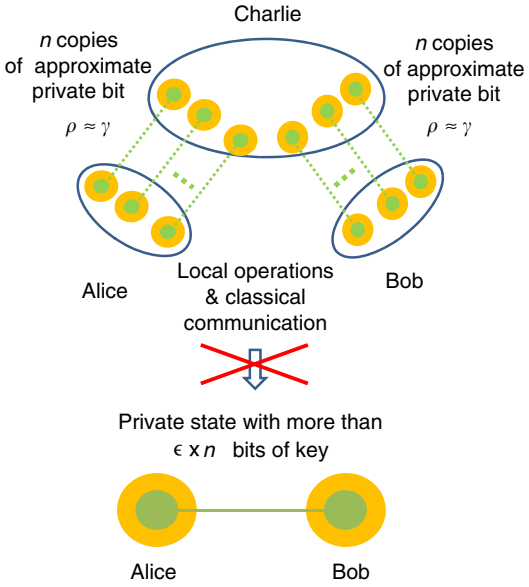

Figure 4 | Limitation on quantum key repeaters. Despite Alice and Charlie as well as Charlie and Bob sharing states containing almost n bits of secrecy there is no LOCC protocol between Alice, Charlie and Bob, which results in a non-negligible amount of secure key between Alice and Bob.

© 2015 Macmillan Publishers Limited. All rights reserved.

quantity for all known bound entangled states (these are the ones with positive partial transpose) in terms of the regularised relative entropy of entanglement of the partially transposed state ρ^Γ : $E_R^\infty(\rho^\Gamma) + E_R^\infty(\tilde{\rho}^\Gamma)$. The relative entropy of entanglement is given by $E_R(\rho) = \min_\sigma D(\rho||\sigma)$ where the minimization extends over separable states; the regularization is analogous to the one above. If we restrict to forward communication from Charlie and $\rho_{AC_A} = \tilde{\rho}_{C_BB}$, the squashed entanglement measure provides a bound: $K_{A\leftarrow C\rightarrow B}(\rho_{AC_A} \otimes \tilde{\rho}_{C_BB}) \leq 4E_{sq}(\rho^\Gamma)$. The squashed entanglement is given as (one half times) the minimal conditional mutual information when minimizing over all extensions of the state (we condition on the extending system). Using invariance under partial transposition directly on the hypothetical quantum key repeater protocol, we obtain for PPT states ρ and $\tilde{\rho}$:

$$\begin{aligned} K_{A\leftrightarrow C\leftrightarrow B}(\rho_{AC_A} \otimes \tilde{\rho}_{C_BB}) &\leq K_D\left(\rho^\Gamma_{AC_A}\right) \\ &\leq \min\left\{E_R^\infty\left(\rho^\Gamma_{AC_A}\right), E_{sq}\left(\rho^\Gamma_{AC_A}\right)\right\}, \end{aligned} \quad (4)$$

where K_D is the key rate, that is, the rate at which secret key can be extracted from ρ by LOCC. The same holds for $\tilde{\rho}^\Gamma_{C_BB}$. The proof can be found in Supplementary Note 4.

We will now give an example of a state $\rho_{AC_A} = \tilde{\rho}_{C_BB}$ for which the key rate is large, but the bounds and hence the quantum key repeater rate, are arbitrarily small. Guided by our intuition, we would like to consider the private bit γ from above whose partial transpose is close to a separable state. The state, however, is not PPT, as no private bit can be PPT[14]. Fortunately, it turns into a PPT state ρ under mixing with a small amount of noise and we find $K_{A\leftrightarrow C\leftrightarrow B}(\rho\otimes\rho)\approx 0$ while $K_D(\rho)\approx 1$. This leads us to the main conclusion of our paper—there exist entangled quantum states that are useful for QKD at small distances but that are virtually useless for long-distance QKD (see Fig. 4).

Bounding the entanglement of the output. Finally, we present a different type of bound on the quantum key repeater rate based on the direct analysis of the entanglement of a concrete output state of a quantum repeater protocol:

$$K_{A\leftarrow C\leftrightarrow B}(\rho_{AC_A} \otimes \tilde{\rho}_{C_BB}) \leq \frac{1}{2}E_C(\rho_{AC_A}) + \frac{1}{2}E_D(\tilde{\rho}_{C_BB}), \quad (5)$$

where E_C denotes the entanglement cost of the state, the rate of EPR states needed to create many copies of the state. This bound, unlike the ones presented above, applies to all quantum states. In particular, it applies to certain states invariant under partial transposition, which escape the techniques presented before. Note that in the case of PPT states, one may partially transpose the states appearing on the right-hand side since $K_{A\leftarrow C\leftrightarrow B}$ is invariant under partial transposition. The proof of equation (5) is obtained by upper bounding the squashed entanglement of the output state of the protocol using a manipulation of entropies resulting in the right-hand side of equation (5). The squashed entanglement in turn upper bounds the distillable key of the output state (which upper bounds the left hand side)[26]. For a detailed proof see Supplementary Note 5. There, we also exhibit a private bit with a significant drop in the repeater rate when compared with the key rate. We further investigate the tightness of the bound (5) and, based on a random construction, show that the left hand side cannot be replaced by the entanglement cost of the output state.

Discussion

The preceding results pose limitations on the entanglement of the output state of a quantum key repeater protocol. As such, they support the PPT-square conjecture: assume that Alice and Charlie share a PPT state and that Bob and Charlie share a PPT state; then the state of Alice and Bob, conditioned on any measurement by Charlie, is always separable[27–29]. Reaching even further, and consistent with our findings, we may speculate that perhaps the only 'transitive' entanglement in quantum states, that is, entanglement that survives a quantum key repeater, is the distillable entanglement. One may also wonder whether apart from equation (5) there are other inequalities between entanglement measures of the in- and output states. In the context of algebro-geometric measures, this question has been raised and relations for the concurrence have been found[30,31]. Our work focuses on operational entanglement measures.

States from which more key than entanglement can be extracted have recently been demonstrated experimentally in a quantum optical set-up[32]. These are exactly the private states discussed in Supplementary Note 2 (X is the SWAP operator) with shield dimension equal to two. As our results for these states only become effective for higher shield dimensions, we cannot conclude that the single-copy key repeater drops when compared with the key contained in these states. This may be overcome by stronger theoretical bounds or experimental progress, which increases the shield dimension; we expect both improvements to be achieved in the near future.

With this paper, we initiate the study of long-distance quantum communication and cryptography beyond the use of entanglement distillation by the introduction of the concept of a quantum key repeater. Even though the reported results provide limitations rather than new possibilities, we hope that this work will lead to a rethinking of the currently used protocols resulting in procedures for long-distance quantum communication that are both more efficient and that can operate in noisier environments. In the following, we will give a simple example of such a rethinking: assume that Alice and Charlie share a private bit γ_{AC_A} that is almost PPT and thus requires a large shield system (see Supplementary Note 6). The quantum repeater based on quantum teleportation would thus require Bob and Charlie to share a large amount of EPR pairs to teleport Charlie's share of γ_{AC_A} to Bob. Alice and Bob can then extract one bit of secret key by measuring the state. Inspired by the work of Smith and Yard[33], we show in Supplementary Note 6 that a single EPR pair and a particular state ρ_{C_BB}, which is so noisy that it contains no (one-way) distillable entanglement, are sufficient to obtain a large quantum key repeater rate (using only one-way communication from Alice and Charlie to Bob). We thus showed that there are situations in which significant amounts of distillable entanglement may be replaced by (one-way) undistillable states.

References

1. Fuchs, C. A. & Peres, A. Quantum-state disturbance versus information gain: uncertainty relations for quantum information. *Phys. Rev. A* **53,** 2038–2045 (1996).
2. Wootters, W. K. & Zurek, W. H. A single quantum cannot be cloned. *Nature* **299,** 802–803 (1982).
3. Bennett, C. H. & Brassard, G. in *Proc. IEEE Int. Conf. Computers, Systems and Signal Processing* 175–179 (Yorktown, NY, USA, 1984).
4. Stucki, D. *et al.* High rate, long-distance quantum key distribution over 250 km of ultra low loss fibres. *New J. Phys.* **11,** 075003 (2009).
5. Gisin, N., Ribordy, G., Tittel, W. & Zbinden, H. Quantum cryptography. *Rev. Mod. Phys.* **74,** 145–195 (2002).
6. Scarani, V. *et al.* The security of practical quantum key distribution. *Rev. Mod. Phys.* **81,** 1301–1350 (2009).
7. Ekert, A. K. Quantum cryptography based on Bell's theorem. *Phys. Rev. Lett.* **67,** 661–663 (1991).
8. Bennett, C. H., Brassard, G. & Mermin, N. D. Quantum cryptography without Bell's theorem. *Phys. Rev. Lett.* **68,** 557–559 (1992).
9. Briegel, H.-J., Dür, W., Cirac, J. I. & Zoller, P. Quantum repeaters: the role of imperfect local operations in quantum communication. *Phys. Rev. Lett.* **81,** 5932–5935 (1998).
10. Sangouard, N., Simon, C., De Riedmatten, H. & Gisin, N. Quantum repeaters based on atomic ensembles and linear optics. *Rev. Mod. Phys.* **83,** 33–80 (2011).

© 2015 Macmillan Publishers Limited. All rights reserved.

11. Żukowski, M., Zeilinger, A., Horne, M. A. & Ekert, A. K. Event-ready-detectors, Bell experiment via entanglement swapping. *Phys. Rev. Lett.* **71,** 4287–4290 (1993).
12. Deutsch, D. *et al.* Quantum privacy amplification and the security of quantum cryptography over noisy channels. *Phys. Rev. Lett.* **77,** 2818–2821 (1996).
13. Shor, P. W. & Preskill, J. Simple proof of security of the BB84 quantum key distribution protocol. *Phys. Rev. Lett.* **85,** 441–444 (2000).
14. Horodecki, K., Horodecki, M., Horodecki, P. & Oppenheim, J. Secure key from bound entanglement. *Phys. Rev. Lett.* **94,** 160502 (2005).
15. Horodecki, K., Horodecki, M., Horodecki, P. & Oppenheim, J. General paradigm for distiling classical key from quantum states. *IEEE Trans. Inf. Theory* **55,** 1898–1929 (2009).
16. Devetak, I. & Winter, A. Distillation of secret key and entanglement from quantum states. *Proc. R. Soc. Lond. A* **461,** 207–235 (2005).
17. Christandl, M., König, R. & Renner, R. Postselection technique for quantum channels with applications to quantum cryptography. *Phys. Rev. Lett.* **102,** 020504 (2009).
18. Renner, R. & König, R. in *Theory of Cryptography, Lecture Notes in Computer Science* vol. 3378 (ed. Kilian, J.) 407–425 (Springer, 2005).
19. Ben-Or, M., Horodecki, M., Leung, D. W., Mayers, D. & Oppenheim, J. in *Theory of Cryptography, Lecture Notes in Computer Science*. vol. 3378 (ed. Kilian, J.) 386–406 (Springer, 2005).
20. Unruh, D. Simulatable security for quantum protocols. Preprint available at http://arxiv.org/abs/quant-ph/0409125 (2004).
21. Horodecki, K., Horodecki, M., Horodecki, P., Leung, D. & Oppenheim, J. Quantum key distribution based on private states: unconditional security over untrusted channels with zero quantum capacity. *IEEE Trans. Inf. Theory* **54,** 2604–2620 (2008).
22. Horodecki, K. *General Paradigm for Distiling Classical Key From Quantum States—On Quantum Entanglement and Security*. Ph.D. thesis, Univ. Warsaw. Available at http://www.mimuw.edu.pl/wiadomosci/aktualnosci/doktoraty/pliki/karol_horodecki/doktorat-kh.pdf (2008).
23. Eggeling, T. & Werner, R. F. Hiding classical data in multipartite quantum states. *Phys. Rev. Lett.* **89,** 97905 (2002).
24. Horodecki, K., Pankowski, Ł., Horodecki, M. & Horodecki, P. Low dimensional bound entanglement with one-way distillable cryptographic key. *IEEE Trans. Inf. Theory* **54,** 2621–2625 (2008).
25. Piani, M. Relative entropy of entanglement and restricted measurements. *Phys. Rev. Lett.* **103,** 160504 (2009).
26. Christandl, M., Schuch, N. & Winter, A. Entanglement of the Antisymmetric State. *Commun. Math. Phys.* **311,** 397–422 (2012).
27. Beth Ruskai, M., Junge, M., Kribs, D., Hayden, P. & Winter, A. (eds) *Banff International Research Station workshop: Operator Structures in Quantum Information Theory* (2012). Available at https://www.birs.ca/workshops/2012/12w5084/report12w5084.pdf.
28. Bäuml, S. *On Bound Key And The Use Of Bound Entanglement*. Diploma thesis, Ludwig Maximilians Universität München. Available at http://www.maths.bris.ac.uk/~masmgb/Diploma_thesis.pdf (2010).
29. Hansen, A. *Swapped Bound Entanglement*. Master thesis, ETH Zurich. Available at http://www.qit.ethz.ch/paperPDFs/Hansen-Masterarbeit.pdf (2013).
30. Gour, G. Mixed-state entanglement of assistance and the generalized concurrence. *Phys. Rev. A* **72,** 042318 (2005).
31. Lee, S., Kim, J. S. & Sanders, B. C. Distribution and dynamics of entanglement in high-dimensional quantum systems using convex-roof extended negativity. *Phys. Lett. A* **375,** 411–414 (2011).
32. Dobek, K., Karpiński, M., Demkowicz-Dobrzański, R., Banaszek, K. & Horodecki, P. Experimental extraction of secure correlations from a noisy private state. *Phys. Rev. Lett.* **106,** 030501 (2011).
33. Smith, G. & Yard, J. Quantum communication with zero-capacity channels. *Science* **321,** 1812–1815 (2008).

Acknowledgements

Part of this work was done when the authors attended the programme 'Mathematical Challenges in Quantum Information', August–December 2013, at the Isaac Newton Institute for Mathematical Sciences, Cambridge, whose hospitality is gratefully acknowledged. M.C. was with ETH Zurich and visiting the Centre for Quantum Information and Foundations, DAMTP, University of Cambridge, during part of this work. We thank Gláucia Murta for pointing out an error in an earlier version of the manuscript. K.H. thanks Michał and Paweł Horodecki and Jonathan Oppenheim for helpful discussions. M.C. was supported by a DFF Sapere Aude grant, an ERC Starting Grant, the CHIST-ERA project 'CQC', an SNSF Professorship, the Swiss NCCR 'QSIT' and the Swiss SBFI in relation to COST action MP1006. K.H. acknowledges support by the ERC Advanced Grant 'QOLAPS' and the National Science Centre project Maestro DEC-2011/02/A/ST2/00305. A.W. was supported by the Spanish MINECO, projects FIS2013-40627-P and FIS2008-01236 with the support of FEDER funds, the Generalitat de Catalunya CIRIT project 2014 SGR 966, the EC STREP 'RAQUEL' and the Philip Leverhulme Trust. A.W. and S.B. were supported by the ERC Advanced Grant 'IRQUAT'.

Author contributions

All authors contributed to defining the formalism and to obtaining the main results of the paper. M.C. and K.H. focused on the distinguishability bound, S.B. and A.W. on bounding the entanglement of the output state.

Additional information

Supplementary Information accompanies this paper at http://www.nature.com/naturecommunications

Competing financial interests: The authors declare no competing financial interests.

Reprints and permission information is available online at http://npg.nature.com/reprintsandpermissions/

How to cite this article: Bäuml, S. *et al.* Limitations on quantum key repeaters. *Nat. Commun.* 6:6908 doi: 10.1038/ncomms7908 (2015).

© 2015 Macmillan Publishers Limited. All rights reserved.