Private information via the Unruh effect

JHEP08(2009)074

(http://iopscience.iop.org/1126-6708/2009/08/074)

Published by IOP Publishing for SISSA

Received: *June 25, 2009*
Accepted: *July 16, 2009*
Published: *August 20, 2009*

Private information via the Unruh effect

Kamil Brádler, Patrick Hayden and Prakash Panangaden

School of Computer Science, McGill University,
Montréal, Canada
E-mail: kbradler@cs.mcgill.ca, patrick@cs.mcgill.ca,
prakash@cs.mcgill.ca

Abstract: In a relativistic theory of quantum information, the possible presence of horizons is a complicating feature placing restrictions on the transmission and retrieval of information. We consider two inertial participants communicating via a noiseless qubit channel in the presence of a uniformly accelerated eavesdropper. Owing to the Unruh effect, the eavesdropper's view of any encoded information is noisy, a feature the two inertial participants can exploit to achieve perfectly secure quantum communication. We show that the associated private quantum capacity is equal to the entanglement-assisted quantum capacity for the channel to the eavesdropper's environment, which we evaluate for all accelerations.

Keywords: Field Theories in Lower Dimensions, Statistical Methods, Space-Time Symmetries, Quantum Dissipative Systems

ArXiv ePrint: 0807.4536

doi:10.1088/1126-6708/2009/08/074

Contents

Quantum information theory for the most part assumes that the senders, receivers and eavesdroppers involved in a protocol share an inertial frame. For many of the applications envisioned in the field this is a good approximation and sometimes, as in the case of quantum key distribution, even a rigorously justifiable simplification. To the extent that quantum information theory attempts to identify fundamental rules governing information processing imposed by the laws of physics , however, neglecting relativity is ultimately unacceptable. Luckily, much of the formalism of quantum information remains valid in relativistic settings and the effect of changing reference frames can usually be modeled as the introduction of noise. Thus, there has been a significant amount of work done to calculate how entanglement degrades under a boost or acceleration [1–6] and how basic quantum information theoretic protocols like teleportation, which were designed for inertial participants, break down under acceleration [7].

The natural next step is to design communications protocols specifically adapted to relativistic situations and, possibly, take advantage of uniquely relativistic features to accomplish otherwise impossible tasks. Kent has demonstrated, for example, that secure bit commitment is possible using a protocol exploiting relativistic causality constraints even though it is known to be impossible otherwise [8]. In this article, we consider a scenario in which two inertial participants communicate via a noiseless, bosonic, dual-rail qubit channel in the presence of a uniformly accelerated eavesdropper. In this context, the eavesdropper's Unruh noise becomes a resource which the inertial participants can potentially exploit to encrypt their communications.

The *private quantum capacity* is the optimal rate at which a sender (Alice) can send *qubits* to a receiver (Bob) while keeping them private from an eavesdropper (Eve). It had not previously been studied because in most settings it is redundant to require privacy in quantum communication: if the eavesdropper is modeled as being part of the environment of the communications channel then quantum communication is automatically private. This was in fact the insight behind Devetak's proof of the quantum capacity theorem [9]. On the other hand, if Eve is assumed to have unrestricted access to the states while they are in transit from Alice to Bob, then unconditional privacy is impossible without secret keys in a nonrelativistic model because Eve and Bob are effectively interchangeable. This symmetry is broken, however, if Eve is assumed to be accelerating. The private quantum capacity problem therefore provides an example of a question which is poorly motivated in non-relativistic settings but very natural when relativity is taken into account. Because of structural features of the Unruh effect, this private quantum capacity is exactly zero if Alice is restricted to isometric encodings. However, for general encodings it is given by the same formula as the entanglement-assisted quantum capacity [10] of the channel to the eavesdropper's environment, despite the absence of any operational connection between the two problems. Of course, it is also possible to define a private classical capacity for this setting, which we study for the purposes of comparison with its quantum version.

1 Unruh channels

The Unruh effect, whereby an observer uniformly accelerated in a vacuum experiences a thermal bath [11, 12], can be understood as a consequence of the fact that an accelerated observer has a different Fock representation of the quantum field than does an inertial observer. In particular, the vacuum state as defined by an inertial observer will be a thermal state in the Fock space defined by a uniformly accelerating observer. The transformation between these Fock spaces is conveniently represented by a transformation of creation and annihilation operators called a Bogoliubov transformation [13].

Consider a state $|\psi\rangle$ of a quantum field. The inertial observers may see this as a many particle state: $\Pi_i a_i^\dagger |\mathsf{vac}\rangle$. The Bogoliubov transformation changes each a_i to some combination of the creation and annihilation operators of the non-inertial observer's Fock decomposition. In our case, the Bogoliubov transformation, which relates the Fock decompositions in the Minkowski and Rindler spacetimes corresponding respectively to the inertial and accelerating observers, has a very special form because of the spacetime symmetries. The only mixing of modes is between the modes with the same momentum in the two Rindler wedges. The *Unruh channel* $\mathcal{N}$ consists of this change composed with tracing over the modes that are inaccessible to the accelerating observer because they are beyond her horizon.

We will assume that Alice encodes information for Bob by preparing quantum states of a bosonic, dual-rail qubit as illustrated in figure 1. In other words, she has access to a two-dimensional sector of her (and Bob's) Fock space, with basis vectors given by a single excitation of a massless scalar field in one of two different modes, which we label by their associated annihilation operators a and b.[1] $U_{ac}(r) = \exp[r(a^\dagger c^\dagger - ac)]$ is the unitary operator transforming the sector of Alice's Fock space to the corresponding sector of Eve's Fock space. (Because the Bogoliubov transformation is diagonal, we can safely ignore all other modes [16, p. 106].) In short, the channel is U_{ac} followed by the appropriate trace.

[1] Throughout the paper, we work with plane wave modes which are not, strictly speaking, physically realizable. Nonetheless, the superpositions involved in defining a wave packet can be carried through our calculations using approximate mode matching because the Bogoliubov transformation does not mix modes. As a result, explicit calculations using wave packets do not lead to substantial differences for our purposes [14, 15].

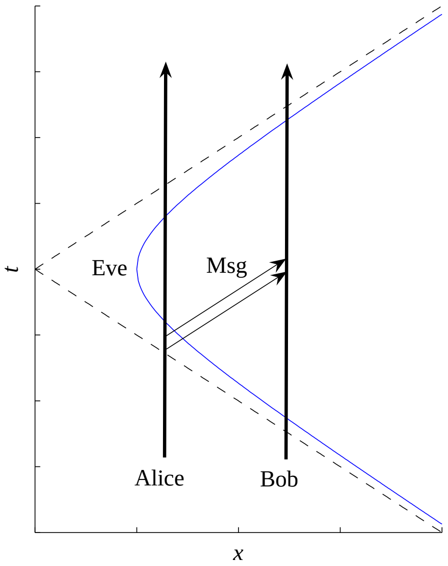

Figure 1. Spacetime diagram of the communication scenario. Alice and Bob are inertial observers, assumed without loss of generality to be at rest. Meanwhile, Eve is uniformly accelerated resulting in future and past horizons indicated by the dashed lines $x = \pm t$. Eve intercepts a message sent from Alice to Bob but will be thwarted in her attempts to determine the contents even though the only restrictions considered on Eve's ability to perform quantum measurements are those arising from the presence of the horizons.

The parameter r is related to Eve's proper acceleration τ and the mode frequency ω by $\tanh r = \exp(-\pi\omega/\tau)$ [7, 13].

In our dual-rail case, an arbitrary pure input state $|\psi\rangle = (\alpha b^\dagger + \beta a^\dagger)\,|\mathsf{vac}\rangle$ is transformed to Eve's Fock space according to $U_{abcd} = U_{ac} \otimes U_{bd}$, which expands to

$$U_{abcd}(r) = \tfrac{1}{\cosh^2 r} e^{\tanh r (a^\dagger c^\dagger + b^\dagger d^\dagger)} \times e^{-\ln\cosh r (a^\dagger a + b^\dagger b + c^\dagger c + d^\dagger d)} e^{-\tanh r (ac+bd)}. \tag{1.1}$$

For all states in the dual-rail basis, equation (1.1) reduces to $U_{abcd}(r) = 1/\cosh^3 r \exp\left[\tanh r (a^\dagger c^\dagger + b^\dagger d^\dagger)\right]$. This allows us to write the state in Eve's Fock space as $|\psi\rangle = U_{abcd}(r)(\alpha b^\dagger + \beta a^\dagger)\,|\mathsf{vac}\rangle = (\alpha b^\dagger + \beta a^\dagger) U_{abcd}(r)\,|\mathsf{vac}\rangle$. If we trace over degrees of freedom beyond Eve's horizon (cd), then $\sigma = \mathcal{N}(|\psi\rangle\langle\psi|) = (1-z)^3 \bigoplus_{k=0}^{\infty} z^k\, \sigma_k$ is block diagonal with blocks σ_k labeled by the total excitation number k $(z = \tanh^2 r)$:

$$\sigma_k = \sum_{n=0}^{k} \Big[|\alpha|^2 (n+1) |k-n, n+1\rangle\langle k-n, n+1| + |\beta|^2 (k-n+1) |k-n+1, n\rangle\langle k-n+1, n| \\ + \alpha\bar{\beta}\sqrt{(n+1)(k-n+1)}\, |k-n, n+1\rangle\langle k-n+1, n| + h.c. \Big]. \tag{1.2}$$

Each block σ_k can be expressed as a linear combination of generators $J_x^{(k+2)}$, $J_y^{(k+2)}$ and $J_z^{(k+2)}$ of the irreducible $(k+2)-$dimensional representation of SU(2). ($\vec{J}^{(2)}$, for example, consists of the Pauli matrices scaled by 1/2.) If $\sigma = \mathcal{N}(\rho)$ with $\rho = \mathbb{I}/2 + \vec{n} \cdot \vec{J}^{(2)}$ arbitrary, then

$$\sigma_k = \mathbb{I}(k+1)/2 + n_x J_x^{(k+2)} + n_y J_y^{(k+2)} + n_z J_z^{(k+2)}. \tag{1.3}$$

As a consequence, the channel $\mathcal{N}$ to Eve is covariant in the sense that $\mathcal{N}(U\rho U^\dagger) = R(U)\mathcal{N}(\rho)R(U^\dagger)$ where R is the infinite dimensional representation of SU(2) given by the direct sum over all its finite dimensional irreps. This makes it easy to diagonalize σ: the eigenvalues of σ_k are equally spaced with spacing $S = \|\vec{n}\|_2$ and largest eigenvalue equal to $(k+1)(S+1)/2$.

2 Private quantum capacity

Capacities are defined by allowing arbitrarily many uses of a channel and asking that the various data transmission or privacy requirements hold to any desired level of approximation in the limit of many uses. The private quantum capacity is defined as the optimal rate at which Alice can send qubits to Bob while simultaneously ensuring that those qubits appear to be completely encrypted from Eve's point of view. There are several equivalent ways of formalizing this notion, but we will take it to mean that Alice would like to transmit halves of entangled pairs to Bob. Privacy in this context means that there should be no correlation between the output of Eve's channel and the halves of the entangled pairs kept in Alice's laboratory. Since the private quantum capacity has not been studied elsewhere, we begin by providing some formal definitions and studying the general case.

Given are a quantum channel $\mathcal{N}_1$ from Alice to Bob and another $\mathcal{N}_2$ from Alice to Eve. Let Φ_{2^k} represent the density operator of k maximally entangled pairs of qubits and τ_{2^k} the maximally mixed state on k qubits. An (n, k, δ, ϵ) *private entanglement transmission code* from Alice to Bob consists of an encoding channel $\mathcal{E}$ taking k qubits into the input of $\mathcal{N}_1^{\otimes n}$ and a decoding channel $\mathcal{D}$ taking the output of Bob's channel $\mathcal{N}_1^{\otimes n}$ back to k qubits satisfying

1. *Transmission:*
   $\left\|(\mathrm{id} \otimes \mathcal{D} \circ \mathcal{N}_1^{\otimes n} \circ \mathcal{E})(\Phi_{2^k}) - \Phi_{2^k}\right\|_1 \leq \delta.$
2. *Privacy:*
   $\left\|(\mathrm{id} \otimes \mathcal{N}_2^{\otimes n} \circ \mathcal{E})(\Phi_{2^k}) - \tau_{2^k} \otimes (\mathcal{N}_2^{\otimes n} \circ \mathcal{E})(\tau_{2^k})\right\|_1 \leq \epsilon.$

A rate Q is an *achievable* rate for private entanglement transmission if for all $\delta, \epsilon > 0$ and sufficiently large n there exist $(n, \lfloor nQ \rfloor, \delta, \epsilon)$ private entanglement transmission codes. The private quantum capacity is the supremum of the achievable rates. For a density operator σ^{AB}, let $H(A)_\sigma$ be the von Neumann entropy of σ^A. The mutual information $I(A;B)_\sigma$ is $H(A)_\sigma + H(B)_\sigma - H(AB)_\sigma$.

Theorem 1 *The private quantum capacity $Q_p(\mathrm{id}, \mathcal{N})$ when the channel from Alice to Bob is noiseless is given by the formula $\max \frac{1}{2} I(A; E_c)_\rho$, where the maximization is over all pure states $|\varphi\rangle^{AA'}$ and $\rho = (\mathrm{id} \otimes \mathcal{N}_c)(\varphi)$. $\mathcal{N}_c$ is the channel to Eve's environment E_c, that is, the complement of $\mathcal{N}$ with respect to its isometric dilation.*

Despite the absence here of any entanglement assistance, the theorem implies that $Q_p(\mathrm{id}_2, \mathcal{N})$ is exactly equal to the entanglement-assisted quantum capacity of $\mathcal{N}_c$, usually written $Q_E(\mathcal{N}_c)$ [10].

To see that the advertised rate is achievable, write $V_{\mathcal{E}}$ for the isometric extension of $\mathcal{E}$, with output on $A'^n F$. The privacy condition applied to $\mathcal{N}$ is equivalent to entanglement transmission to FE_c^n via Uhlmann's theorem [17]. It is therefore sufficient to find codes that simultaneously perform entanglement transmission to Bob and to FE_c^n. The encodings analyzed in [18] do not depend on the channels, however, just the dummy input φ, so the same encodings can be employed for both tasks. Choosing $|F| = 2^{nf}$, the following sufficient conditions for successful transmission can be extracted from [18, 19]:

$$Q < H(A)_\varphi - f \quad \text{and} \quad Q < I(A\rangle E_c)_\rho + f, \tag{2.1}$$

where $I(A\rangle E_c)_\rho$ is the coherent information $H(E_c)_\rho - H(AE_c)_\rho$. These constraints have intuitive interpretations: the first is the noiseless rate to Bob through $V_{\mathcal{E}}$ reduced by the rate at which qubits are lost to F, while the second is the standard coherent information rate for $\mathcal{N}_c$ augmented by a noiseless channel to F. Q is maximized subject to these constraints when $H(A)_\varphi - f = I(A\rangle E_c)_\rho + f$. Using the fact that $H(A)_\varphi = H(A)_\rho$ and purifying ρ to $|\rho\rangle^{AEE_c}$, this equation can be written as $f = \frac{1}{2}I(A;E)_\rho$. Therefore, the rate Q is achievable provided $Q < H(A)_\rho - \frac{1}{2}I(A;E)_\rho = \frac{1}{2}I(A;E_c)_\rho$.

To prove optimality, suppose we have an $(n, \lfloor nQ \rfloor, \delta, \epsilon)$ private entanglement transmission code. Use R to denote the reference space for the maximally entangled state Φ_{2^k} in the definition. Let $|\sigma\rangle^{RFE^nE_c^n}$ be the purified final state after $\mathcal{N}_2^{\otimes n} \circ \mathcal{E}$ has acted on Φ_{2^k}. The privacy condition and the Alicki-Fannes' inequality [20] imply that there is a function $g(\delta)$ satisfying $\lim_{\delta \to 0} g(\delta) = 0$ such that

$$\begin{aligned} 2\lfloor nQ \rfloor = 2\log|R| &\leq I(R;E_c^n F)_\sigma + ng(\delta) \\ &= I(R;F)_\sigma + I(R;E_c^n|F)_\sigma \\ &\leq I(R;E_c^n|F)_\sigma + ng(\delta+\epsilon) \\ &\leq I(RF;E_c^n)_\sigma + ng(\delta+\epsilon). \end{aligned} \tag{2.2}$$

The first inequality is a consequence of the existence of the decoding channel $\mathcal{D}$ and the monotonicty of mutual information. The second inequality holds because entanglement transmission to Bob requires no leakage to F, leading to an upper bound on $I(R;F)_\sigma$. The final inequality follows from the chain rule and the nonnegativity of mutual information. Labeling RF by A, we can conclude that

$$Q_p(\mathrm{id}, \mathcal{N}) \leq \lim_{n\to\infty} \max \frac{1}{2n} I(A;E_c^n)_\rho, \tag{2.3}$$

where the maximization is pure states $|\varphi\rangle^{A^nA'^n}$ and $\rho = (\mathrm{id} \otimes \mathcal{N}_c^{\otimes n})(\varphi)$. It is well-known, however, that fixing $n = 1$ does not affect the expression on the right hand side of the inequality [10], finishing the proof of optimality.

2.1 Unruh case

Let us now focus on the the case where $\mathcal{N}$ is the Unruh channel. Inspection of figure 1 reveals that there is only a finite amount of time during which Eve can intercept messages from Alice to Bob. The limit $n \to \infty$ of infinite length messages considered in the definition of the private classical capacity therefore does not formally apply, but codes nearly achieving the capacity can be found for reasonably small n.

It is instructive to first consider encodings $\mathcal{E}$ that are isometric, a restriction that does not affect the regular (non-private) quantum capacity. Private entanglement transmission codes then simply become codes that transmit entanglement beyond Eve's horizon to E_c.

Taking the partial trace over (ab) instead of (cd) of the pure state $|\psi\rangle$ from Eve's Fock space yields the channel $\mathcal{N}_c$ from Alice to E_c, the Hilbert space describing degrees of freedom beyond Eve's horizon. The result is

$$\mathcal{N}_c(\rho) = z\,\bar{\sigma} + (1-z)\,\omega_0, \tag{2.4}$$

where $\sigma = \mathcal{N}(\rho)$ and ω_0 is a diagonal state independent of ρ. Therefore, given the output σ to her channel, Eve can simulate the channel to E_c up to complex conjugation. The simulation is simple. With probability z she does nothing to σ and with probability $1-z$ she prepares ω_0 and uses it to replace σ.

Now suppose that it is possible to transmit entanglement (and therefore quantum states) beyond Eve's horizon. Write $\mathcal{D}(\tau) = \sum_j D_j \tau D_j^\dagger$ for the decoding channel on E_c. Since $\bar{\mathcal{D}}(\tau) = \sum_j \bar{D}_j \tau \bar{D}_j^\dagger$ is also a quantum channel, Eve can apply $\bar{\mathcal{D}}$ to the output of her simulation. Assuming high fidelity transmission of a quantum state $|\psi\rangle$ beyond Eve's horizon, the output of $\bar{\mathcal{D}}$ will be a high fidelity transmission of $|\bar{\psi}\rangle$. That is impossible because the map $|\psi\rangle \mapsto |\psi\rangle\,|\bar{\psi}\rangle$, the result of applying both decodings in parallel, is nonlinear. The only possible conclusion is that it must be impossible to transmit entanglement beyond Eve's horizon. It is therefore impossible to achieve private entanglement transmission using isometric codes.

Releasing the restriction, however, yields a non-zero capacity. In fact, because $I(A;E_c)_\rho$ in Theorem 1 is a concave function of $\varphi^{A'}$ and the Unruh channel is covariant, the maximum will be achieved with $\varphi^{A'}$ maximally mixed. Evaluating the formula yields a compact expression for $Q_p(\mathrm{id}, \mathcal{N})$ which we have plotted in figure 2:

$$\frac{1}{2}\left(1 - \frac{(1-z)^3}{2}\frac{\partial^2}{\partial z^2}\frac{\partial}{\partial s}\left[(z-1)\mathrm{Li}\,(s,z)\right]_{s=0}\right), \tag{2.5}$$

where $\mathrm{Li}\,(s,z)$ is the polylogarithm function.

3 Private classical capacity

Define the private classical capacity $C_p(\mathcal{N}_1, \mathcal{N}_2)$ as the optimal rate, measured in bits per channel use, at which Alice can send classical data to Bob over the channel $\mathcal{N}_1$ in such a way that Eve is incapable of distinguishing the messages based on her view, the output of the channel $\mathcal{N}_2$. This definition generalizes the notion of private classical capacity introduced in [9], which corresponds to the special case where $\mathcal{N}_2$ is the complement of $\mathcal{N}_1$.

Using the methods of that paper and some additional arguments, one can show that $C_p(\mathrm{id}_2, \mathcal{N}) = \lim_{n\to\infty} C_p^{(n)}(\mathrm{id}_2, \mathcal{N})$, where $C_p^{(n)}(\mathrm{id}_2, \mathcal{N})$ is

$$1 - H\big(\mathcal{N}(I/2)\big) + \max_{|\psi_n\rangle}\frac{1}{n}H\big(\mathcal{N}^{\otimes n}(|\psi_n\rangle\langle\psi_n|)\big) \tag{3.1}$$

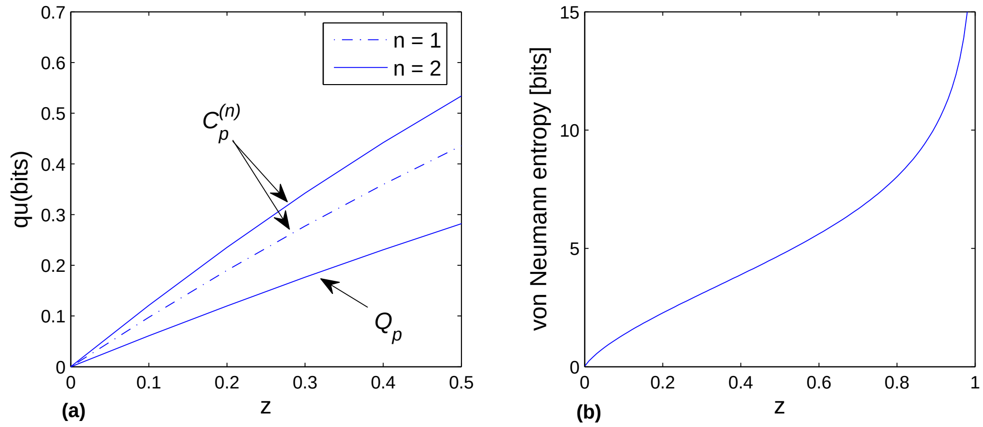

Figure 2. **(a)** The private quantum capacity $Q_p(\mathrm{id}_2, \mathcal{N})$ is non-zero for all positive accelerations and strictly less than $C_p^{(n)}$ for all n, which give successively better lower bounds on the private classical capacity. **(b)** $H(\mathcal{N}(|\psi_1\rangle\langle\psi_1|))$, the entropy of the output state for a pure input or, equivalently, the entanglement between Eve's output and Eve's environment. This is an intermediate quantity required in the evaluation of $C_p^{(1)}$ and was also the focus of [7], where it was approximated by diagonalizing the $k = 0, 1$ blocks of equation (1.2). Using our methods, it can be shown that the exact value of the entanglement is $-3\left[z \ln z/(1-z) + \ln(1-z)\right] + (1-z)^2 \frac{\partial}{\partial z}\frac{\partial}{\partial s}\mathrm{Li}\,(s,z)\,|_{s=0}$ nats.

and $|\psi_n\rangle$ is any pure input state to n copies of the channel. Evaluating the capacity therefore reduces to determining the maximal output entropy of the Unruh channels $\mathcal{N}^{\otimes n}$ for pure input states. The optimization for $n = 1$ is trivial due to the covariance of $\mathcal{N}$ and gives that $C_p(\mathrm{id}_2, \mathcal{N})$ is bounded below by

$$C_p^{(1)}(\mathrm{id}_2, \mathcal{N}) \;=\; (1-z)^2 \frac{\partial}{\partial z}\left[\frac{\partial}{\partial s}\mathrm{Li}\,(s,z)\,|_{s=0}\right] - \frac{(1-z)^3}{2}\frac{\partial^2}{\partial z^2}\left[z\frac{\partial}{\partial s}\mathrm{Li}\,(s,z)\,|_{s=0}\right]. \quad (3.2)$$

We plot these bounds for $n = 1, 2$ in figure 2.

4 Conclusions

The assumption that an eavesdropper is accelerating can be exploited to send data securely for all non-zero accelerations. In the case of the private quantum data, we found a single-letter formula for the capacity for general eavesdropper channels, demonstrating it to be equal to the entanglement-assisted quantum capacity of the channel to the eavesdropper's environment. We leave it as an open question to explain why these seemingly unrelated tasks should have matching capacity formulas but note that in light of [21], these are now the only channel capacity problems in quantum information that can be considered fully solved.[2] In the case of private classical data transmission, the problem of calculating the associated private classical capacity reduces to that of determining the maximal output

[2] There is also a remarkable formula for the so-called environment-assisted quantum capacity of a quantum channel [22] but that problem is of a very different type since it assumes full control of the channel's environment, nearly the opposite of what is normally meant by a noisy channel.

entropy of the Unruh channel for pure input states. This entropy corresponds to the entanglement between Rindler field modes accessible to the eavesdropper and those not accessible, a question of independent interest [7] resolved in this paper.

When evaluating the private quantum capacity with an accelerating eavesdropper, we began by considering isometric encodings, a class known to be sufficient for non-private quantum data transmission. With this restriction, private quantum data transmission reduces to sending entanglement beyond the eavesdropper's horizon. An argument related to the impossibility of cloning demonstrates this to be impossible, an observation reminiscent of the analysis in [23, 24], where the interplay of the no-cloning theorem and horizons was used to place self-consistency constraints on the black hole complementarity principle. We ended by evaluating the private quantum capacity for unrestricted encodings, finding a compact expression for the capacity which is non-zero for all positive accelerations, in sharp contrast to no-go result for isometric encoders.

Acknowledgments

The authors thank John Preskill for reminding us of the dangers of preliminary calculations and Jon Yard for helpful conversations. This work was supported financially by the Canada Research Chairs program, CIFAR, FQRNT, MITACS, the Office of Naval Research Basic Research Challenges program, NSERC, QuantumWorks and the Sloan Foundation.

References

[1] M. Czachor and M. Wilczewski, *Relativistic Bennett-Brassard cryptographic scheme, relativistic errors, and how to correct them*, *Phys. Rev.* **A 68** (2003) 010302 [quant-ph/0303077]

[2] A. Peres and D.R. Terno, *Quantum information and relativity theory*, *Rev. Mod. Phys.* **76** (2004) 93 [quant-ph/0212023] [SPIRES].

[3] R.M. Gingrich and C. Adami, *Quantum entanglement of moving bodies*, *Phys. Rev. Lett.* **89** (2002) 270402 [quant-ph/0205179].

[4] D. Ahn, H.-j. Lee, Y. H. Moon and S.W. Hwang, *Relativistic entanglement and Bell inequality*, *Phys. Rev.* **A 67** (2003) 012103 [quant-ph/0209164].

[5] P. Caban and J. Rembieliński, *Lorentz-covariant reduced spin density matrix and Einstein-Podolsky-Rosen-Bohm correlations*, *Phys. Rev.* **A 72** (2005) 012103 [quant-ph/0507056]

[6] I. Fuentes-Schuller and R.B. Mann, *Alice falls into a black hole: Entanglement in non-inertial frames*, *Phys. Rev. Lett.* **95** (2005) 120404 [quant-ph/0410172] [SPIRES].

[7] P.M. Alsing and G.J. Milburn, *Teleportation with a uniformly accelerated partner*, *Phys. Rev. Lett.* **91** (2003) 180404 [quant-ph/0302179] [SPIRES].

[8] A. Kent, *Unconditionally Secure Bit Commitment*, *Phys. Rev. Lett.* **83** (1999) 1447 [quant-ph/9810068] [SPIRES].

[9] I. Devetak, *The private classical capacity and quantum capacity of a quantum channel*, *IEEE Trans. Inform. Theory* **51** (2005) 44 [quant-ph/0304127].

[10] 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 Trans. Inform. Theory* **48** (2002) 2637.

[11] W.G. Unruh, *Notes on black hole evaporation*, *Phys. Rev.* **D 14** (1976) 870 [SPIRES].

[12] L.C.B. Crispino, A. Higuchi and G.E.A. Matsas, *The Unruh effect and its applications*, *Rev. Mod. Phys.* **80** (2008) 787 [arXiv:0710.5373] [SPIRES].

[13] R.M. Wald, *Quantum field theory in curved spacetime and black hole thermodynamics*, University of Chicago Press, Chicago U.S.A. (1999).

[14] J. Audretsch and R. Muller, *Localized discussion of stimulated processes for Rindler observers and accelerated detectors*, *Phys. Rev.* **D 49** (1994) 4056 [SPIRES].

[15] K. Brádler, *Eavesdropping of quantum communication from a noninertial frame*, *Phys. Rev.* **A 75** (2007) 022311.

[16] V.F. Mukhanov and S. Winitzki, *Introduction to quantum effects in gravity*, Cambridge University Press, Cambridge U.K. (2007).

[17] M.A. Nielsen and I.L. Chuang, *Quantum Computation and Quantum Information*, Cambridge University Press, Cambridge U.K. (2000).

[18] P. Hayden, M. Horodecki, A. Winter and J. Yard, *A decoupling approach to the quantum capacity*, *Open Syst. Inf. Dyn.* **15** (2008) 7 [quant-ph/0702005].

[19] I. Bjelaković, H. Boche and J. Nötze, *On quantum capacity of compound channels*, arXiv:0808.1007.

[20] R. Alicki and M. Fannes, *Continuity of quantum mutual information*, quant-ph/0312081.

[21] M. Hastings, *Superadditivity of communication capacity using entangled inputs*, *Natur. Phys.* **5** (2009) 255.

[22] J.A. Smolin, F. Verstraete and A. Winter, *Entanglement of assistance and multipartite state distillation*, *Phys. Rev.* **A 72** (2005) 052317.

[23] L. Susskind, L. Thorlacius and J. Uglum, *The Stretched horizon and black hole complementarity*, *Phys. Rev.* **D 48** (1993) 3743 [hep-th/9306069] [SPIRES].

[24] P. Hayden and J. Preskill, *Black holes as mirrors: quantum information in random subsystems*, *JHEP* **09** (2007) 120 [arXiv:0708.4025] [SPIRES].