Entanglement Cost of Quantum Channels

Mario Berta and Matthias Christandl
Institute for Theoretical Physics
ETH Zurich
8093 Zurich, Switzerland

Fernando G.S.L. Brandao
Departamento de Fisica
Universidade Federal de Minas Gerais
Belo Horizonte 30123-970, Brazil

Stephanie Wehner
Centre for Quantum Technologies
National University of Singapore
117543 Singapore

***Abstract*—A natural question in characterizing the information theoretic power of quantum channels is to ask at what rate entanglement is needed in order to asymptotically simulate a quantum channel in the presence of free classical communication. We call this the entanglement cost of a channel, and prove a formula describing it for all channels. We discuss two applications. Firstly, we are able to link the security in the noisy-storage model to a problem of sending quantum rather than classical information through the adversary's storage device. This not only greatly improves the range of parameters where security could be shown previously, but allows us to prove security for storage devices for which no non-trivial statements were known before. Secondly, our result has consequences for the study of the strong converse quantum capacity. Here, we show that any coding scheme that sends quantum information through a quantum channel at a rate larger than the entanglement cost of the channel has an exponentially small fidelity.**

I. Introduction

One of the most fundamental problems in quantum information theory is to quantify the information theoretic power of quantum channels. Of particular interest is thereby the study of a channel's capacity for information transmission. This quantity tells us how many bits m we can send reliably when using the channel n times, using the best possible encoding and decoding process. Unlike classical channels, quantum channels have various distinct capacities. These depend, among other things, on what kind of information should be sent over the channel (e.g. classical or quantum) or on what kind of assistance is allowed (e.g. free entanglement or free classical communication). Important examples of quantum channel capacities include the entanglement assisted classical capacity C_E [1], and the classical forward communication assisted quantum capacity $Q_{\rightarrow}$ [2], [3], [4]. The first deals with sending classical information over a quantum channel in the presence of freely usable entanglement. The latter deals with the problem of sending quantum information itself, when we are allowed free classical communication from the sender to the receiver. One way of tackling the problem of capacities is to think more broadly in terms of one channel simulating another. For example, the process of sending m bits reliably using n uses of a channel $\mathcal{E}$ can be understood as a simulation of m perfect, noise-free, channels using n copies of $\mathcal{E}$. The capacity of the channel $\mathcal{E}$ is then simply the rate m/n at which such a simulation is possible in the limit of large n. Instead of simulating a perfect channel from some noisy channel, one can also approach the problem from the other end. In particular, we can ask what is the optimal asymptotic rate at which a perfect channel can simulate some noisy one? When our simulation can consume free entanglement between the sender and the receiver, this question is answered by the quantum reverse Shannon theorem. It states that the rate is given by the entanglement assisted classical capacity C_E [5], [6]. Apart from its deep conceptual appeal, the quantum reverse Shannon theorem led to the proof that C_E is in fact a strong converse capacity; a concept which we discuss in more detail below.

II. Main Result

It is a natural question to ask what happens to such a simulation in the presence of other resources. In this work, we ask what is the optimal asymptotic rate at which a perfect quantum channel can simulate some noisy quantum channel $\mathcal{E}$ in the presence of free classical communication? We note that it does not matter if we allow free classical forward, backward, or even two-way communication; the optimal asymptotic rate turns out to be the same in all scenarios. The problem be understood as the 'reverse problem' for the classical communication assisted quantum capacities. Note that by quantum teleportation [7], the perfect quantum channel can equivalently be replaced with perfect entanglement. The central question of this paper can thus be summarized as

At what rate is entanglement needed in order to asymptotically simulate a quantum channel $\mathcal{E}$, when classical communication is given for free?

We call this rate the entanglement cost E_C of a quantum channel. Our main contribution in this paper is to prove the following formula

$$E_C(\mathcal{E}) = \lim_{n\to\infty} \frac{1}{n} \max_{\psi^n} E_F\left(\left(\mathcal{E}^{\otimes n} \otimes \mathcal{I}\right)(\psi^n)\right) \ , \qquad (1)$$

where the maximization is over all purifications ψ^n of input states to the n-fold tensor product quantum channel $\mathcal{E}^{\otimes n}$, $\mathcal{I}$ stands for the identity channel on the purifying system, and E_F denotes the entanglement of formation defined as

$$E_F(\rho_{AB}) = \inf_{\{p_i,\rho^i\}} \sum_i p_i H(A)_{\rho^i} \ , \qquad (2)$$

where the infimum ranges over all pure state decompositions $\rho_{AB} = \sum_i p_i |\rho^i\rangle\langle\rho^i|_{AB}$, and $H(.)$ denotes the von Neumann entropy. As with the known formula for the classical forward communication assisted quantum capacity, Equation (1) involves a regularization, and hence is not a single-letter formula. Note that even if we would know that we can restrict the maximization to non-entangled input states, Equation (1) would still not be a single-letter formula, due to Hasting's counterexample for the additivity of the entanglement of formation [8], [9]. However, we want to emphasize that we can compute explicit upper bounds for E_C, which are particularly useful for the applications given below. The entanglement cost is in general larger than the classical communication assisted quantum capacities, which is in contrast to the case of free entanglement (where the rate is C_E for both, the channel capacity and the reverse problem). Hence, simulating the perfect channel from a noisy one and then again the noisy channel, results in a net loss.

As the name entanglement cost suggests, $E_C(\mathcal{E})$ can be seen as the channel analogue of the entanglement cost of quantum states $E_C(\rho)$, which is defined as the optimal asymptotic rate of entanglement that is needed in order to create a quantum state ρ in the iid scenario using local operations and classical communication [10], [11]. It is known that

$$E_C(\rho) = \lim_{n\to\infty} \frac{1}{n} E_F(\rho^{\otimes n}) \ , \tag{3}$$

where E_F again denotes the entanglement of formation. In the state problem, it is interesting to compare the entanglement cost $E_C(\rho)$ with the distillable entanglement $E_D(\rho)$, which is the optimal asymptotic rate at which perfect entanglement can be distilled in the iid scenario using local operations and classical communication [12]. As it turns out, there are quantum states with $E_C(\rho) > E_D(\rho)$, and even with $E_D(\rho) = 0$ but $E_C(\rho) > 0$. These states are called bound entangled [13]. The corresponding quantum channel problem is then to compare $E_C(\mathcal{E})$ with e.g. $Q_{\rightarrow}(\mathcal{E})$, since by teleportation, $Q_{\rightarrow}(\mathcal{E})$ is actually the same as the entanglement generating capacity $E_{\rightarrow}(\mathcal{E})$ [2]. And indeed there are bound entangled quantum channels, e.g. all channels with positive partial transpose (PPT [14], [15]) but entangled Choi-Jamiolkowski state, because then $E_C(\mathcal{E}) > 0$ but $Q_{\rightarrow}(\mathcal{E}) = 0$. In further analogy with the state problem, we can also show that $E_C(\mathcal{E})$ is zero if and only if $\mathcal{E}$ is entanglement breaking.

III. Proof idea

We use one-shot information theory to derive our main result Equation (1). In contrast to the usual assumption of asymptotic iid resources in quantum information theory, one-shot information theory applies to arbitrary (structureless) resources. In the asymptotic iid regime many operational quantities can be expressed in terms of a few information measures based on the von Neumann entropy. The same holds true for the one-shot case by means of the smooth entropy formalism [16], [17], [18], [19], [20], [21], [22]. We work in this smooth entropy formalism and our proof is conceptually very similar to the proof of the quantum reverse Shannon theorem given in [6]. In order to prove the direct part of Equation (1), we need to show the existence of a channel simulation for $\mathcal{E}^{\otimes n}$, whose asymptotic rate of entanglement consumption is upper bounded by $E_C(\mathcal{E})$. That is, we need to construct a completely positive and trace preserving (CPTP) map that is asymptotically arbitrarily close to $\mathcal{E}^{\otimes n}$ in the diamond norm (which is the dual of the completely bounded norm [23]), and that consists only of using maximally entangled states at an asymptotic rate of at most $E_C(\mathcal{E})$, local operations, and classical communication. Here it is worth to note that even though the channel to simulate $\mathcal{E}^{\otimes n}$ has iid structure, the channel simulation also has to work on non-iid inputs (and this is also the reason why Equation (1) does not just easily follow from Equation (3)). The crucial idea is to employ the post-selection technique for quantum channels [24], which is a tool to bound the distance in diamond norm between two completely positive and trace preserving (CPTP) maps that act symmetrically on an n-partite system. The technique upper bounds this distance by the distance arising from the purification of a special de Finetti input state. That is, the purification of a state which consists of n identical and independent copies of an (unknown) state on a single subsystem. Note that this purification does not have iid structure. But now it is sufficient to find a CPTP map that creates the state given by $\mathcal{E}^{\otimes n}$ applied to the purification of the special de Finetti input state. It then remains to quantify how much entanglement is needed in order to create this state. Since this state does not have iid structure, we employ the one-shot entanglement cost for quantum states $E_C^{(1)}(\rho_{AB}, \varepsilon)$, which quantifies how much entanglement is needed in order to create one single copy of a bipartite quantum state ρ_{AB} up to an error $\varepsilon \geq 0$ using local operations and classical communication [25], [26]. Note that this is in contrast to the quantity $E_C(\rho_{AB})$ mentioned before, which answers the question of how much entanglement is needed in the asymptotic iid regime. The resulting asymptotic entanglement cost of the channel simulation is then upper bounded by an expression close to Equation (1), but with the maximization over input states and the minimization in the definition of the entanglement of formation interchanged. Finally, in order to arrive at Equation (1), we discretize the set of Kraus decompositions of $\mathcal{E}$ and apply Sion's minimax theorem [27].

IV. Applications and Examples

We present two applications of our formula for the entanglement cost of channels and calculate some examples of interest. We start with the problem of proving security in the noisy storage model and then turn to the problem of deriving bounds for the strong converse of quantum capacities.

A. Security in the Noisy Storage Model

As a first application we discuss security in the noisy-storage model [28], [29], [30]. For the first time, we relate security in this model to a problem of sending quantum rather than classical information through the adversary's storage device. In particular, we show that any two-party cryptographic

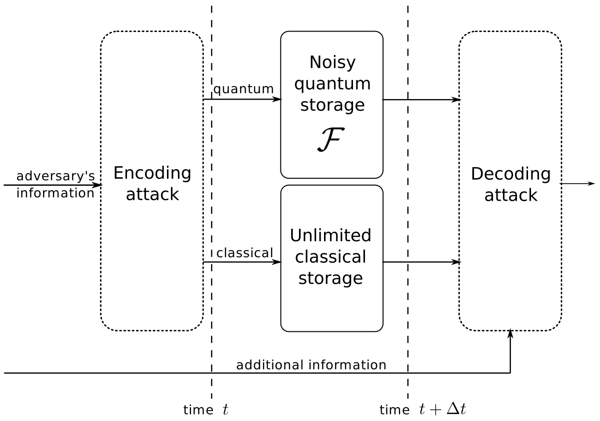

Fig. 1. Noisy-storage assumption: During waiting times Δt, the adversary can only use his noisy memory device to store quantum information. However, he is otherwise all powerful, and storage of classical information is free.

primitive can be implemented securely whenever

$$E_C(\mathcal{E}) \cdot \nu < \frac{1}{2} \ , \tag{4}$$

where the adversary's storage is of the form $\mathcal{E}^{\otimes \nu \cdot m}$, m is the number of qubits transmitted during the protocol, and ν is the storage rate (see Fig. 1). We can compute bounds for various channels of interest by means of our non-regularized achievability result for the entanglement cost

$$E_C(\mathcal{E}) \leq E_C^1(\mathcal{E}) = \max_{\psi} E_F\left(\left(\mathcal{E} \otimes \mathcal{I}\right)(\psi)\right) \ , \tag{5}$$

which simplifies for qubit channels to the explicit form

$$E_C^1(\mathcal{E}) = h\left(\frac{1}{2} + \frac{1}{2} \cdot \sqrt{1 - C^2\left(\left(\mathcal{E} \otimes \mathcal{I}\right)(\phi)\right)}\right) \ , \tag{6}$$

where $h(.)$ denotes the binary Shannon entropy, $C(.)$ the concurrence (see [31], [32]), and ϕ is the maximally entangled state between the input and the purifying system. Our analysis not only greatly improves the range of parameters when security can be obtained, we also obtain non-trivial bounds for dephasing noise, and can find bounds for the security for any qubit channel such as amplitude damping noise (see Fig. 2-4).

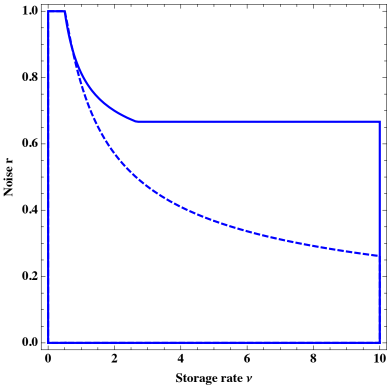

Fig. 2. Depolarizing channel. Security was previously known below the dashed line. Now for (r, ν) inside the solid line.

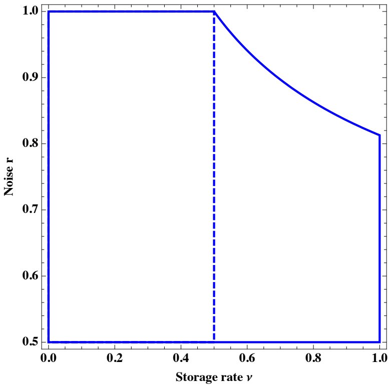

Fig. 3. Dephasing channel. Before security was no better than for bounded storage, left of dashed line. Now for (r, ν) inside the solid line.

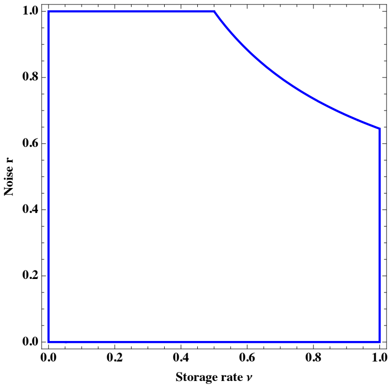

Fig. 4. Amplitude damping channel. No security statement was known previously. Now for (r, ν) inside the solid line.

B. Upper Bound on the Strong Converse Quantum Capacity

To determine a quantum channel's capacity for sending information, two aspects need to be addressed. First of all, one needs to show that the capacity can be achieved. That is, there exists some coding scheme that allows to transmit information reliably at any rate up to the capacity. Second, however, the capacity should really form a threshold for information transmission. That is, if one tries to send information at a rate above the capacity, then there exists no coding scheme that allows to send information without any error. Such a statement is also known as a weak converse. This however, does not yet exclude the possibility of sending information with a small error at a rate that exceeds the capacity. The minimal rate for which the success in transmitting information drops exponentially with the number of channel uses, is known as the strong converse capacity. The strong converse capacity is appealing since it really gives a sharp threshold for information transmission. But to determine the strong converse capacity forms a challenge even when it comes to sending classical information. Only when restricted to non-entangled input states [33], [34] or certain classes of quantum channels [35], it is known that the strong converse classical capacity is actually the same as the classical capacity. However, upper bounds on the strong converse classical capacity are known [5], [36], [37]. For example, the quantum reverse Shannon theorem shows that the entanglement assisted classical capacity C_E and its strong converse version are identical [5]. Of course C_E is then also an upper bound on the unassisted strong converse classical capacity. In addition, the result immediately implies that the entanglement assisted quantum capacity $Q_E = C_E/2$ and its strong converse version are identical. Thus, Q_E is an upper bound on the unassisted strong converse quantum capacity.

The second application of our result is a new upper bound to the strong converse capacity for sending quantum information. Similar to the quantum reverse Shannon theorem, we employ the idea of a channel simulation to prove that when we send quantum information at a rate exceeding E_C, the error rate is lower bounded by

$$\varepsilon_n \geq 1 - 2^{-O(n)} \ . \tag{7}$$

Our bound holds for all channels $\mathcal{E}$ and the two-way classical communication assisted quantum capacity $Q_{\leftrightarrow}$ (and with that also for $Q_{\rightarrow}$). We note that he bound E_C is independent of Q_E and can in general be stronger or weaker. As an example we mention the qubit dephasing channel $\mathcal{E}_{\text{deph}}(\rho) = (1-p)\rho + p \cdot \sigma_z \rho \sigma_z$ with $\sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$, for which we get

$$Q_{\rightarrow}(\mathcal{E}_{\text{deph}}) = 1 - h(p) \tag{8}$$

$$E_C^1(\mathcal{E}_{\text{deph}}) = h\left(\frac{1}{2} + \sqrt{p(1-p)}\right) \tag{9}$$

$$Q_E(\mathcal{E}_{\text{deph}}) = 1 - \frac{1}{2} \cdot h(\frac{p}{2}) \ , \tag{10}$$

where $h(.)$ denotes the binary Shannon entropy. As shown in Fig. 5 this is far from being tight, but we are not aware of any better better bounds on the strong converse quantum capacity. In addition, note that $Q_{\leftrightarrow}$ can be much larger than $Q_{\rightarrow}$ and we conclude with the following upper bound, which holds for every qubit channel

$$Q_{\leftrightarrow}(\mathcal{E}) \leq h\left(\frac{1}{2} + \frac{1}{2} \cdot \sqrt{1 - C^2\left(\left(\mathcal{E} \otimes \mathcal{I}\right)(\phi)\right)}\right) \ , \tag{11}$$

where ϕ is the maximally entangled state between the input and the purifying system.

V. Conclusion and Outlook

We calculated the rate of entanglement needed in order to asymptotically simulate a quantum channel when classical communication is for free. Because of the free classical communication, the problem is equivalent to the question about the rate of quantum communication needed in order to simulate a quantum channel. A natural subsequent question is to ask what rate of classical communication is actually needed. However, in the spirit about general quantum channel simulations, we might even want to ask more generally about rate triples (q, e, c) needed in order to achieve the channel simulation, where q denotes quantum communication, e entanglement, and c classical communication. The quantum reverse Shannon theorem can then be understood as e.g. $(Q_E, \infty, 0)$ or $(0, \infty, C_E)$ (to be precise, the entanglement has to be given in the form of so-called embezzling states [38], [5]), whereas our entanglement cost corresponds to e.g. $(0, E_C, \infty)$ or $(E_C, 0, \infty)$. Some more examples are discussed in [5, Figure 2] and a particularly interesting case is the following. For $e = 0$, $c = 0$, and product state inputs, the channel simulation can be done for [5, Theorem 3]

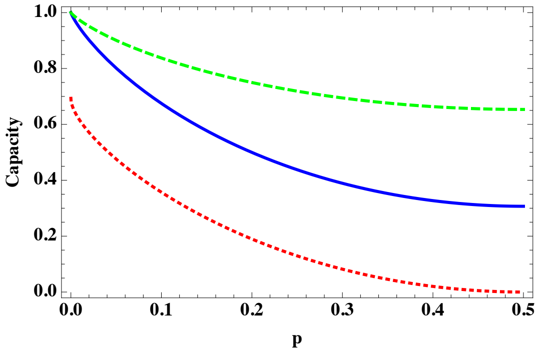

Fig. 5. The qubit dephasing channel with dephasing parameter p - quantum capacity Q (dotted line) vs. upper bound E_C^1 on the entanglement cost (solid line) vs. entanglement assisted quantum capacity Q_E (dashed line).

$$q = \lim_{n\rightarrow\infty} \frac{1}{n} E_P\left(\left(\mathcal{E} \otimes \mathcal{I}\right)(\phi)^{\otimes n}\right) \tag{12}$$

with ϕ the maximally entangled state between the input and the purifying system, and E_P the entanglement of purification [39]

$$E_P(\rho_{AB}) = \min_{\rho_{AA'BB'}:\mathrm{tr}_{A'B'}[|\rho\rangle\langle\rho|_{AA'BB'}]=\rho_{AB}} E_F(\rho_{AA'BB'}) \ . \tag{13}$$

Now one could hope to generalize this to a channel simulation for general input states using the techniques presented above, leading to

$$q = \lim_{n\rightarrow\infty} \frac{1}{n} \max_{\psi^n} E_P\left(\left(\mathcal{E}^{\otimes n} \otimes \mathcal{I}\right)(\psi^n)\right) \ , \tag{14}$$

where the maximization is over all purifications ψ^n of input states to the n-fold tensor product quantum channel $\mathcal{E}^{\otimes n}$, and $\mathcal{I}$ stands for the identity channel on the purifying system. However, this does not work for same reason as the quantum reverse Shannon theorem can not be proven for general input states using only maximally entangled states; an issue known as entanglement spread [5], [40], [41], [42].

Another interesting open question concerns the relation of $E_C(\mathcal{E})$ and $Q_{\rightarrow}(\mathcal{E})$. We know that $E_C(\mathcal{E}) \geq Q_{\rightarrow}(\mathcal{E})$, with the inequality typically being strict. Can we obtain a characterization of channels for which $E_C(\mathcal{E}) = Q_{\rightarrow}(\mathcal{E})$? This is an analogue of the problem of characterizing bipartite states for which the distillable entanglement is equal the entanglement cost, which is still wide open.

Note added. After completion of this work, security in the noisy storage model was linked to the strong converse quantum capacity of the adversary's storage device [43]. This means that our bound on the strong converse from Section IV-B can also be applied directly to calculate rates for security. However, our arguments from Section IV-A apply to virtually any form of the noisy storage model, whereas the results from [43] are only applicable for the so-called six-state encoding.

Acknowledgment

We acknowledge discussions with Jonathan Oppenheim, Michael Walter, Reinhard Werner, Mark Wilde, and Andreas Winter. MB and MC are supported by the SNF (grant PP00P2-128455), the DFG (grants CH 843/1-1 and CH 843/2-1), and the National Centre of Competence in Research 'Quantum Science and Technology'. FB and SW are supported by the National Research Foundation and the Ministry of Education, Singapore. FB is supported by a 'Conhecimento Novo' fellowship from the Brazilian agency FAPEMIG. MB, FB and SW would like to thank the Institut Mittag-Leffler (Djursholm, Sweden), where part of this work was done.

References

[1] C. H. Bennett, P. W. Shor, J. A. Smolin, and A. V. Thapliyal, "Entanglement-assisted capacity of a quantum channel and the reverse Shannon theorem," *IEEE Transactions on Information Theory*, vol. 48, p. 2637, 2002, arXiv:quant-ph/0106052v2.

[2] I. Devetak, "The private classical capacity and quantum capacity of a quantum channel," *IEEE Transactions on Information Theory*, vol. 51, p. 44, 2005, arXiv:quant-ph/0304127v6.

[3] P. W. Shor, "The quantum channel capacity and coherent information," *Lecture notes, MSRI Workshop on Quantum Computation*, 2002.

[4] S. Lloyd, "Capacity of the noisy quantum channel," *Physics Review A*, vol. 55, p. 1613, 1997, arXiv:quant-ph/9604015v2.

[5] C. H. Bennett, I. Devetak, A. W. Harrow, P. W. Shor, and A. Winter, "The quantum reverse Shannon theorem," 2009, arXiv:0912.5537v2.

[6] M. Berta, M. Christandl, and R. Renner, "The quantum reverse Shannon theorem based on one-shot informationtheory," *Communications in Mathematical Physics*, vol. 306, no. 3, pp. 579–615, 2011, arXiv:0912.3805v2.

[7] C. H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres, and W. K. Wootters, "Teleporting an unknown quantum state via dual classical and einstein-podolsky-rosen channels," *Physical Review Letters*, vol. 70, p. 1895, 1993.

[8] M. B. Hastings, "A counterexample to additivity of minimum output entropy," *Nature Physics*, vol. 5, p. 255, 2009, arXiv:0809.3972v4.

[9] P. W. Shor, "Equivalence of additivity questions in quantum information theory," *Communications in Mathematical Physics*, vol. 3, pp. 453–472, 2004, arXiv:quant-ph/0305035v4.

[10] P. M. Hayden, M. Horodecki, and B. T. Terhal, "The asymptotic entanglement cost of preparing a quantum state," *Journal of Physics A*, vol. 34, pp. 6891–6898, 2001, arXiv:quant-ph/0008134v1.

[11] C. H. Bennett, D. P. DiVincenzo, J. A. Smolin, and W. K. Wootters, "Mixed state entanglement and quantum error correction," *Physical Review A*, vol. 54, pp. 3824–3851, 1996, arXiv:quant-ph/9604024v2.

[12] I. Devetak and A. Winter, "Distillation of secret key and entanglement from quantum state," *Proceedings of Royal Society A*, vol. 461, p. 207, 2005, arXiv:quant-ph/0306078v1.

[13] M. Horodecki, P. Horodecki, and R. Horodecki, "Mixed-state entanglement and distillation: is there a "bound" entanglement in nature?" *Physical Review Letters*, vol. 80, p. 5239, 1998, arXiv:quant-ph/9801069v1.

[14] A. Peres, "Separability criterion for density matrices," *Physical Review Letters*, vol. 77, pp. 1413–1415, 1996, arXiv:quant-ph/9604005v2.

[15] M. Horodecki, P. Horodecki, and R. Horodecki, "Separability of mixed states: necessary and sufficient conditions," *Physics Letters A*, vol. 223, pp. 1–8, 1996, arXiv:quant-ph/9605038v2.

[16] R. Renner, "Security of quantum key distribution," *International Journal of Quantum Information*, vol. 6, p. 1, 2008, arXiv:quant-ph/0512258v2.

[17] R. Renner and S. Wolf, "Smooth Rényi entropy and applications," *Proceedings of IEEE International Symposium Information Theory*, p. 233, 2004.

[18] R. Renner and R. König, "Universally composable privacy amplification against quantum adversaries," *Springer Lecture Notes in Computer Science*, vol. 3378, p. 407, 2005, arXiv:quant-ph/0403133v2.

[19] R. König, R. Renner, and C. Schaffner, "The operational meaning of min- and max-entropy," *IEEE Transactions on Information Theory*, vol. 55, no. 9, pp. 4674–4681, 2009, arXiv:0807.1338v1.

[20] M. Tomamichel, R. Colbeck, and R. Renner, "A fully quantum asymptotic equipartition property," *IEEE Transactions on Information Theory*, vol. 55, pp. 5840–5847, 2009, arXiv:0811.1221v3.

[21] ——, "Duality between smooth min- and max-entropies," *IEEE Transactions on Information Theory*, vol. 56, p. 4674, 2010, arXiv:0907.5238v2.

[22] N. Datta, "Min- and max- relative entropies and a new entanglement monotone," *IEEE Transactions on Information Theory*, vol. 55, no. 6, p. 2816, 2009, arXiv:0803.2770v3.

[23] A. Kitaev, "Quantum computations: algorithms and error correction," *Russian Mathematical Surveys*, vol. 52, p. 1191, 1997.

[24] M. Christandl, R. König, and R. Renner, "Post-selection technique for quantum channels with applications to quantum cryptography," *Physics Review Letters*, vol. 102, p. 020504, 2009, arXiv:0809.3019v1.

[25] F. Buscemi and N. Datta, "Entanglement cost in practical scenarios," *Physical Review Letters*, vol. 106, p. 130503, 2011, arXiv:0906.3698v3.

[26] M. Hayashi, *Quantum Information: An Introduction*. Springer, 2006.

[27] M. Sion, "On general minimax theorems," *Pacific Journal of Mathematics*, vol. 8, p. 171, 1958.

[28] S. Wehner, C. Schaffner, and B. Terhal, "Cryptography from noisy storage," *Physical Review Letters*, vol. 100, p. 220502, 2008, arXiv:0711.2895v3.

[29] R. König, S. Wehner, and J. Wullschleger, "Unconditional security from noisy quantum storage," *IEEE Transactions on Information Theory - To appear*, 2009, arXiv:0906.1030v4.

[30] I. B. Damgård, S. Fehr, L. Salvail, and C. Schaffner, "Cryptography in the Bounded-Quantum-Storage Model," in *Proceedings of 46th IEEE FOCS*, 2005, pp. 449–458, arXiv:quant-ph/0508222v2.

[31] B. D. M. F. Verstraete, J. Dehaene, "Local filtering operations on two qubits," *Phys. Rev. A*, vol. 64, p. 010101, 2000, arXiv:quant-ph/0011111v1.

[32] T. Konrad, F. de Melo, M. Tiersch, C. Kasztelan, A. Aragao, and A. Buchleitner, "A factorization law for entanglement decay," *Nature Physics*, vol. 4, pp. 99–102, 2008, arXiv:0708.0180v3.

[33] A. Winter, "Coding theorem and strong converse for quantum channels," *IEEE Transactions on Information Theory*, vol. 45, no. 7, pp. 2481–2485, 1999.

[34] T. Ogawa and H. Nagaoka, "Strong converse to the quantum channel coding theorem," *IEEE Transactions on Information Theory*, vol. 45, no. 7, pp. 2486–2489, 1999, arXiv:quant-ph/9808063v2.

[35] R. König and S. Wehner, "A strong converse for classical channel coding using entangled inputs," *Physical Review Letters*, vol. 103, p. 070504, 2009, arXiv.org:quant-ph/0903.2838v1.

[36] N. Datta, M. Hsieh, and F. Brandão, "Strong converse rates and an example of violation of the strong converse property," 2011, arXiv:1106.3089v1.

[37] T. Dorlas and C. Morgan, "The invalidity of a strong capacity for a quantum channel with memory," 2011, arXiv:1108.4282v1.

[38] W. van Dam and P. Hayden, "Universal entanglement transformations without communication," *Physics Review A*, vol. 67, p. 060302(R), 2003, arXiv:quant-ph/0201041v1.

[39] B. M. Terhal, M. Horodecki, D. W. Leung, and D. P. DiVincenzo, "The entanglement of purification," *Journal of Mathematical Physics*, vol. 43, pp. 4286–4298, 2002, arXiv:quant-ph/0202044v3.

[40] A. W. Harrow, "Entanglement spread and clean resource inequalities," *Proceedings of 16th International Congress Mathematical Physics*, 2009, arXiv:0909.1557v1.

[41] P. Hayden and A. Winter, "On the communication cost of entanglement transformations," *Physical Review A*, vol. 67, p. 012326, 2003, arXiv:quant-ph/0204092v3.

[42] A. W. Harrow and H.-K. Lo, "A tight lower bound on the classical communication cost of entanglement dilution," *IEEE Transactions on Information Theory*, vol. 50, no. 2, pp. 319–327, 2004, arXiv:quant-ph/0204096v2.

[43] M. Berta, O. Fawzi, and S. Wehner, "Quantum to classical randomness extractors," 2011, arXiv:1111.2026v1.