# Limitations on quantum privacy swapping

Stefan Bäuml,[1,2,*] Matthias Christandl,[3] and Andreas Winter[4,2,1,5]

[1]*Department of Mathematics, University of Bristol, Bristol BS8 1TW, U.K.*

[2]*Física Teòrica: Informació i Fenomens Quàntics,*

*Universitat Autònoma de Barcelona, ES-08193 Bellaterra (Barcelona), Spain*

[3]*Institute for Theoretical Physics, ETH Zürich, 8093 Zürich, Switzerland*

[4]*ICREA - Institució Catalana de Recerca i Estudis Avançats, ES-08010 Barcelona, Spain*

[5]*Centre for Quantum Technologies, National University of Singapore, 3 Science Drive 2, Singapore 117543*

(Dated: June 13, 2013)

Maximally entangled states are an important resource in quantum information protocols such as quantum key distribution (QKD) [1] or teleportation [2]. Another application is *entanglement swapping* [3], a protocol involving three parties, Alice, Charlie and Bob. Alice and Charlie initially share a maximally entangled state. A second maximally entangled state is shared between Charlie and Bob who are equipped with a classical line of communication, as well. If Charlie and Bob then use their state and the classical line to teleport Charlie's part of the state he shares with Alice to Bob, Alice and Bob end up with a maximally entangled state, with no need of having interacted. Entanglement swapping is an essential ingredient in a quantum repeater [4], which is necessary to distribute maximally entangled states over long absorptive channels, such as optical fibers: As absorption usually scales exponentially with the length of the channel, states cannot simply be sent through an arbitrarily long channel. Instead, maximally entangled states are first distributed over short segments of the channel. The final state is obtained by repeated entanglement swapping steps between the nodes. Apart from maximally entangled states, entanglement swapping has also been studied for Werner states [4]. It has been shown that the singlet fraction decreases exponentially with the number of steps, requiring entanglement distillation before each swapping operation, a technique called nested purification. Examples of mixed states where distillation is not necessary in order to maintain entanglement have also been discovered [5, 6].

An important application of quantum repeaters is the distribution of maximally or nearly maximally entangled states between distant parties who then extract cryptographic key from them. However, it has been shown [7] that maximally entangled states are not the only states that can be used for that purpose. In fact, there exists a much larger class of so called *private states* which

*Electronic address: stefan.baeuml@bristol.ac.uk

can serve as a source of key. Surprisingly there exist bound entangled states that are arbitrarily close to private states in trace distance [7]. This shows that privacy is a truly different property of a quantum state than its distillable entanglement, motivating the definition of a quantity known as *distillable key* ($K_D$)[7], which is defined in the same way as distillable entanglement but with the maximally entangled state replaced by a private state.

A natural question arising now is how such nearly bound entangled private states can be distributed between distant parties. Of course it would be possible to distribute maximal entanglement using a conventional repeater and then distill the state needed. This would, however, have no advantage over using the maximal entanglement directly for QKD. Here, we deal with the question whether there are other, not maximally entangled, possibly even bound entangled states that could be initially distributed between the nodes and then swapped yielding a state useful for cryptography. We call this *quantum privacy swapping*. The question of swapability of bound entangled states has been addressed before [8, 9]. In the following, we consider a protocol where Alice and Charlie initially share a state $\rho^1_{AC_1}$ and Charlie and Bob share a state $\rho^2_{C_2B}$. Charlie and Bob then perform a general LOCC protocol, during which Charlie's subsystems are being discarded, resulting in a state $\tau_{A\tilde{B}}$ shared by Alice and Bob. Alice's subsystem remains untouched during the protocol. Note that this is a generalisation of the entanglement swapping protocol described above. Our main result is an upper bound on the classical squashed entanglement [10] of $\tau_{A\tilde{B}}$, which in turn is an upper bound on the distillable key [11, 12]. Namely

$$K_D(\tau_{A\tilde{B}}) \leq E_{sq,c}(\tau_{A\tilde{B}}) \leq \frac{1}{2}E_D(\rho^2_{C_2B}) + \frac{1}{2}E_F(\rho^1_{AC_1}) \tag{1}$$

If the protocol performed by Charlie and Bob is limited to Charlie performing a POVM on $C_1C_2$ and classically communicating the result to Bob who then performs some local operation on his subsystem, we can also show that

$$K_D(\tau_{A\tilde{B}}) \leq E_{sq,c}(\tau_{A\tilde{B}}) \leq \frac{1}{2}E_D^{C_1\to A}(\rho^1_{AC_1}) + \frac{1}{2}E_F(\rho^2_{C_2B}) \tag{2}$$

where $E_D^{C_1\to A}$ describes the one way distillable entanglement. Hence, if we intend to use $\tau$ for QKD, bound entangled input states have to be 'compensated for' by a large entanglement of formation of the other input state.

Let us now give an example of a state where our results provide a significant reduction of the key rate. Assume that $\rho^1_{AC_1}$ and $\rho^2_{C_2B}$ are *flag states* as introduced in [13]:

$$\rho^{\text{flag}}_{ABA'B'} = \frac{1}{2}|\Phi^+\rangle\langle\Phi^+|_{AB} \otimes \sigma^+_{A'B'} + \frac{1}{2}|\Phi^-\rangle\langle\Phi^-|_{AB} \otimes \sigma^-_{A'B'} \tag{3}$$

where $\sigma^{\pm}$ are the separable *hiding states* [17] introduced in [14]. In [15], it was shown that, as $\sigma^{\pm}$ are almost orthogonal, $K_D(\rho^{\text{flag}}) \approx 1$ but $E_D(\rho^{\text{flag}})$ almost vanishes. The intuition behind this is that, instead of bits, the entanglement is 'hidden' away from LOCC observers. Since $\sigma^{\pm}$ are separable, $\rho^{\text{flag}}$ can be obtained from $|\Phi^+\rangle\langle\Phi^+|$ by LOCC, hence $E_F(\rho^{\text{flag}}) \leq 1$. By our results, swapping results in a state with distillable key at most slightly larger than $\frac{1}{2}$, which is a significant reduction.

In conclusion, we have provided an upper bound on the distillable key of states resulting from entanglement swapping. In case of a bound entangled input state, this bound is given by half the entanglement of formation of the other input state, which can be seen as a limitation on the use of bound entangled states in a privacy swapping protocol. Further investigation might either yield a stronger result, showing that the key rate always decreases when bound entangled input states are used as input or provide examples bound entangled states that can be used for privacy swapping.

---


[1] A.K. Ekert. Quantum cryptography based on Bells theorem. *PRL*, 67(6):661–663, 1991.

[2] C.H. Bennett, G. Brassard, C. Crepeau, R. Jozsa, A. Peres, and W.K. Wootters. Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels. *PRL*, 70(13):1895–1899, 1993.

[3] M. Żukowski, A. Zeilinger, MA Horne, and AK Ekert. Event-ready-detectors, Bell experiment via entanglement swapping. *PRL*, 71(26):4287–4290, 1993.

[4] W. Dür, H.J. Briegel, JI Cirac, and P. Zoller. Quantum repeaters based on entanglement purification. *PRA*, 59(1):169–181, 1999.

[5] J. Modławska and A. Grudka. Increasing singlet fraction with entanglement swapping. *PRA*, 78(3):032321, Sep 2008.

[6] A. Sen, U. Sen, Č. Brukner, V. Bužek, and M. Żukowski. Entanglement swapping of noisy states: A kind of superadditivity in nonclassicality. *PRA*, 72(4):42310, 2005.

[7] K. Horodecki, M. Horodecki, P. Horodecki, and J. Oppenheim. Secure key from bound entanglement. *PRL*, 94(16):160502, 2005.

[8] M. Christandl and K. Horodecki. 2009. unpublished.

[9] S. Bäuml. On bound key and the use of bound entanglement. Diploma thesis, 2010, Ludwig Maximilians Universität, Munich, Germany.

[10] R.R. Tucci. Entanglement of distillation and conditional mutual information. *arXiv preprint quant-ph/0202144*, 2002.

[11] M. Christandl and A. Winter. Squashed entanglement: An additive entanglement measure. *Journal of Mathematical Physics*, 45:829, 2004.

[12] M. Christandl. The structure of bipartite quantum states-Insights from group theory and cryptography. *Arxiv preprint quant-ph/0604183*, 2006.

[13] K. Horodecki, M. Horodecki, P. Horodecki, and J. Oppenheim. General paradigm for distilling classical key from quantum states. *IEEE Transactions on Information Theory*, 55(4):1898, 2009.

[14] T. Eggeling and RF Werner. Hiding classical data in multipartite quantum states. *PRL*, 89(9):97905, 2002.

[15] K. Horodecki. General paradigm for distilling classical key from quantum states-on quantum entanglement and security. *PhD thesis*, 2008. Available at https://www.mimuw.edu.pl/wiadomosci/aktualnosci/doktoraty/pliki/karol_horodecki/doktorat-kh.pdf.

[16] D.P. DiVincenzo, D.W. Leung, and B.M. Terhal. Quantum data hiding. *Information Theory, IEEE Transactions on*, 48(3):580–598, 2002.

[17] A pair of bipartite states $\sigma^{\pm}_{AB}$ is called (perfect) hiding states, if they are (perfectly) distinguishable by global operations but (completely) indistinguishable by LOCC operations. They have this name because in a state of the form $\rho_{bAB} = \frac{1}{2}|0\rangle\langle 0|_b \otimes \sigma^{+}_{AB} + \frac{1}{2}|1\rangle\langle 1|_b \otimes \sigma^{-}_{AB}$, the bit $b$ is hidden away from LOCC observers. The concept of data hiding was introduced by [16].