Limitations on Quantum Key Repeaters

Stefan Bäuml, Matthias Christandl, Karol Horodecki, and Andreas Winter

(Dated: September 10, 2014)

A major application of quantum communication is the distribution of entangled particles for use in quantum key distribution [1–3] (QKD). Due to unavoidable noise in the communication line, QKD is in practice limited to a distance of a few hundred kilometers [4–6], and can only be extended to longer distances by use of a so-called quantum repeater [7, 8], a device which performs iterated entanglement distillation and quantum teleportation. The existence of entangled particles that are undistillable but nevertheless useful for QKD [9] raises the question of the feasibility of a *quantum key repeater*, which would work beyond the limits of entanglement distillation, hence possibly tolerating much higher noise than existing protocols. Here, we show that any such apparatus is severely limited in its performance; in particular, we exhibit entanglement suitable for QKD but unsuitable for the most general conceivable quantum key repeater protocol. Our results are in the form of general bounds on the rate at which secure key can be obtained by such protocols. The mathematical techniques we develop may be seen as a step towards opening the theory of entanglement measures to networks of communicating parties. A technical version of this work is available at [10].

When a signal is passed from a sender to a receiver, it inevitably degrades due to the noise present in any realistic communication channel (e.g. 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 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 (e.g. encoded in non-orthogonal polarisations of a single photon), such an amplifier cannot work anymore, since the measurement inevitably disturbs the signal [11]. Sending a quantum mechanical signal, however, is the basis of quantum key distribution, a method to distribute a cryptographic key which can later be used for perfectly secure communication between sender and receiver [1]. 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 [5, 6].

A way around this limitation is the use of entanglement-based quantum key distribution schemes [2, 3] in conjunction with a so-called quantum repeater [7]. 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. 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 [12]. 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 and more repeater stations can be inserted to efficiently extend the distance arbitrarily. The implementation of quantum repeaters is therefore one of the focal points of experimental quantum information science [8].

Due to the tight connection between the distillation of EPR pairs and QKD [13, 14], it came as a surprise that there are bound entangled states (i.e. entangled states with $E_D = 0$) from which secret key can be obtained (i.e. the distillable key satisfies $K_D > 0$) [9]. 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*. More formally, 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. By a private bit we mean an entangled state containing a unit of privacy paralleling the EPR pair as a unit of entanglement [9, 15]. Mathematically, a private bit is given by a density matrix $\gamma_{AA'BB'}$ with four subsystems A, A' and B, B'. A and B are the qubits that contain the key bits and A' and B' are d-dimensional systems, called shield systems. Moreover, each private bit is represented by an operator X which is a d^2 by d^2 matrix with $\|X\|_1 = 1$.

Note that just as the definition of the distillable key [9, 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 information to the eavesdropper. We also note that 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.

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]. 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. Here, the distinguishability can easily be bounded by $\|X^\Gamma\|_1 = \frac{1}{\sqrt{d}}$, where Γ indicates the partial transpose, that is, the transpose of one of the systems [23]. 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. 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 [9]. This implies an LOCC procedure for Alice & 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 quantum key repeater protocol (see Section III.B of[10]).

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 $\tilde{\rho}$ (see Section III.C of [10]):

$$K_{A\leftrightarrow C\leftrightarrow B}(\rho_{AC_A} \otimes \tilde{\rho}_{C_BB}) \leq D^{\infty}_{C\leftrightarrow AB}(\rho_{AC_A} \otimes \tilde{\rho}_{C_BB}), \tag{1}$$

where the RHS is the regularised LOCC-restricted relative entropy distance to the closest separable state [24]. Observing invariance of this bound under partial transposition, we obtain for states remaining positive under partial transposition (PPT) a bound in terms of the regularised relative entropy of entanglement of their partially transposed version ρ^Γ: $E^{\infty}_R(\rho^\Gamma) + E^{\infty}_R(\tilde{\rho}^\Gamma)$. If we restrict to forward communication from Charlie and $\rho_{AC_A} = \tilde{\rho}_{BC_B}$, squashed entanglement provides a bound: $K_{A\leftarrow C\rightarrow B}(\rho_{AC_A} \otimes \tilde{\rho}_{C_BB}) \leq 4E_{sq}(\rho^\Gamma)$. Using invariance under partial transposition directly on the hypothetical quantum key repeater protocol, we obtain for PPT states ρ and $\tilde{\rho}$ (see Section

III.A of [10]):

$$K_{A\leftrightarrow C\leftrightarrow B}(\rho_{AC_A}\otimes\tilde{\rho}_{C_BB})\leq K_D(\rho^{\Gamma}_{AC_A})\leq\min\{E^{\infty}_R(\rho^{\Gamma}_{AC_A}),E_{sq}(\rho^{\Gamma}_{AC_A})\}. \tag{2}$$

We will now give an example of a state $\rho_{AC_A}=\tilde{\rho}_{BC_B}$ 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 (no private bit can be PPT [9]). 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 quantum key distribution at small distances but that are virtually useless for long-distance quantum key distribution.

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 (see Section III.D of [10]):

$$K_{A\leftarrow C\leftrightarrow B}(\rho_{AC_A}\otimes\tilde{\rho}_{C_BB})\leq\frac{1}{2}E_C(\rho_{AC_A})+\frac{1}{2}E_D(\tilde{\rho}_{C_BB}). \tag{3}$$

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 (3) is obtained by upper bounding the squashed entanglement of the output state of the protocol using a manipulation of entropies resulting in the RHS of (3). The squashed entanglement in turn upper bounds the distillable key of the output state (which upper bounds the LHS) [25].

The preceding results pose limitations on the entanglement of the output state of a quantum key repeater protocol. As such, they support the PPT^2 *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 [26–28]. Reaching even further, and consistent with our findings, we may speculate that perhaps the only "transitive" entanglement in quantum states, i.e. entanglement that survives a quantum key repeater, is the distillable entanglement. One may also wonder whether there are inequalities between the entanglement of in- and output for other entanglement measures. In the context of algebro-geometric measures, this question has been raised and relations for the concurrence have been found [29, 30]. As our work focuses on operational entanglement measures, we investigated the tightness (3) and, based on a random construction, showed that the LHS cannot be replaced by the entanglement cost of the output state.

With this paper we initiate a study of long-distance quantum communication and cryptography beyond the use of entanglement distillation. 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.

---

[1] Charles H. Bennett and Gilles Brassard. Quantum Cryptography: Public Key Distribution and Coin Tossing. In *Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing*, pages 175–179, Bangalore, India, December 1984, 1984. IEEE Computer Society Press, New York.

[2] A. K. Ekert. Quantum cryptography based on Bell's theorem. *Phys. Rev. Lett.*, 67(6):661–663, 1991.

[3] Charles H. Bennett, Gilles Brassard, and N. David Mermin. Quantum cryptography without Bell's theorem. *Phys. Rev. Lett.*, 68:557–559, Feb 1992.

[4] Damien Stucki, Nino Walenta, Fabien Vannel, Robert Thomas Thew, Nicolas Gisin, Hugo Zbinden, S. Gray, C. R. Towery, and S. Ten. High rate, long-distance quantum key distribution over 250 km of ultra low loss fibres. *New J. Phys.*, 11(7):075003, 2009.

[5] Nicolas Gisin, Grégoire Ribordy, Wolfgang Tittel, and Hugo Zbinden. Quantum cryptography. *Rev. Mod. Phys.*, 74:145–195, Mar 2002.

[6] Valerio Scarani, Helle Bechmann-Pasquinucci, Nicolas J. Cerf, Miloslav Dušek, Norbert Lütkenhaus, and Momtchil Peev. The security of practical quantum key distribution. *Rev. Mod. Phys.*, 81(3):1301, 2009.

[7] H.-J. Briegel, W. Dür, J. I. Cirac, and P. Zoller. Quantum repeaters: The role of imperfect local operations in quantum communication. *Phys. Rev. Lett.*, 81:5932–5935, 1998.

[8] Nicolas Sangouard, Christoph Simon, Hugues De Riedmatten, and Nicolas Gisin. Quantum repeaters based on atomic ensembles and linear optics. *Rev. Mod. Phys.*, 83(1):33, 2011.

[9] K. Horodecki, M. Horodecki, P. Horodecki, and J. Oppenheim. Secure key from bound entanglement. *Phys. Rev. Lett.*, 94:160502, 2005.

[10] Stefan Bäuml, Matthias Christandl, Karol Horodecki, and Andreas Winter. Limitations on quantum key repeaters. *arXiv preprint arXiv:1402.5927*, 2014.

[11] Christopher A. Fuchs and Asher Peres. Quantum-state disturbance versus information gain: Uncertainty relations for quantum information. *Phys. Rev. A*, 53:2038–2045, Apr 1996.

[12] M. Żukowski, A. Zeilinger, M. A. Horne, and A. K. Ekert. Event-ready-detectors, Bell experiment via entanglement swapping. *Phys. Rev. Lett.*, 71(26):4287–4290, 1993.

[13] David Deutsch, Artur Ekert, Richard Jozsa, Chiara Macchiavello, Sandu Popescu, and Anna Sanpera. Quantum Privacy Amplification and the Security of Quantum Cryptography over Noisy Channels. *Phys. Rev. Lett.*, 77:2818–2821, Sep 1996.

[14] Peter W. Shor and John Preskill. Simple Proof of Security of the BB84 Quantum Key Distribution Protocol. *Phys. Rev. Lett.*, 85:441–444, Jul 2000.

[15] K. Horodecki, M. Horodecki, P. Horodecki, and J. Oppenheim. General paradigm for distilling classical key from quantum states. *IEEE Trans. Inf. Theory*, 55:1898, 2009.

[16] I. Devetak and A. Winter. Distillation of secret key and entanglement from quantum states. *Proc. R. Soc. Lond. A*, 461:207–235, 2005.

[17] Matthias Christandl, Robert König, and Renato Renner. Postselection technique for quantum channels with applications to quantum cryptography. *Phys. Rev. Lett.*, 102:020504, Jan 2009.

[18] Renato Renner and Robert König. Universally composable privacy amplification against quantum adversaries. In Joe Kilian, editor, *Theory of Cryptography*, volume 3378 of *Lecture Notes in Computer Science*, pages 407–425. Springer Berlin Heidelberg, 2005.

[19] Michael Ben-Or, Micha Horodecki, DebbieW. Leung, Dominic Mayers, and Jonathan Oppenheim. The universal composable security of quantum key distribution. In Joe Kilian, editor, *Theory of Cryptography*, volume 3378 of *Lecture Notes in Computer Science*, pages 386–406. Springer Berlin Heidelberg, 2005.

[20] D. Unruh. Simulatable security for quantum protocols. 2004.

[21] K. Horodecki, M. Horodecki, P. Horodecki, D. Leung, and J. Oppenheim. Quantum key distribution based on private states: unconditional security over untrusted channels with zero quantum capacity. *IEEE Trans. Inf. Theory*, 54(6):2604–2620, 2008.

[22] K. Horodecki. *General paradigm for distilling classical key from quantum states — On quantum entanglement and security.* PhD thesis, University of Warsaw, 2008.

[23] K. Horodecki, Ł. Pankowski, M. Horodecki, and P. Horodecki. Low dimensional bound entanglement with one-way distillable cryptographic key. *IEEE Trans. Inf. Theory*, 54:2621, 2008.

[24] M. Piani. Relative Entropy of Entanglement and Restricted Measurements. *Phys. Rev. Lett.*, 103(16):160504, October 2009.

[25] Matthias Christandl, Norbert Schuch, and Andreas Winter. Entanglement of the antisymmetric state. *Commun. Math. Phys.*, 311:397–422, 2012.

[26] M Christandl. PPT square conjecture (problem G). In *Banff International Research Station workshop: Operator structures in quantum information theory*, 2012.

[27] S. Bäuml. On bound key and the use of bound entanglement. Diploma thesis, Ludwig Maximilians Universität München, Munich, Germany, 2010.
[28] A. Hansen. Swapped Bound Entanglement. Master thesis, ETH Zurich, 2013.
[29] Gilad Gour. Mixed-state entanglement of assistance and the generalized concurrence. *Phys. Rev. A*, 72:042318, Oct 2005.
[30] Soojoon Lee, Jeong San Kim, and Barry C Sanders. Distribution and dynamics of entanglement in high-dimensional quantum systems using convex-roof extended negativity. *Phys. Lett. A*, 375(3):411–414, 2011.