Private information via the Unruh effect

Kamil Brádler† Patrick Hayden† Prakash Panangaden†

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.

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], [2], [3], [4], [5], [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.

I. 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: $\Pi_i a_i^\dagger |\text{vac}\rangle$. 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 $N$ 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
Each block \( \sigma_k \) 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 \( 1/2 \).

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

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 \( \sigma_k \): the eigenvalues of \( \sigma_k \) are equally spaced with spacing \( S = \|\vec{n}\|_2 \) and largest eigenvalue equal to \((k+1)(S+1)/2\).

### II. 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 \( \Phi_{2k} \) represent the density operator of \( k \) maximally entangled pairs of qubits and \( \tau_{2k} \) the maximally mixed state on \( k \) qubits. An \((n,k,\delta,\epsilon)\) private entanglement transmission code from Alice to Bob consists of an encoding channel \( E \) taking \( k \) qubits into the input of \( \mathcal{N}_1^{\otimes n} \) and a decoding channel \( D \) taking the output of Bob’s channel \( \mathcal{N}_1^{\otimes n} \) back to \( k \) qubits satisfying

1. **Transmission:**
\[
\left\| (id \otimes \mathcal{N}_2^{\otimes n} \circ E)(\Phi_{2k}) - \Phi_{2k} \right\|_1 \leq \delta.
\]

2. **Privacy:**
\[
\left\| (id \otimes \mathcal{N}_2^{\otimes n} \circ E)(\Phi_{2k}) - \tau_{2k} \otimes (\mathcal{N}_2^{\otimes n} \circ E)(\tau_{2k}) \right\|_1 \leq \epsilon.
\]

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

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

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

To see that the advertised rate is achievable, write $V_E$ for the Stinespring extension of $E$, with output on $A^N \mathcal{F}$. The privacy condition applied to $V_E$ is equivalent to entanglement transmission to $F E^n_2$ via Uhlmann’s theorem [17]. It is therefore sufficient to find codes that simultaneously perform entanglement transmission to Bob and to $F E^n_2$. The encodings analyzed in [18] do not depend on the channels, however, just the dummy input $\varphi$, so the same encodings can be employed for both tasks. Choosing $|F| = 2^n f$, the following sufficient conditions for successful transmission can be extracted from [18], [19]:

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

where $I(A; E_c)_\rho$ 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 $V_E$ reduced by the rate at which qubits are lost to $F$, while the second is the standard coherent information rate for $N_c$ augmented by a noiseless channel to $F$. $Q$ is maximized subject to these constraints when $H(A)_\varphi - f = I(A; E_c)_\rho + f$. Using the fact that $H(A)_\varphi = H(A)_\rho$ and purifying $\rho$ to $|\varphi\rangle^{A^N E E'}_\rho$, 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 $(n, [nQ], \delta, \epsilon)$ private entanglement transmission code. Use $R$ to denote the reference space for the maximally entangled state $\Phi_2^\otimes n$ in the definition. Let $|\sigma\rangle^{RFE_2 F_2}$ be the purified final state after $N_c^{\otimes n} \otimes E$ has acted on $\Phi_2^\otimes n$. The privacy condition and the Aliki-Fannes’ inequality [20] imply that there is a function $g(\delta)$ satisfying $\lim_{\delta \to 0} g(\delta) = 0$ such that

$$2|nQ| = 2 \log |R| \leq I(R; E^n_2 F)_\sigma + ng(\delta)$$

$$= I(R; F)_\sigma + I(R; E^n_2 F)_\sigma$$

$$\leq I(R; E^n_2 F)_\sigma + ng(\delta + \epsilon)$$

$$\leq I(R; F)_\sigma + ng(\delta + \epsilon).$$

The first inequality is a consequence of the existence of the decoding channel $D$ and the monotonicity 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

$$Q_p(\text{id}, N) \leq \lim_{n \to \infty} \max_{\rho} \frac{1}{2n} I(A; E^n_c)_\rho,$$

where the maximization is pure states $|\varphi\rangle^{A^N A^n}$ and $\rho = (\text{id} \otimes N_c^{\otimes n})(\varphi)$. 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.

**A. Unruh case**

Let us now focus on the the case where $N$ 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 $E$ 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 $N_c$ from Alice to $E_c$, the Hilbert space describing degrees of freedom beyond Eve’s horizon. The result is

$$N_c(\rho) = z \bar{\sigma} + (1 - z) \omega_0,$$

where $\sigma = N(\rho)$ and $\omega_0$ is a diagonal state independent of $\rho$. Therefore, given the output $\sigma$ 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 $\sigma$ and with probability $1 - z$ she prepares $\omega_0$ and uses it to replace $\sigma$.

Now suppose that it is possible to transmit entanglement (and therefore quantum states) beyond Eve’s horizon. Write $D(\tau) = \sum_j D_j \tau D_j$ for the decoding channel on $E_c$. Since $D(\tau) = \sum_j D_j \tau D_j$ is also a quantum channel, Eve can apply $D$ to the output of her simulation. Assuming high fidelity transmission of a quantum state $|\psi\rangle$ beyond Eve’s horizon, the output of $D$ will be a high fidelity transmission of $|\bar{\psi}\rangle$. That is impossible because the map $|\psi\rangle \mapsto |\bar{\psi}\rangle$ is not linear. 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 $Q_p(\text{id}, N)$ which we have plotted in figure[2]

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

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

**III. PRIVATE CLASSICAL CAPACITY**

Define the private classical capacity $C_p(N_1, N_2)$ as the optimal rate, measured in bits per channel use, at which Alice can send classical data to Bob over the channel $N_1$ 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 $C_p(\text{id}_2, \mathcal{N}) = \lim_{n \to \infty} C_p^{(n)}(\text{id}_2, \mathcal{N})$, where $C_p^{(n)}(\text{id}_2, \mathcal{N})$ is

$$1 - H\left(\mathcal{N}^{(1/2)}\right) + \max_{|\psi_n\rangle} \frac{1}{n} H\left(\mathcal{N}^{\otimes n}|(\psi_n)(\psi_n)\right)$$

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 $C_p(\text{id}_2, \mathcal{N})$ is bounded below by

$$C_p^{(1)}(\text{id}_2, \mathcal{N}) = (1 - z)^2 \frac{\partial^2}{\partial z^2} \bigg[ \frac{\partial}{\partial s} \text{Li} (s, z) \bigg|_{s=0} \bigg] - \frac{(1 - z)^3}{2} \frac{\partial^3}{\partial z^3} \bigg[ \frac{\partial}{\partial s} \text{Li} (s, z) \bigg|_{s=0} \bigg].$$

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

IV. 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.

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 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 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, NRO, NSERC, QuantumWorks and the Sloan Foundation.

REFERENCES

[1] M. Czachor and M. Wó³czewski. Relativistic Bennett-Brassard cryptographic scheme, relativistic errors, and how to correct them. Physical Review A, 68(1):010302, 2003.

[2] A. Peres and D. R. Terno. Quantum information and relativity theory. Reviews of Modern Physics, 76:93–123, 2004.

[3] R. M. Gingrich and C. Adami. Quantum entanglement of moving bodies. Physical Review Letters, 89(27):270402, 2002.

[4] D. Ahn, H.-j. Lee, Y. H. Moon, and S. W. Hwang. Relativistic entanglement and bells inequality. Physical Review A, 67:012103, 2003.

[5] P. Caban and J. Rembieliñski. Lorentz-covariant reduced spin density matrix and Einstein-Podolsky-Rosen-Bohm correlations. Physical Review A, 72:012103, 2005.

[6] J. Fuentes-Schuller and R. B. Mann. Alice falls into a black hole: Entanglement in noninertial frames. Physical Review Letters, 95(12):120404, 2005.

[7] Paul M. Alsing and G. J. Milburn. Teleportation with a uniformly accelerated partner. Physical Review Letters, 91(18):180404, 2003.

[8] A. Kent. Unconditionally secure bit commitment. Physical Review Letters, 83:1447–1450, 1999.

[9] I. Devetak. The private classical capacity and quantum capacity of a quantum channel. IEEE Transactions on Information Theory, 51(1):44–55, 2005.

[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 Transactions on Information Theory, 48(10):2637–2655, 2002.

[11] W. G. Unruh. Notes on black-hole evaporation. Physical Review D, 14(4):870–892, 1976.
[12] L. C. B. Crispino, A. Higuchi, and G. E. A. Matsas. The Unruh effect and its applications. Reviews of Modern Physics, 80:787, 2008.
[13] Robert M. Wald. Quantum field theory in curved spacetime and black hole thermodynamics. University of Chicago Press, Chicago, 1999.
[14] J. Audretsch and R. Müller. Localized discussion of stimulated processes for Rindler observers and accelerated detectors. Physical Review D, 49(8):4056–4065, 1994.
[15] K. Brädler. Eavesdropping of quantum communication from a noninertial frame. Physical Review A, 75(2):022311–+, 2007.
[16] V. F. Mukhanov and S. Winitzki. Introduction to quantum effects in gravity. Cambridge University Press, Cambridge, 2007.
[17] M. A. Nielsen and I. L. Chuang. Quantum Computation and Quantum Information. Cambridge University Press, Cambridge, 2000.
[18] P. Hayden, M. Horodecki, A. Winter, and J. Yard. A decoupling approach to the quantum capacity. Open Systems and Information Dynamics, 15:7–19, 2008.
[19] Igor Bjelaković, Holger Boche, and Janis Nötze. On quantum capacity of compound channels. arXiv:0808.1007, 2008.
[20] R. Alicki and M. Fannes. Continuity of quantum mutual information. quant-ph/0312081, 2003.
[21] M. Hastings. Superadditivity of communication capacity using entangled inputs. Nature Physics, 5:255–257, 2009.
[22] John A. Smolin, Frank Verstraete, and Andreas Winter. Entanglement of assistance and multipartite state distillation. Physical Review A, 72:052317, 2005.
[23] L. Susskind, L. Thorlacius, and J. Uglum. The stretched horizon and black hole complementarity. Physical Review D, 48(8):3743–3761, 1993.
[24] P. Hayden and J. Preskill. Black holes as mirrors: quantum information in random subsystems. JHEP, 9:120–+, 2007.