Private Information via the Unruh Effect

Prakash Panangaden
McGill University
joint work with
Kamil Bradler and Patrick Hayden

Relativistic Quantum Information Theory

Relativistic Quantum Information Theory

- Does this make sense?

Relativistic Quantum Information Theory

- Does this make sense?
- If we are going to use quantum communication on a large scale, relativistic effects are essential.

Relativistic Quantum Information Theory

- Does this make sense?
- If we are going to use quantum communication on a large scale, relativistic effects are essential.
- Relativistic effects in classical information theory had already been investigated as early as 1981.

Early Work

- Jarrett and Cover 1981: Relativistic classical information theory.
- Relativistic effects on transmission rates and energy requirements.
- Closely related to time dilation: special relativity.

Our direct inspiration

Our direct inspiration

- Alsing and Milburn 2002 : Entanglement and Lorentz invariance. How does the entanglement of maximally entangled states transform under Lorentz transformation?

Our direct inspiration

- Alsing and Milburn 2002 : Entanglement and Lorentz invariance. How does the entanglement of maximally entangled states transform under Lorentz transformation?
- Entanglement fidelity is preserved even though the finite dimensional Lorentz transformations are not unitary.

Our direct inspiration

- Alsing and Milburn 2002 : Entanglement and Lorentz invariance. How does the entanglement of maximally entangled states transform under Lorentz transformation?
- Entanglement fidelity is preserved even though the finite dimensional Lorentz transformations are not unitary.
- Remarks on the effect of Unruh or Hawking radiation.

“It is tantalizing to contemplate whether Unruh and/or Hawking radiation might be derived from an information theoretic point of view.”

"It is tantalizing to contemplate whether Unruh and/or Hawking radiation might be derived from an information theoretic point of view."

Alsing and Milburn

"It is tantalizing to contemplate whether Unruh and/or Hawking radiation might be derived from an information theoretic point of view."

Alsing and Milburn

Teleportation with a uniformly accelerated partner : PRL Alsing and Milburn

“It is tantalizing to contemplate whether Unruh and/or Hawking radiation might be derived from an information theoretic point of view.”

Alsing and Milburn

Teleportation with a uniformly accelerated partner : PRL Alsing and Milburn

We decided to investigate the information-theoretic properties of the Unruh effect.

Outline

- Review of quantum field theory: a biased view.
- QFT in curved spacetimes: the Unruh effect.
- Private capacity and quantum private capacity.
- Private information via the Unruh effect.

Geometrical Classical Mechanics

Geometrical Classical Mechanics

Basic arena: phase space. Each point represents a position *and* momentum. This is the real "state space" of classical physics. [Cotangent bundle over configuration space]

Geometrical Classical Mechanics

Basic arena: phase space. Each point represents a position *and* momentum. This is the real "state space" of classical physics. [Cotangent bundle over configuration space]

$$\{A, B\} := \frac{\partial A}{\partial q}\frac{\partial B}{\partial p} - \frac{\partial A}{\partial p}\frac{\partial B}{\partial q}$$

Geometrical Classical Mechanics

Basic arena: phase space. Each point represents a position *and* momentum. This is the real "state space" of classical physics. [Cotangent bundle over configuration space]

$$\{A, B\} := \frac{\partial A}{\partial q}\frac{\partial B}{\partial p} - \frac{\partial A}{\partial p}\frac{\partial B}{\partial q}$$

Poisson brackets = symplectic form

Geometrical Classical Mechanics

Basic arena: phase space. Each point represents a position *and* momentum. This is the real "state space" of classical physics. [Cotangent bundle over configuration space]

$$\{A, B\} := \frac{\partial A}{\partial q}\frac{\partial B}{\partial p} - \frac{\partial A}{\partial p}\frac{\partial B}{\partial q}$$

Poisson brackets = symplectic form

Dynamics

Geometrical Classical Mechanics

Basic arena: phase space. Each point represents a position *and* momentum. This is the real "state space" of classical physics. [Cotangent bundle over configuration space]

$$\{A, B\} := \frac{\partial A}{\partial q}\frac{\partial B}{\partial p} - \frac{\partial A}{\partial p}\frac{\partial B}{\partial q}$$

Poisson brackets = symplectic form

$$\frac{\mathrm{d}A}{\mathrm{d}t} = \{A, H\}$$

Dynamics

Quantum Mechanics Recap

1. States are rays in a Hilbert space
2. Measurements are described by hermitian operators...
3. Evolution is given by a particular unitary operator $\exp(-iHt)$
4. The algebra of observables is non-commutative and is given by Dirac's rule

$$\{P, Q\} \longrightarrow [P, Q]$$

Wave Equations

What is the precise dynamical law?

Figure out H (and get Nobel prize) then time evolution is given by:

$$i\hbar \frac{\partial \Psi}{\partial t} = H\Psi$$

Harmonic Oscillator

Harmonic Oscillator

The Hamiltonian is $H = \frac{p^2}{2m} + \frac{1}{2}m\omega^2 x^2$.

Harmonic Oscillator

The Hamiltonian is $H = \frac{p^2}{2m} + \frac{1}{2}m\omega^2 x^2$.

The energy levels are equally spaced: $E_n = \hbar\omega(n + \frac{1}{2})$

Harmonic Oscillator

The Hamiltonian is $H = \frac{p^2}{2m} + \frac{1}{2}m\omega^2 x^2$.

The energy levels are equally spaced: $E_n = \hbar\omega(n + \frac{1}{2})$

Some marvellous operators

Harmonic Oscillator

The Hamiltonian is $H = \frac{p^2}{2m} + \frac{1}{2}m\omega^2 x^2$.

The energy levels are equally spaced: $E_n = \hbar\omega(n + \frac{1}{2})$

Some marvellous operators

$$a = C(x + iC'p), \quad a^\dagger = C(x - iC'p)$$

Harmonic Oscillator

The Hamiltonian is $H = \frac{p^2}{2m} + \frac{1}{2}m\omega^2 x^2$.

The energy levels are equally spaced: $E_n = \hbar\omega(n + \frac{1}{2})$

Some marvellous operators

$$a = C(x + iC'p), \quad a^\dagger = C(x - iC'p)$$

$$a|n\rangle = \sqrt{n}|n-1\rangle, \;\; a^\dagger|n\rangle = \sqrt{n+1}|n+1\rangle$$

$$[a, a^\dagger] = 1, \;\; H = \hbar\omega(a^\dagger a + \frac{1}{2})$$

Relativistic QM

Relativistic QM

Possible relativistic wave equations arise from the representation theory of the Lorentz group. Dirac guessed the right equation for the electron from physical intuition and formal arguments.

Relativistic QM

Possible relativistic wave equations arise from the representation theory of the Lorentz group. Dirac guessed the right equation for the electron from physical intuition and formal arguments.

Problem: the energy spectrum was not bounded below. What stops an electron from falling into the negative energy states and radiating away an infinite amount of energy?

Relativistic QM

Possible relativistic wave equations arise from the representation theory of the Lorentz group. Dirac guessed the right equation for the electron from physical intuition and formal arguments.

Problem: the energy spectrum was not bounded below. What stops an electron from falling into the negative energy states and radiating away an infinite amount of energy?

Dirac's hack: Fill the negative energy states. The "vacuum" is a sea of negative energy electrons and Pauli's exclusion principle will keep ordinary electrons from falling into the sea.

Relativistic QM

Possible relativistic wave equations arise from the representation theory of the Lorentz group. Dirac guessed the right equation for the electron from physical intuition and formal arguments.

Problem: the energy spectrum was not bounded below. What stops an electron from falling into the negative energy states and radiating away an infinite amount of energy?

Dirac's hack: Fill the negative energy states. The "vacuum" is a sea of negative energy electrons and Pauli's exclusion principle will keep ordinary electrons from falling into the sea.

A negative energy electron may be kicked upstairs and become an ordinary electron leaving a "hole". The hole will behave just like a positively charged electron: a positron.

Quantum Field Theory

Quantum Field Theory

Hole theory was replaced by quantum field theory created by too many people to name them all but a few should be mentioned: Wigner, Weisskopf, Jordan, Heisenberg, Fermi and Dirac.

Quantum Field Theory

Hole theory was replaced by quantum field theory created by too many people to name them all but a few should be mentioned: Wigner, Weisskopf, Jordan, Heisenberg, Fermi and Dirac.

The main ideas: particles are no longer “conserved”, they can be created and destroyed. The state space is the symmetric tensor algebra or the Grassman algebra over the old Hilbert space. This is called Fock space.

Quantum Field Theory

Hole theory was replaced by quantum field theory created by too many people to name them all but a few should be mentioned: Wigner, Weisskopf, Jordan, Heisenberg, Fermi and Dirac.

The main ideas: particles are no longer "conserved", they can be created and destroyed. The state space is the symmetric tensor algebra or the Grassman algebra over the old Hilbert space. This is called Fock space.

The old "wave functions" become operator fields. They act on Fock space and create or annihilate particles: second quantization.

Quantum Field Theory

Hole theory was replaced by quantum field theory created by too many people to name them all but a few should be mentioned: Wigner, Weisskopf, Jordan, Heisenberg, Fermi and Dirac.

The main ideas: particles are no longer "conserved", they can be created and destroyed. The state space is the symmetric tensor algebra or the Grassman algebra over the old Hilbert space. This is called Fock space.

The old "wave functions" become operator fields. They act on Fock space and create or annihilate particles: second quantization.

The mathematical complexity rises a whole level beyond that of ordinary quantum mechanics.

Classical Field Theory: Klein-Gordon field

Classical Field Theory: Klein-Gordon field

$$-\frac{\partial^2\phi}{\partial t^2}+\frac{\partial^2\phi}{\partial x^2}+\frac{\partial^2\phi}{\partial y^2}+\frac{\partial^2\phi}{\partial z^2}-m^2\phi=0$$

Classical Field Theory: Klein-Gordon field

$$-\frac{\partial^2\phi}{\partial t^2}+\frac{\partial^2\phi}{\partial x^2}+\frac{\partial^2\phi}{\partial y^2}+\frac{\partial^2\phi}{\partial z^2}-m^2\phi=0$$

Often written $\Box\phi - m^2\phi = 0$.

Classical Field Theory: Klein-Gordon field

$$-\frac{\partial^2\phi}{\partial t^2}+\frac{\partial^2\phi}{\partial x^2}+\frac{\partial^2\phi}{\partial y^2}+\frac{\partial^2\phi}{\partial z^2}-m^2\phi=0$$

Often written $\Box\phi - m^2\phi = 0$.

Let V be the real vector space of classical solutions; it is the analogue of phase space.

Classical Field Theory: Klein-Gordon field

$$-\frac{\partial^2\phi}{\partial t^2}+\frac{\partial^2\phi}{\partial x^2}+\frac{\partial^2\phi}{\partial y^2}+\frac{\partial^2\phi}{\partial z^2}-m^2\phi=0$$

Often written $\Box\phi - m^2\phi = 0$.

Let V be the real vector space of classical solutions; it is the analogue of phase space.

The symplectic form is:

Classical Field Theory: Klein-Gordon field

$$-\frac{\partial^2\phi}{\partial t^2}+\frac{\partial^2\phi}{\partial x^2}+\frac{\partial^2\phi}{\partial y^2}+\frac{\partial^2\phi}{\partial z^2}-m^2\phi=0$$

Often written $\Box\phi - m^2\phi = 0.$

Let V be the real vector space of classical solutions; it is the analogue of phase space.

The symplectic form is:

$$\Omega(\phi_1,\phi_2)=\int_\Sigma(\phi_1\vec{\nabla}\phi_2-\phi_2\vec{\nabla}\phi_1)\cdot d\vec{\sigma}$$

Traditional Quantum Field Theory

Traditional Quantum Field Theory

Start with $\Box\phi - m^2\phi$

Traditional Quantum Field Theory

Start with $\Box\phi - m^2\phi$ Put it in a “box” to avoid hassles.

Traditional Quantum Field Theory

Start with $\Box\phi - m^2\phi$ Put it in a "box" to avoid hassles.

$$\phi(\vec{x},t) = \sum_{\vec{k}} \phi_{\vec{k}}(t) e^{i\vec{k}\cdot\vec{x}}; \quad \vec{k} = 2\pi(n_x, n_y, n_z).$$

Traditional Quantum Field Theory

Start with $\Box\phi - m^2\phi$ Put it in a "box" to avoid hassles.

$$\phi(\vec{x}, t) = \sum_{\vec{k}} \phi_{\vec{k}}(t) e^{i\vec{k}\cdot\vec{x}}; \quad \vec{k} = 2\pi(n_x, n_y, n_z).$$

Now the Hamiltonian is

Traditional Quantum Field Theory

Start with $\Box\phi - m^2\phi$ Put it in a "box" to avoid hassles.

$$\phi(\vec{x}, t) = \sum_{\vec{k}} \phi_{\vec{k}}(t) e^{i\vec{k}\cdot\vec{x}}; \quad \vec{k} = 2\pi(n_x, n_y, n_z).$$

Now the Hamiltonian is

$$\sum_{\vec{k}} \{ \frac{1}{2} |\dot{\phi}_{\vec{k}}|^2 + \frac{1}{2} \omega_{\vec{k}}^2 |\phi_{\vec{k}}|^2 \}$$

Traditional Quantum Field Theory

Start with $\Box\phi - m^2\phi$ Put it in a "box" to avoid hassles.

$$\phi(\vec{x},t) = \sum_{\vec{k}} \phi_{\vec{k}}(t) e^{i\vec{k}\cdot\vec{x}}; \quad \vec{k} = 2\pi(n_x, n_y, n_z).$$

Now the Hamiltonian is

$$\sum_{\vec{k}} \{\frac{1}{2}|\dot{\phi}_{\vec{k}}|^2 + \frac{1}{2}\omega_{\vec{k}}^2|\phi_{\vec{k}}|^2\} \quad \text{where } \omega_{\vec{k}}^2 = \vec{k}^2 + m^2.$$

Traditional Quantum Field Theory

Start with $\Box\phi - m^2\phi$ Put it in a "box" to avoid hassles.

$$\phi(\vec{x},t) = \sum_{\vec{k}} \phi_{\vec{k}}(t) e^{i\vec{k}\cdot\vec{x}}; \quad \vec{k} = 2\pi(n_x, n_y, n_z).$$

Now the Hamiltonian is

$$\sum_{\vec{k}} \{\frac{1}{2}|\dot{\phi}_{\vec{k}}|^2 + \frac{1}{2}\omega_{\vec{k}}^2|\phi_{\vec{k}}|^2\} \quad \text{where } \omega_{\vec{k}}^2 = \vec{k}^2 + m^2.$$

This looks like a collection of harmonic oscillators.

Traditional Quantum Field Theory

Start with $\Box\phi - m^2\phi$ Put it in a "box" to avoid hassles.

$$\phi(\vec{x},t) = \sum_{\vec{k}} \phi_{\vec{k}}(t) e^{i\vec{k}\cdot\vec{x}}; \quad \vec{k} = 2\pi(n_x, n_y, n_z).$$

Now the Hamiltonian is

$$\sum_{\vec{k}} \{\frac{1}{2}|\dot{\phi}_{\vec{k}}|^2 + \frac{1}{2}\omega_{\vec{k}}^2 |\phi_{\vec{k}}|^2\} \quad \text{where } \omega_{\vec{k}}^2 = \vec{k}^2 + m^2.$$

This looks like a collection of harmonic oscillators.

Fermi

The $a, a^\dagger$ operators now destroy and create quanta of different modes:
particles have emerged from the field!

The $a, a^\dagger$ operators now destroy and create quanta of different modes:
particles have emerged from the field!

The innocent harmonic oscillator plays a foundational role in QFT.

The $a, a^\dagger$ operators now destroy and create quanta of different modes:
particles have emerged from the field!

The innocent harmonic oscillator plays a foundational role in QFT.

The a and $a^\dagger$ come from the positive and negative frequencies of the field.

The $a, a^\dagger$ operators now destroy and create quanta of different modes:
particles have emerged from the field!

The innocent harmonic oscillator plays a foundational role in QFT.

The a and $a^\dagger$ come from the positive and negative frequencies of the field.

The vacuum is the state killed by all the a operators.

How do we know what is positive frequency and what is negative frequency?

How do we know what is positive frequency and what is negative frequency?

The Fourier transform tells us:

How do we know what is positive frequency and what is negative frequency?

The Fourier transform tells us:

$$\Phi(\vec{x}, t) = \sum_k f_k(\vec{x}, t)\mathbf{a}_k + \overline{f_k}(\vec{x}, t)\mathbf{a}_k^\dagger$$

How do we know what is positive frequency and what is negative frequency?

The Fourier transform tells us:

$$\Phi(\vec{x},t) = \sum_k f_k(\vec{x},t)\mathbf{a}_k + \overline{f_k}(\vec{x},t)\mathbf{a}_k^\dagger$$

Operators are in **bold face**.

How do we know what is positive frequency and what is negative frequency?

The Fourier transform tells us:

$$\Phi(\vec{x}, t) = \sum_k f_k(\vec{x}, t)\mathbf{a}_k + \overline{f_k}(\vec{x}, t)\mathbf{a}_k^\dagger$$

Operators are in **bold face**.

The f_k are classical positive energy solutions:

How do we know what is positive frequency and what is negative frequency?

The Fourier transform tells us:

$$\Phi(\vec{x},t) = \sum_k f_k(\vec{x},t)\mathbf{a}_k + \overline{f_k}(\vec{x},t)\mathbf{a}_k^\dagger$$

Operators are in **bold face**.

The f_k are classical positive energy solutions:

$$f_k = (\cdot\cdot)\exp(i\vec{k}\cdot\vec{x} - i\omega t)$$

How do we know what is positive frequency and what is negative frequency?

The Fourier transform tells us:

$$\Phi(\vec{x},t) = \sum_k f_k(\vec{x},t)\mathbf{a}_k + \overline{f_k}(\vec{x},t)\mathbf{a}_k^\dagger$$

Operators are in **bold face**.

The f_k are classical positive energy solutions:

$$f_k = (\cdot\cdot)\exp(i\vec{k}\cdot\vec{x} - i\omega t)$$

One needs the canonical Fourier transform that one has in a flat spacetime.

Fock Space

Fock Space

A Hilbert space that accomodates multiple particles.

Fock Space

A Hilbert space that accomodates multiple particles.

Suppose that $\mathcal{H}$ is the ordinary (1 particle) Hilbert space.

Fock Space

A Hilbert space that accomodates multiple particles.

Suppose that $\mathcal{H}$ is the ordinary (1 particle) Hilbert space.

$$\mathcal{F}(\mathcal{H}) = \mathbb{C} \oplus \mathcal{H} \oplus (\mathcal{H} \otimes_S \mathcal{H}) \oplus (\mathcal{H} \otimes_S \mathcal{H} \otimes_S \mathcal{H}) \ldots$$

Fock Space

A Hilbert space that accomodates multiple particles.

Suppose that $\mathcal{H}$ is the ordinary (1 particle) Hilbert space.

$$\mathcal{F}(\mathcal{H}) = \mathbb{C} \oplus \mathcal{H} \oplus (\mathcal{H} \otimes_S \mathcal{H}) \oplus (\mathcal{H} \otimes_S \mathcal{H} \otimes_S \mathcal{H}) \dots$$

$$C(\sigma)\Psi = (0, \sigma^{\alpha}\xi, \sqrt{2}\sigma^{(\alpha}\xi^{\beta)}, \sqrt{3}\sigma^{(\alpha}\xi^{\beta\gamma)}, \dots)$$

Fock Space

A Hilbert space that accomodates multiple particles.

Suppose that $\mathcal{H}$ is the ordinary (1 particle) Hilbert space.

$$\mathcal{F}(\mathcal{H}) = \mathbb{C} \oplus \mathcal{H} \oplus (\mathcal{H} \otimes_S \mathcal{H}) \oplus (\mathcal{H} \otimes_S \mathcal{H} \otimes_S \mathcal{H}) \dots$$

$$C(\sigma)\Psi = (0, \sigma^\alpha \xi, \sqrt{2}\sigma^{(\alpha}\xi^{\beta)}, \sqrt{3}\sigma^{(\alpha}\xi^{\beta\gamma)}, \dots)$$

$$A(\bar{\tau})\Psi = (\xi^\mu \bar{\tau}_\mu, \sqrt{2}\xi^{\mu\alpha}\bar{\tau}_\mu, \sqrt{3}\xi^{\mu\alpha\beta}\bar{\tau}_\mu, \dots)$$

Fock Space

A Hilbert space that accomodates multiple particles.

Suppose that $\mathcal{H}$ is the ordinary (1 particle) Hilbert space.

$$\mathcal{F}(\mathcal{H}) = \mathbb{C} \oplus \mathcal{H} \oplus (\mathcal{H} \otimes_S \mathcal{H}) \oplus (\mathcal{H} \otimes_S \mathcal{H} \otimes_S \mathcal{H}) \ldots$$

$$C(\sigma)\Psi = (0, \sigma^\alpha \xi, \sqrt{2}\sigma^{(\alpha}\xi^{\beta)}, \sqrt{3}\sigma^{(\alpha}\xi^{\beta\gamma)}, \ldots)$$

$$A(\bar{\tau})\Psi = (\xi^\mu \bar{\tau}_\mu, \sqrt{2}\xi^{\mu\alpha}\bar{\tau}_\mu, \sqrt{3}\xi^{\mu\alpha\beta}\bar{\tau}_\mu, \ldots)$$

The "harmonic oscillators" give the creation and annihilation operators of QFT.

A critique

A critique

- These concepts are wrong -- or, at least, misleading -- for QFT in curved spacetimes.

A critique

- These concepts are wrong -- or, at least, misleading -- for QFT in curved spacetimes.
- The notion of "particle" is not absolute.

A critique

- These concepts are wrong -- or, at least, misleading -- for QFT in curved spacetimes.
- The notion of “particle” is not absolute.
- Particles may appear out of the vacuum: Leonard Parker, Stephen Hawking and Bill Unruh.

A critique

- These concepts are wrong -- or, at least, misleading -- for QFT in curved spacetimes.
- The notion of "particle" is not absolute.
- Particles may appear out of the vacuum: Leonard Parker, Stephen Hawking and Bill Unruh.
- Particles are a useful abstraction when talking about detectors coupled to quantum fields.

Algebraic Quantum Field Theory

Algebraic Quantum Field Theory

We need to construct:

(a) A *-algebra of observables

(b) A Hilbert space carrying a *-representation

(c) A rule for the dynamics.

Algebraic Quantum Field Theory

We need to construct:
(a) A *-algebra of observables
(b) A Hilbert space carrying a *-representation
(c) A rule for the dynamics.

We will use the classical data to guide the construction of the QFT.

What is a $*$-algebra?

What is a $*$-algebra?

A complex vector space A

What is a $*$-algebra?

A complex vector space A,

What is a $*$-algebra?

A complex vector space A,

with a *product* defined on A.

What is a $*$-algebra?

A complex vector space A,

with a *product* defined on A.

The product is associative and bi-linear.

What is a $*$-algebra?

A complex vector space A,

with a *product* defined on A.

The product is associative and bi-linear.

Finally an *involution*, written $*$, satisfying:

What is a $*$-algebra?

A complex vector space A,

with a *product* defined on A.

The product is associative and bi-linear.

Finally an *involution*, written $*$, satisfying:

$$A^{**} = A$$

What is a $*$-algebra?

A complex vector space A,

with a *product* defined on A.

The product is associative and bi-linear.

Finally an *involution*, written $*$, satisfying:

$$A^{**} = A$$

$$(A + \alpha B)^* = A^* + \overline{\alpha} B^*$$

What is a $*$-algebra?

A complex vector space A,

with a *product* defined on A.

The product is associative and bi-linear.

Finally an *involution*, written $*$, satisfying:

$$A^{**} = A$$

$$(A + \alpha B)^* = A^* + \overline{\alpha} B^*$$

$$(AB)^* = B^* A^*$$

What is a $*$-algebra?

A complex vector space A,

with a *product* defined on A.

The product is associative and bi-linear.

Finally an *involution*, written $*$, satisfying:

$$A^{**} = A$$

$$(A + \alpha B)^* = A^* + \overline{\alpha} B^*$$

$$(AB)^* = B^* A^*$$

$*$ is an abstraction of $\dagger$.

What is a $*$-algebra?

A complex vector space A,

with a *product* defined on A.

The product is associative and bi-linear.

Finally an *involution*, written $*$, satisfying:

$$A^{**} = A$$

$$(A + \alpha B)^* = A^* + \overline{\alpha} B^*$$

$$(AB)^* = B^* A^*$$

$*$ is an abstraction of $\dagger$.

An abstract $*$-algebra can be represented as a concrete collection of operators on a Hilbert space: $*$-representation.

The $*$-Algebra of Observables

A $*$-algebra is a vector space with a multiplication and an involution $(*)$.

The $*$-Algebra of Observables

A $*$-algebra is a vector space with a multiplication and an involution $(*)$.

Start with the real vector space V of classical solutions to the KG equation.

The $*$-Algebra of Observables

A $*$-algebra is a vector space with a multiplication and an involution ($*$).

Start with the real vector space V of classical solutions to the KG equation.

Take the *free* $*$-algebra generated by V.

The $*$-Algebra of Observables

A $*$-algebra is a vector space with a multiplication and an involution ($*$).

Start with the real vector space V of classical solutions to the KG equation.

Take the *free* $*$-algebra generated by V. Write $F[\phi]$ for the element of the algebra corresponding to $\phi \in V$.

The $*$-Algebra of Observables

A $*$-algebra is a vector space with a multiplication and an involution $(*)$.

Start with the real vector space V of classical solutions to the KG equation.

Take the *free* $*$-algebra generated by V.

Write $F[\phi]$ for the element of the algebra corresponding to $\phi \in V$.

Impose the Dirac condition:

The $*$-Algebra of Observables

A $*$-algebra is a vector space with a multiplication and an involution $(*)$.

Start with the real vector space V of classical solutions to the KG equation.

Take the *free* $*$-algebra generated by V.
Write $F[\phi]$ for the element of the algebra corresponding to $\phi \in V$.

Impose the Dirac condition:

$$[F[\phi], F[\psi]] := F[\phi]F[\psi] - F[\psi]F[\phi] = \Omega(\phi, \psi)$$

How should the the abstract $*$-algebra be realized as as operators on a Hilbert space?

We should have a Fock space built out of V, the classical solutions.

How can we make the real vector space V into a complex vector space?

Look for a *complex structure*: $J : V \to V$

$$J^2 = -I$$

But what *physical idea* will motivate the choice of J?

Polarizations and Complex Structures

$$\phi = \phi^{(+)} + \phi^{(-)}$$

Polarizations and Complex Structures

$$\phi = \phi^{(+)} + \phi^{(-)}$$

$\phi^{(\pm)}$ live in $V_{\mathbb{C}} := V \oplus iV$

Polarizations and Complex Structures

$$\phi = \phi^{(+)} + \phi^{(-)}$$

$\phi^{(\pm)}$ live in $V_{\mathbb{C}} := V \oplus iV$

$$(a + ib)(u, v) = (au - bv, bu + av)$$

Polarizations and Complex Structures

$$\phi = \phi^{(+)} + \phi^{(-)}$$

$\phi^{(\pm)}$ live in $V_{\mathbb{C}} := V \oplus iV$

$$(a+ib)(u,v) = (au - bv, bu + av)$$

$$V_{\mathbb{C}} = V^{(+)} \oplus V^{(-)}$$

Polarizations and Complex Structures

$$\phi = \phi^{(+)} + \phi^{(-)}$$

$\phi^{(\pm)}$ live in $V_{\mathbb{C}} := V \oplus iV$

$$(a+ib)(u,v) = (au - bv, bu + av)$$

$$V_{\mathbb{C}} = V^{(+)} \oplus V^{(-)}$$

$$P^{(\pm)} : V_{\mathbb{C}} \to V^{(\pm)}$$

Polarizations and Complex Structures

$$\phi = \phi^{(+)} + \phi^{(-)}$$

$\phi^{(\pm)}$ live in $V_{\mathbb{C}} := V \oplus iV$

$$(a+ib)(u,v) = (au - bv, bu + av)$$

$$V_{\mathbb{C}} = V^{(+)} \oplus V^{(-)}$$

$$P^{(\pm)} : V_{\mathbb{C}} \to V^{(\pm)}$$

$$\overline{\phi^{(+)}} = \phi^{(-)}$$

Complex Structure $\equiv$ Polarization

$$J\phi = i\phi^{(+)} - i\phi^{(-)}$$

$$P^{(+)}\phi = -\frac{i}{2}[J\phi + i\phi]$$

$$P^{(-)}\phi = \frac{i}{2}[J\phi - i\phi]$$

Complex Structure $\equiv$ Polarization

$$J\phi = i\phi^{(+)} - i\phi^{(-)}$$

$$P^{(+)}\phi = -\frac{i}{2}[J\phi + i\phi]$$

$$P^{(-)}\phi = \frac{i}{2}[J\phi - i\phi]$$

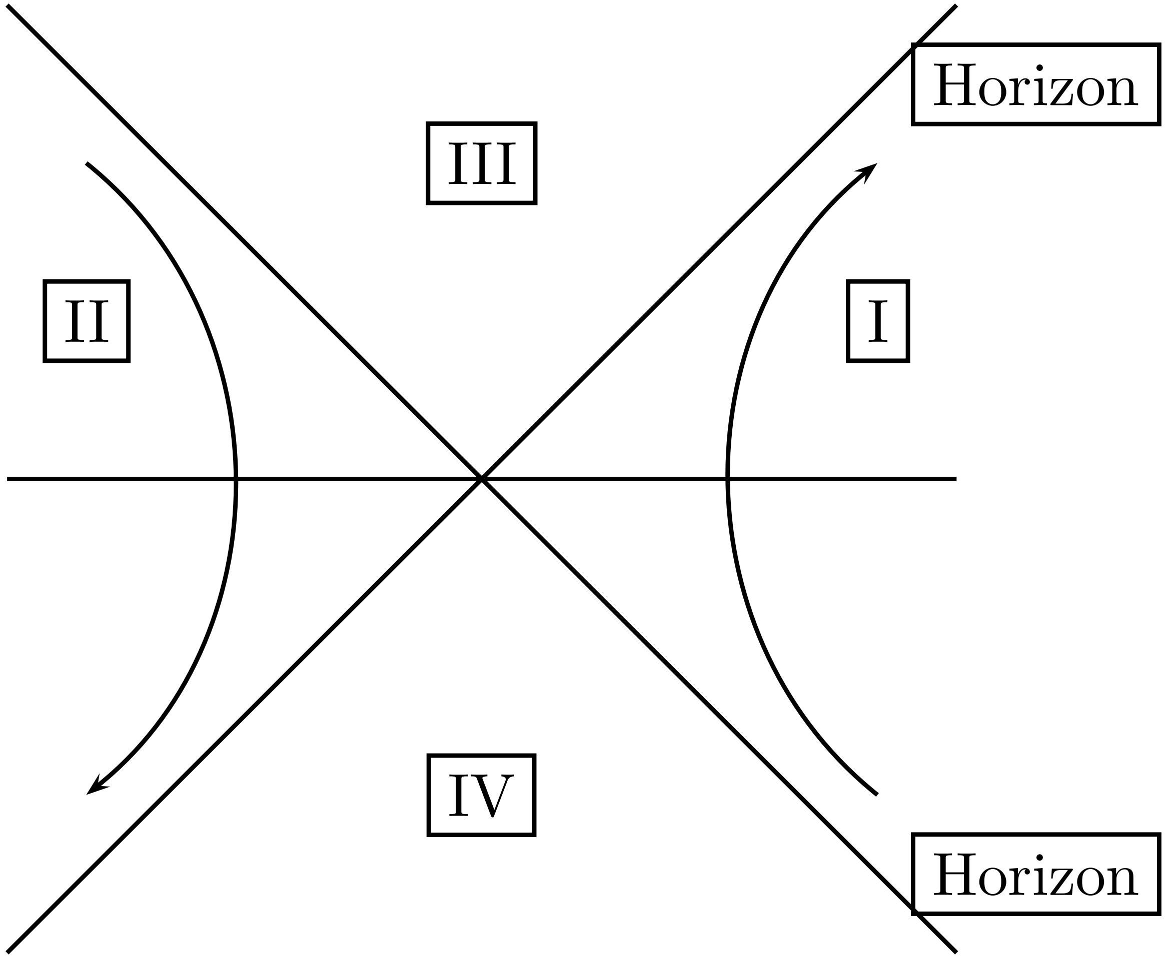
Choosing a decomposition into positive and negative frequencies is equivalent to choosing a complex structure.

In curved spacetime we have have no canonical choice of complex structure.

Hence no canonical choice of positive and negative frequencies.

Hence, one observer's vacuum may not be another observer's vacuum.

Thus there is a transformation from one observer's Fock space to another's.



Rindler spacetime.

The accelerating observer and the inertial observer will disagree about the vacuum.

The accelerating observer and the inertial observer will disagree about the vacuum.

The transformation is given by

The accelerating observer and the inertial observer will disagree about the vacuum.

The transformation is given by

$$a_k \mapsto \alpha_k \tilde{a}_k + \beta_k \tilde{a}_k^\dagger$$

The accelerating observer and the inertial observer will disagree about the vacuum.

The transformation is given by

$$a_k \mapsto \alpha_k \tilde{a}_k + \beta_k \tilde{a}_k^\dagger$$

where $\tilde{a}$ is the accelerating observer's annihilation operator.

The accelerating observer and the inertial observer will disagree about the vacuum.

The transformation is given by

$$a_k \mapsto \alpha_k \tilde{a}_k + \beta_k \tilde{a}_k^\dagger$$

where $\tilde{a}$ is the accelerating observer's annihilation operator.

The change of annihilation and creation operators is called a *Bogolioubov transformation*

The accelerating observer and the inertial observer will disagree about the vacuum.

The transformation is given by

$$a_k \mapsto \alpha_k \tilde{a}_k + \beta_k \tilde{a}_k^\dagger$$

where $\tilde{a}$ is the accelerating observer's annihilation operator.

The change of annihilation and creation operators is called a *Bogolioubov transformation*

There will be modes corresponding to the inaccessible region,

The accelerating observer and the inertial observer will disagree about the vacuum.

The transformation is given by

$$a_k \mapsto \alpha_k \tilde{a}_k + \beta_k \tilde{a}_k^\dagger$$

where $\tilde{a}$ is the accelerating observer's annihilation operator.

The change of annihilation and creation operators is called a *Bogolioubov transformation*

There will be modes corresponding to the inaccessible region,

so the accelerating observer's density matrix will involve a partial trace over the modes of the inaccessible region.

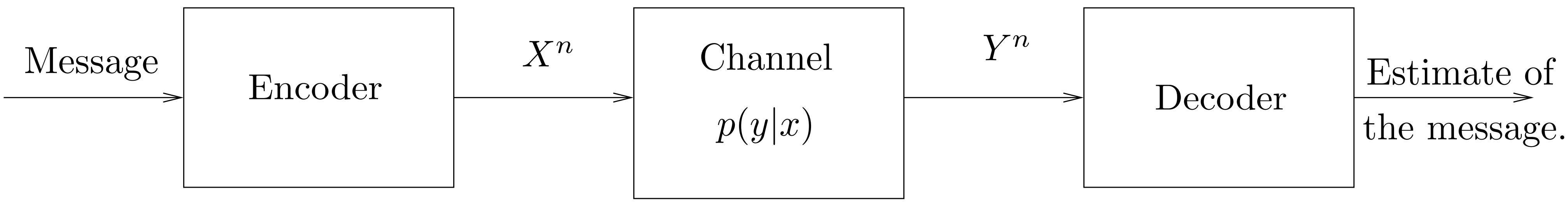
Unruh Effect

The inertial observer's vacuum will look like a bath of thermal radiation to the accelerating observer.

The notion of "particle" is not absoute:

it only refers to the effects of a detector interacting with a field.

Channels



A typical channel.

How well can we estimate the intended message if the channel is noisy?

Channel Capacity

- The basic measure of information transmission.
- Shannon's coding theorem: All transmission rates below the capacity are achievable with asymptotically zero probability of error.

What is a quantum channel?

What is a quantum channel?

Must take density matrices to density matrices:

What is a quantum channel?

Must take density matrices to density matrices:

$$\rho \mapsto \mathcal{E}(\rho)$$

What is a quantum channel?

Must take density matrices to density matrices:

$$\rho \mapsto \mathcal{E}(\rho)$$

Most general form for $\mathcal{E}$

What is a quantum channel?

Must take density matrices to density matrices:

$$\rho \mapsto \mathcal{E}(\rho)$$

Most general form for $\mathcal{E}$

$$\mathcal{E}(\rho) = \sum_i A_i \rho A_i^\dagger$$

What is a quantum channel?

Must take density matrices to density matrices:

$$\rho \mapsto \mathcal{E}(\rho)$$

Most general form for $\mathcal{E}$

$$\mathcal{E}(\rho) = \sum_i A_i \rho A_i^\dagger$$

where the A_i are linear maps
and $\sum_i A_i^\dagger A_i = I$

von Neumann Entropy

von Neumann Entropy

$$H(\rho) = -\mathrm{tr}(\rho \log_2 \rho) = -\sum_i \lambda_i \log_2 \lambda_i$$

von Neumann Entropy

$$H(\rho) = -\mathrm{tr}(\rho \log_2 \rho) = -\sum_i \lambda_i \log_2 \lambda_i$$

Holevo χ quantity

von Neumann Entropy

$$H(\rho) = -\mathrm{tr}(\rho \log_2 \rho) = -\sum_i \lambda_i \log_2 \lambda_i$$

Holevo χ quantity

If $\rho = \sum_i p_i \rho_i$ then define

von Neumann Entropy

$$H(\rho) = -\mathrm{tr}(\rho \log_2 \rho) = -\sum_i \lambda_i \log_2 \lambda_i$$

Holevo χ quantity

If $\rho = \sum_i p_i \rho_i$ then define

$$\chi(\rho) = H(\rho) - \sum_i p_i H(\rho_i)$$

von Neumann Entropy

$$H(\rho) = -\mathrm{tr}(\rho \log_2 \rho) = -\sum_i \lambda_i \log_2 \lambda_i$$

Holevo χ quantity

If $\rho = \sum_i p_i \rho_i$ then define

$$\chi(\rho) = H(\rho) - \sum_i p_i H(\rho_i)$$

Holevo bound: χ is an upper bound on accessible information in ρ.

Quantum Channels 1

Quantum Channels 1

- We want to send quantum data from Alice to Bob.

Quantum Channels 1

- We want to send quantum data from Alice to Bob.
- Sending classical data: choose a basis to represent classical data and encode classical data in a quantum state. Bob has to extract the classical data from the quantum state.

Quantum Channels 1

- We want to send quantum data from Alice to Bob.
- Sending classical data: choose a basis to represent classical data and encode classical data in a quantum state. Bob has to extract the classical data from the quantum state.
- Sending quantum data: Alice wants to send the whole quantum state.

Quantum Channels 2

- New possibility: If Alice uses multiple copies of the channel she could entangle the quantum states across multiple uses of the channel.
- We do not know how to compute the capacity in this case!

Quantum Channels 3

Quantum Channels 3

Restriction: Alice can only prepare product states:

Quantum Channels 3

Restriction: Alice can only prepare product states:

$$\rho_1 \otimes \rho_2 \otimes \ldots \otimes \rho_n$$

Quantum Channels 3

Restriction: Alice can only prepare product states:

$$\rho_1 \otimes \rho_2 \otimes \ldots \otimes \rho_n$$

One for each use of the channel

Quantum Channels 3

Restriction: Alice can only prepare product states:

$$\rho_1 \bigotimes \rho_2 \bigotimes \ldots \bigotimes \rho_n$$

One for each use of the channel

$C^{(1)}(\mathcal{E})$

Quantum Channels 3

Restriction: Alice can only prepare product states:

$$\rho_1 \otimes \rho_2 \otimes \ldots \otimes \rho_n$$

One for each use of the channel

$C^{(1)}(\mathcal{E})$ the one-shot capacity

Quantum Channels 3

Restriction: Alice can only prepare product states:

$$\rho_1 \otimes \rho_2 \otimes \ldots \otimes \rho_n$$

One for each use of the channel

$C^{(1)}(\mathcal{E})$ the one-shot capacity

In this case we have the Holevo-Schumacher-Westmoreland theorem, which gives us a "formula" for the capacity.

The Holevo-Schumacher-Westmoreland Theorem

The Holevo-Schumacher-Westmoreland Theorem

$$C^{(1)}(\mathcal{E}) = \max_{(p_j,\rho_j)} [H(\mathcal{E}(\sum_j p_j \rho_j) - \sum_j p_j H(\mathcal{E}(\rho_j))]$$

The Holevo-Schumacher-Westmoreland Theorem

$$C^{(1)}(\mathcal{E}) = \max_{(p_j,\rho_j)} [H(\mathcal{E}(\sum_j p_j \rho_j) - \sum_j p_j H(\mathcal{E}(\rho_j))]$$

ρ_j are the possible input states.

The Holevo-Schumacher-Westmoreland Theorem

$$C^{(1)}(\mathcal{E}) = \max_{(p_j,\rho_j)} [H(\mathcal{E}(\sum_j p_j \rho_j) - \sum_j p_j H(\mathcal{E}(\rho_j))]$$

ρ_j are the possible input states.

Pure state ensembles suffice.

The Holevo-Schumacher-Westmoreland Theorem

$$C^{(1)}(\mathcal{E}) = \max_{(p_j,\rho_j)} [H(\mathcal{E}(\sum_j p_j \rho_j) - \sum_j p_j H(\mathcal{E}(\rho_j))]$$

ρ_j are the possible input states.

Pure state ensembles suffice.

I will spare you hideous formulas in what follows!

Private Capacity

Private Capacity

Quantum communication can be used for establishing secret correlations. [BB84]

Private Capacity

Quantum communication can be used for establishing secret correlations. [BB84]

What is the capacity for sending *private* data?

Private Capacity

Quantum communication can be used for establishing secret correlations. [BB84]

What is the capacity for sending *private* data?

Purely classical: Maurer (1994) and Ahlswede & Csiszar (1993)

Private Capacity

Quantum communication can be used for establishing secret correlations. [BB84]

What is the capacity for sending *private* data?

Purely classical: Maurer (1994) and Ahlswede & Csiszar (1993)

What is the private capacity of a quantum channel for communicating classical data? [Devetak 2005]

Private Capacity

Quantum communication can be used for establishing secret correlations. [BB84]

What is the capacity for sending *private* data?

Purely classical: Maurer (1994) and Ahlswede & Csiszar (1993)

What is the private capacity of a quantum channel for communicating classical data? [Devetak 2005]

What is the private capacity of a quantum channel for communicating quantum data? [Hayden et al. in progress]

$$\begin{tikzcd}
 & \cdot \arrow[r] & B \\
A \arrow[ur] \arrow[dr] & & \\
 & \cdot \arrow[r] & E
\end{tikzcd}$$

$$
\begin{tikzcd}
 & \cdot \arrow[r] & B \\
A \arrow[ur] \arrow[dr] & & \\
 & \cdot \arrow[r] & E
\end{tikzcd}
$$

Quantum state is a density matrix on $B \otimes E$

$$\begin{tikzcd}
 & \cdot \arrow[r] & B \\
A \arrow[ur] \arrow[dr] & & \\
 & \cdot \arrow[r] & E
\end{tikzcd}$$

Quantum state is a density matrix on $B \otimes E$

Alice wants to send a message to Bob
so that with high probability Bob can decode it
and Eve is very unlikely to be able to decode it.

$$
\begin{tikzcd}
 & \cdot \arrow[r] & B \\
A \arrow[ur] \arrow[dr] & & \\
 & \cdot \arrow[r] & E
\end{tikzcd}
$$

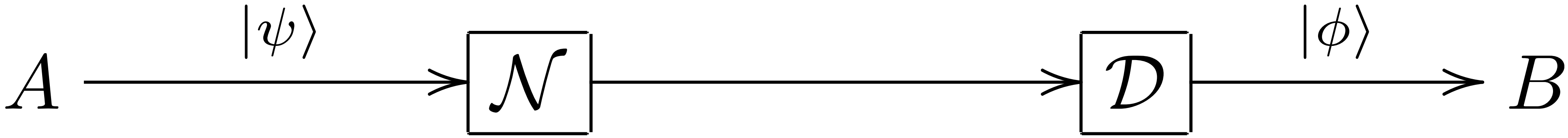
Quantum state is a density matrix on $B \otimes E$

Alice wants to send a message to Bob
so that with high probability Bob can decode it
and Eve is very unlikely to be able to decode it.

An (n, ϵ) private channel code
of rate R allows Alice to send one of 2^{nR}
messages,Bob can decode with error less than ϵ
and Eve cannot find out more than ϵ bits.

Private Quantum Communication

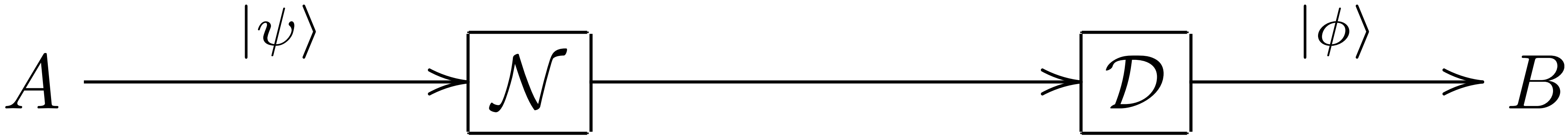
Private Quantum Communication



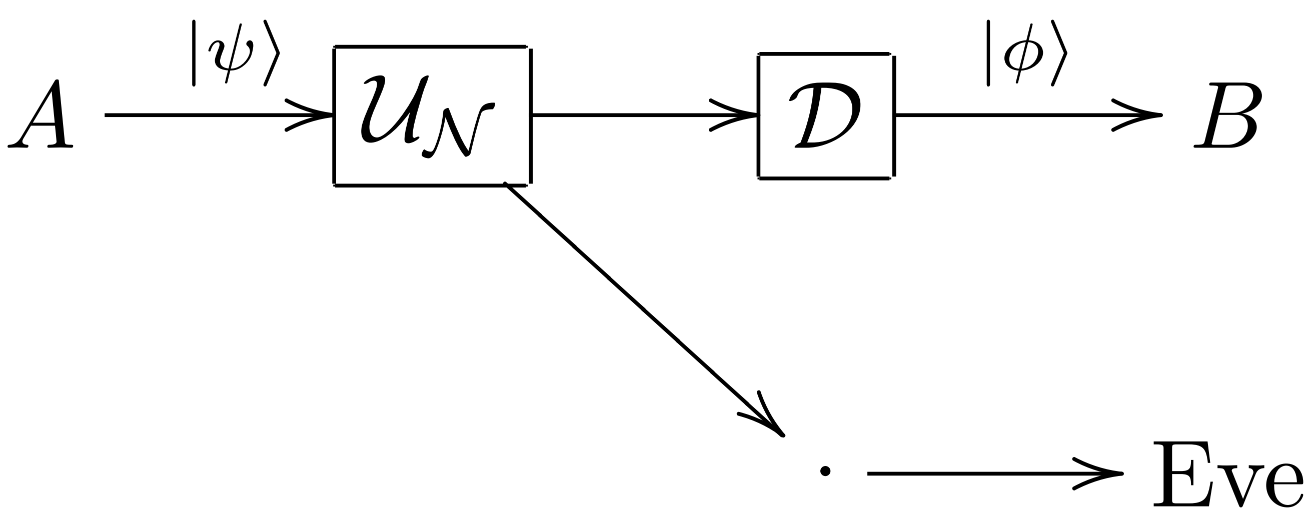
Noisy channel

Decoder

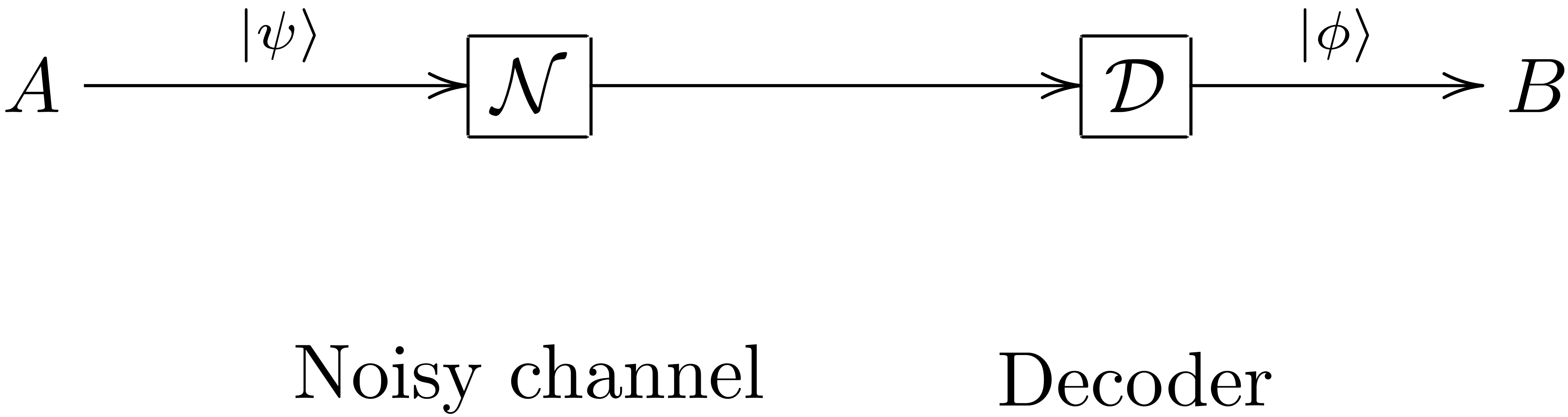
Private Quantum Communication

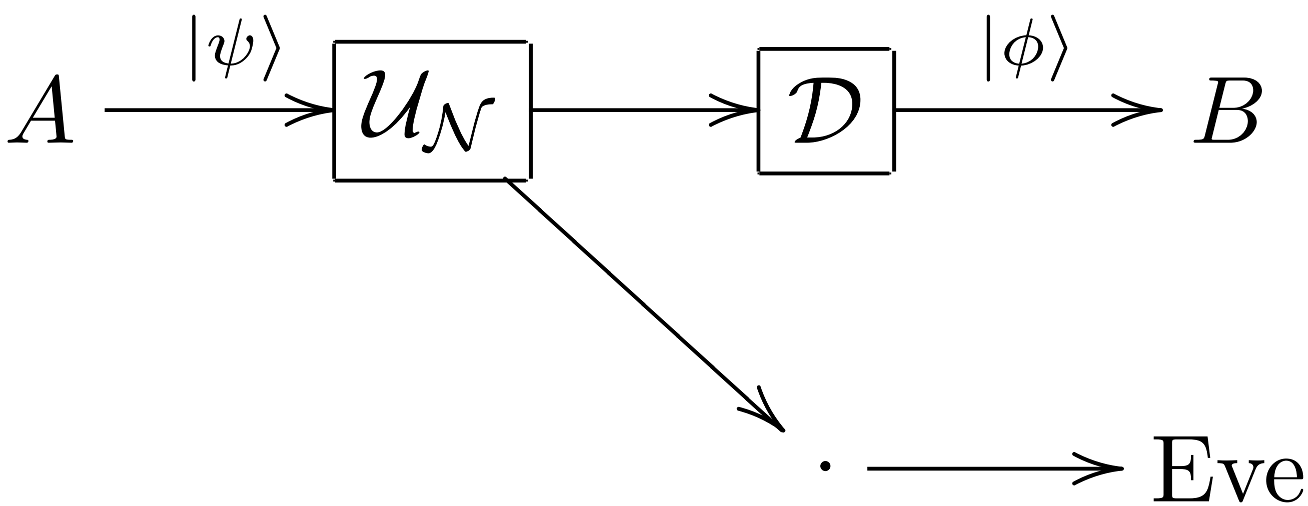


Noisy channel Decoder



Private Quantum Communication





Eve cannot get a copy of ϕ: automatic privacy.

Our Setting Today

Our Setting Today

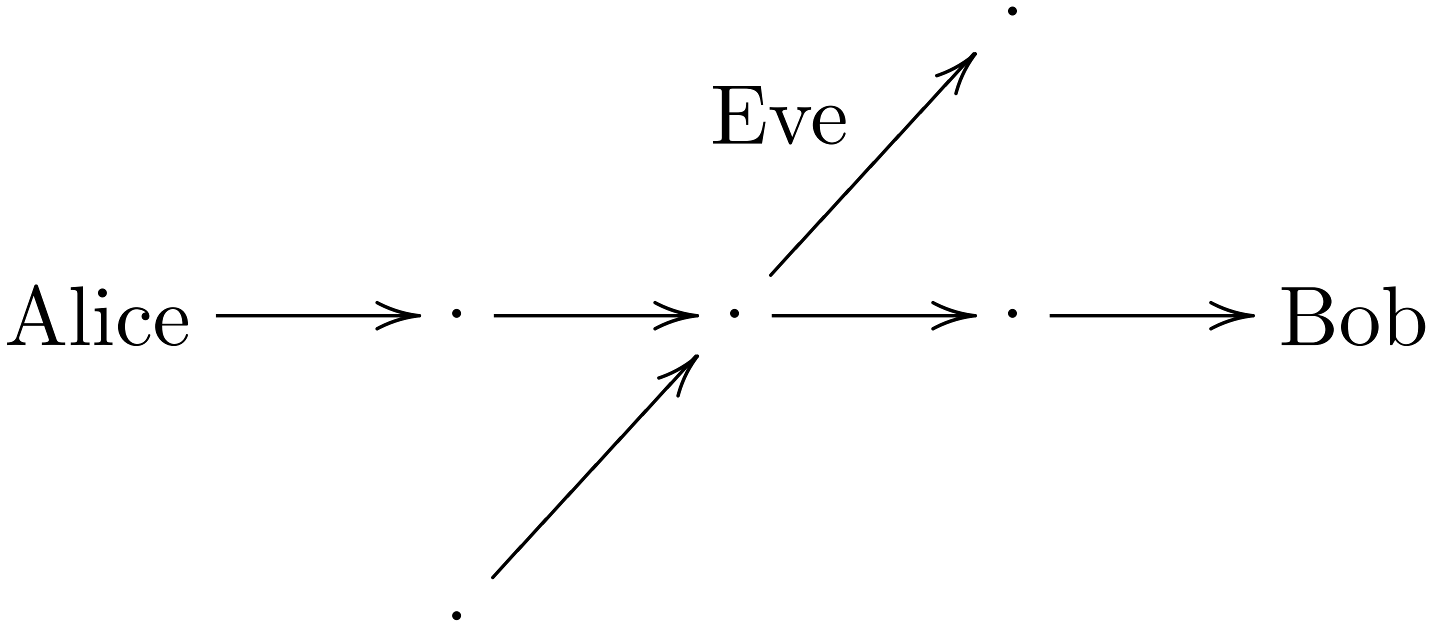
- Quantum communication: Alice sending quantum data to Bob, and Eve intercepts.

Our Setting Today

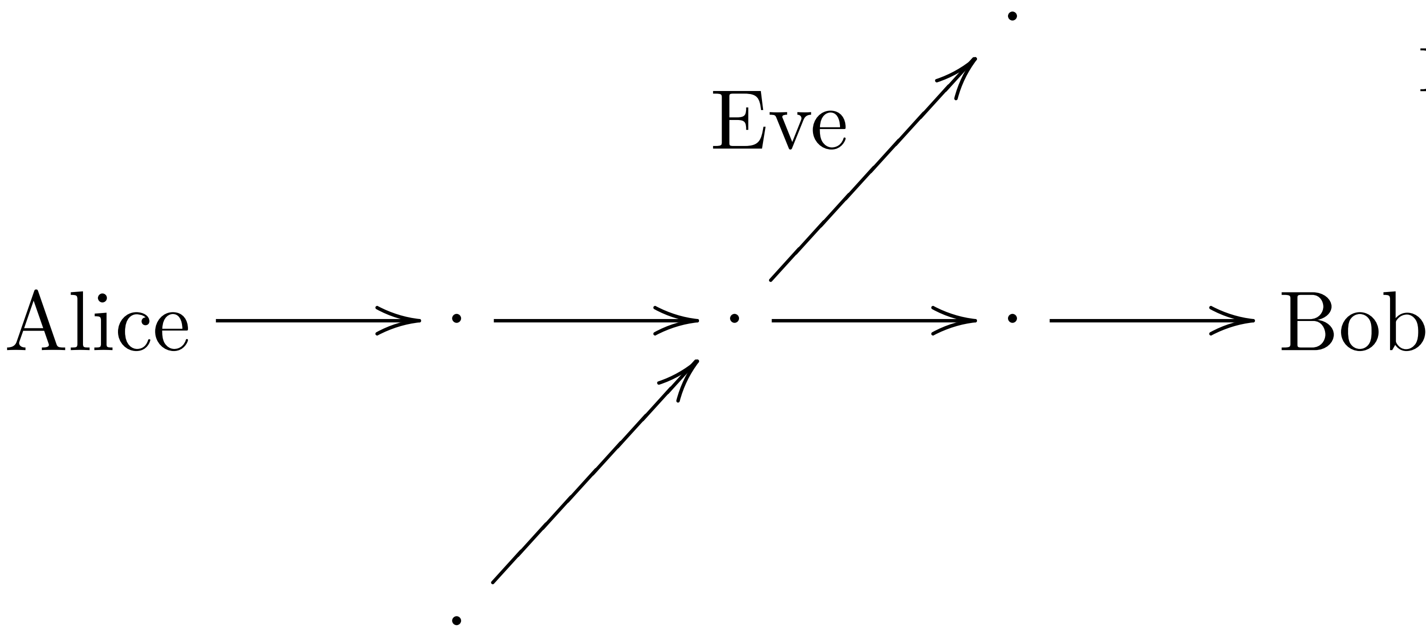
- Quantum communication: Alice sending quantum data to Bob, and Eve intercepts.
- However, Eve is accelerating so gets Unruh noise.

Our Setting Today

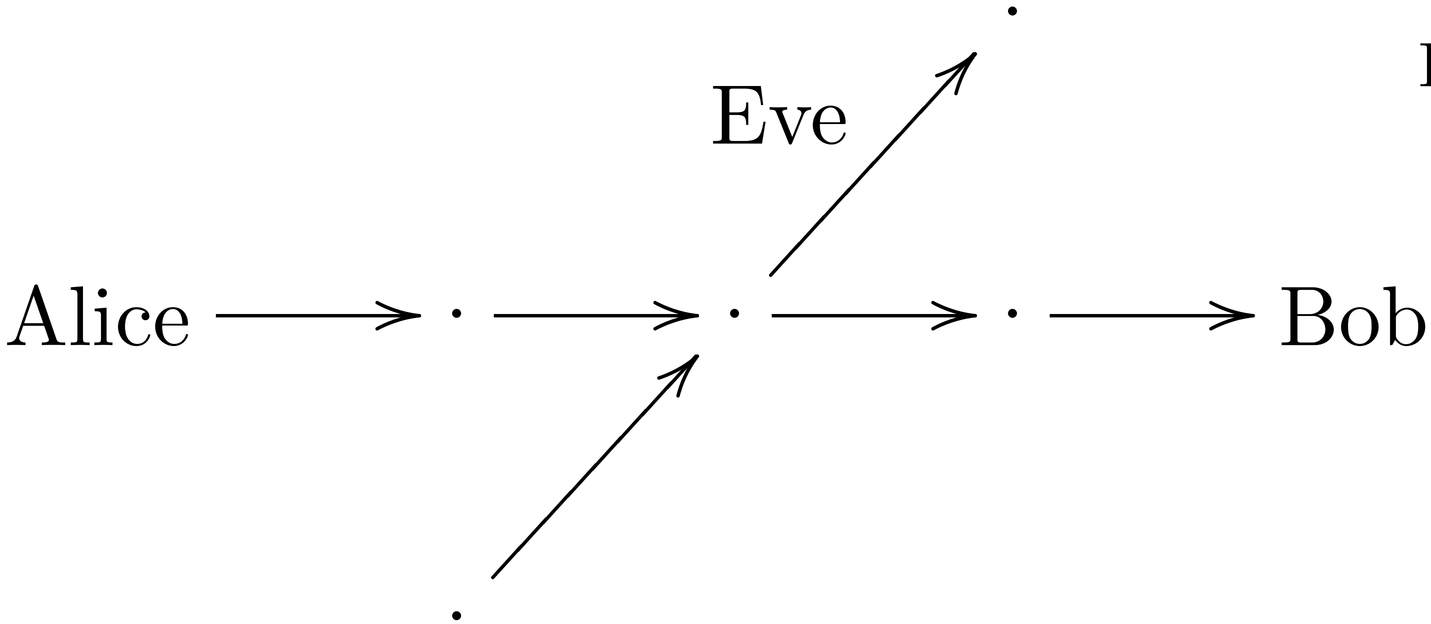
- Quantum communication: Alice sending quantum data to Bob, and Eve intercepts.
- However, Eve is accelerating so gets Unruh noise.
- What is the private capacity for Alice to Bob? Can we use the Unruh noise?

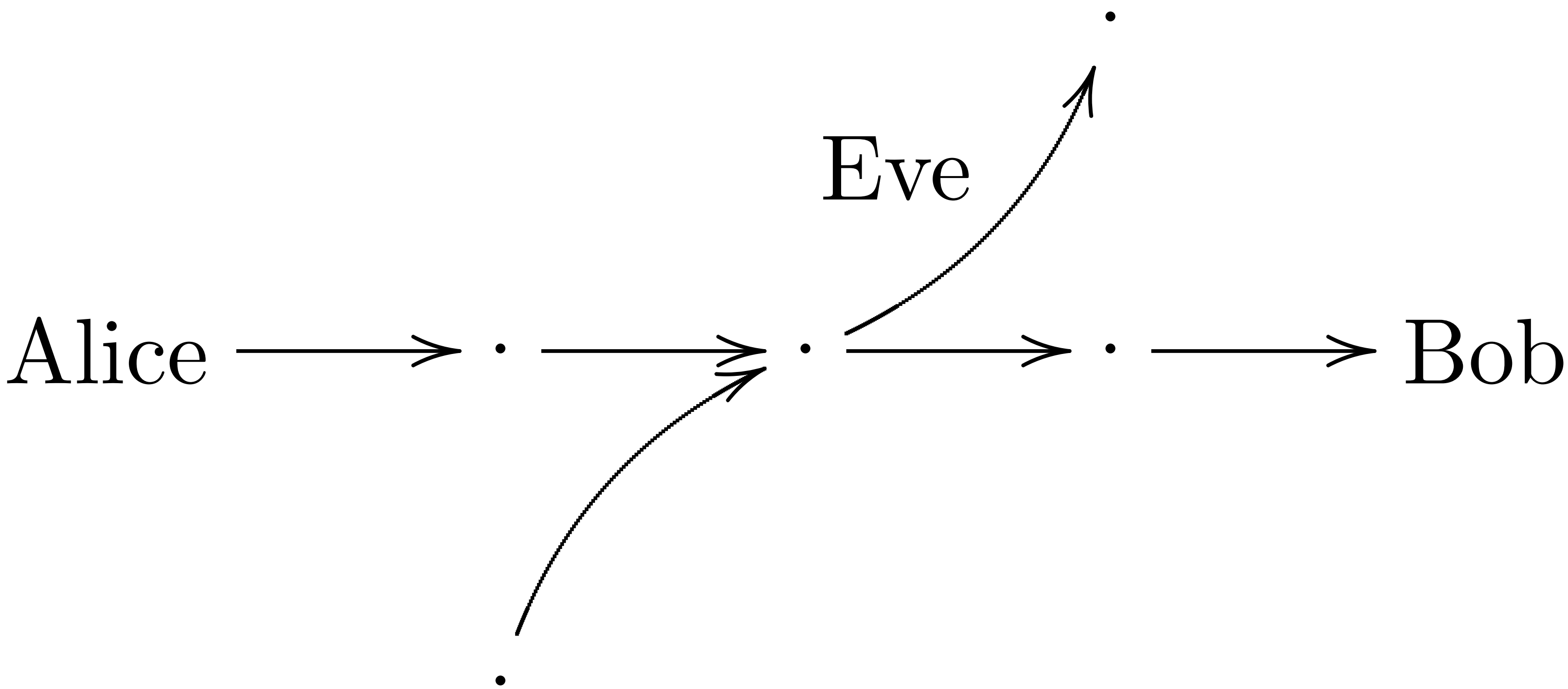

Eve
Alice
Bob

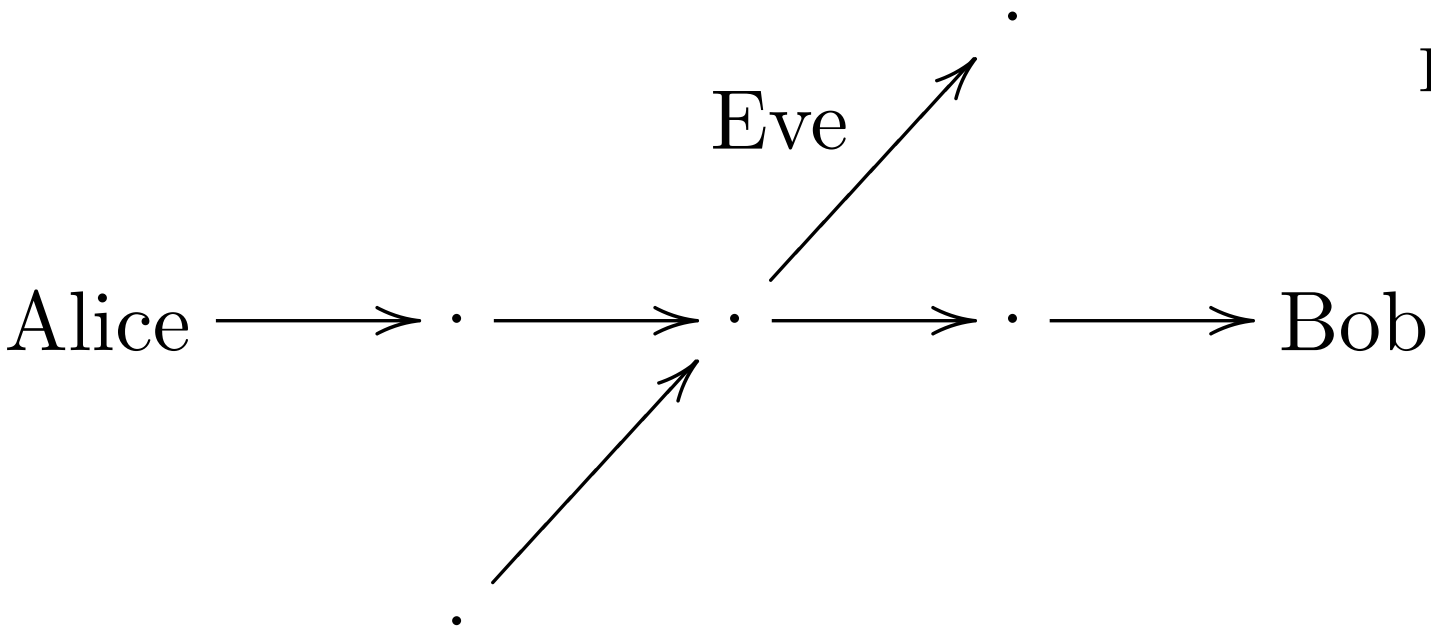
Eve intercepts.



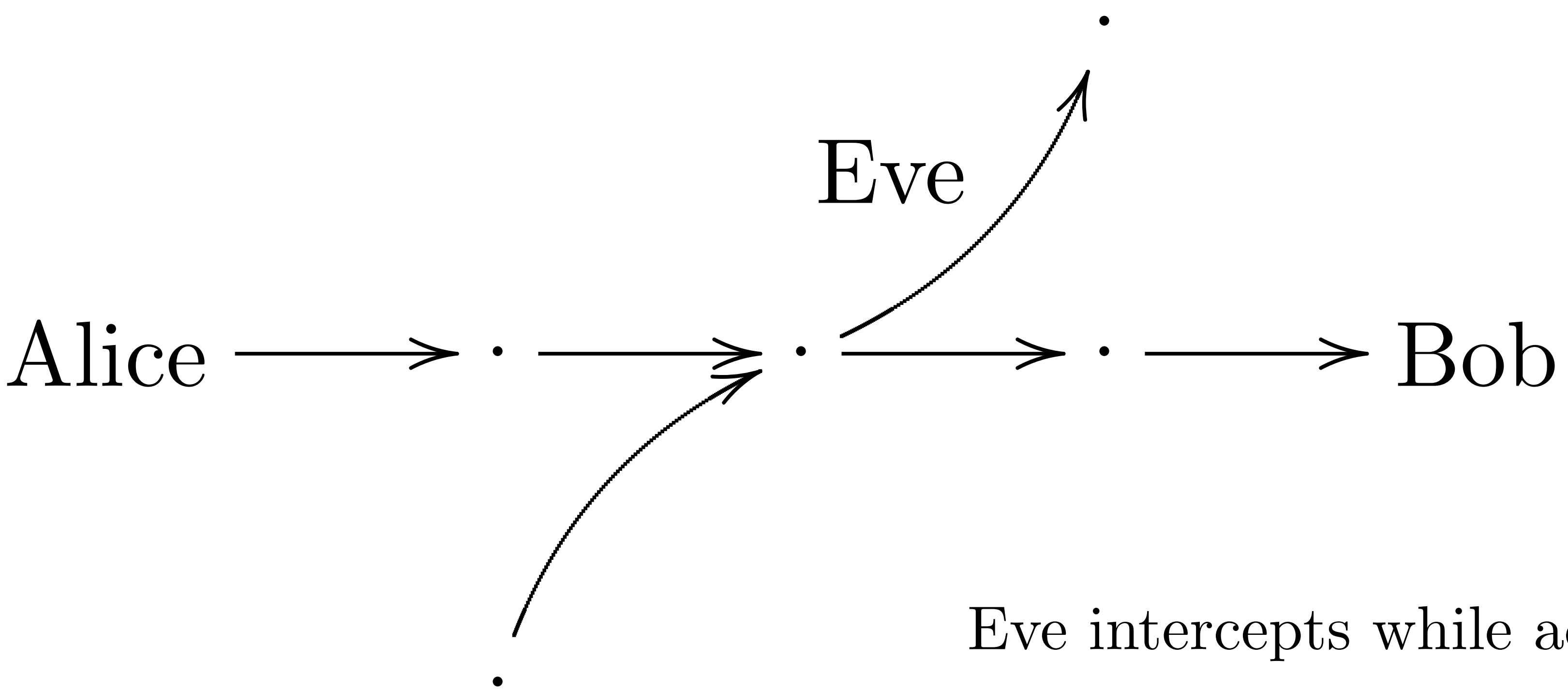
Eve intercepts.







Eve intercepts.



Eve intercepts while accelerating.

$$\text{Alice} \longrightarrow \mathcal{N} \longrightarrow \text{Bob}$$

$$\text{Alice} \longrightarrow \mathcal{N} \longrightarrow \text{Bob}$$

$$\text{Alice} \longrightarrow \mathcal{E} \longrightarrow \text{Eve}$$

$$\text{Alice} \longrightarrow \mathcal{N} \longrightarrow \text{Bob}$$

$$\text{Alice} \longrightarrow \mathcal{E} \longrightarrow \text{Eve}$$

Eve is not a "part" of the environment $[Eve \not\subseteq Env]$

$$\text{Alice} \longrightarrow \mathcal{N} \longrightarrow \text{Bob}$$

$$\text{Alice} \longrightarrow \mathcal{E} \longrightarrow \text{Eve}$$

Eve is not a "part" of the environment $[Eve \not\subseteq Env]$

Does the Unruh effect give a channel from Alice to Bob with nonzero quantum and classical private capacity?

Alice

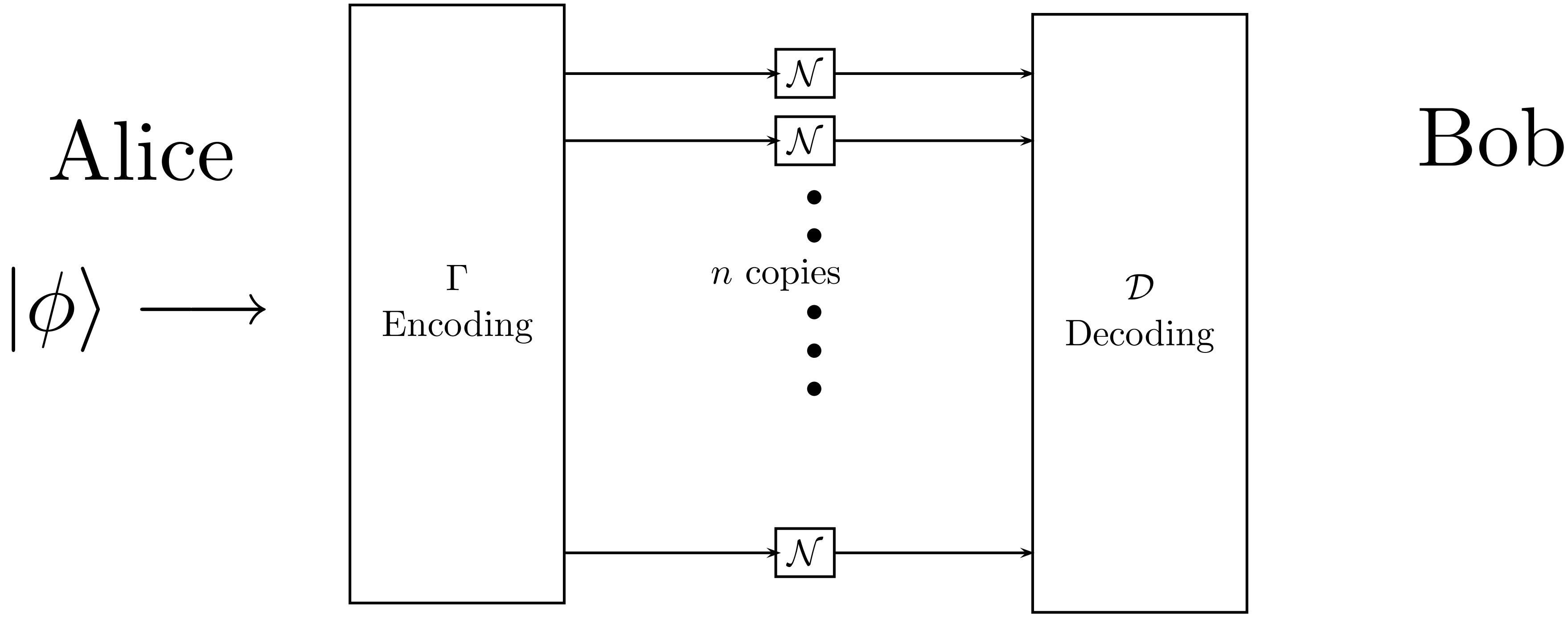
Alice

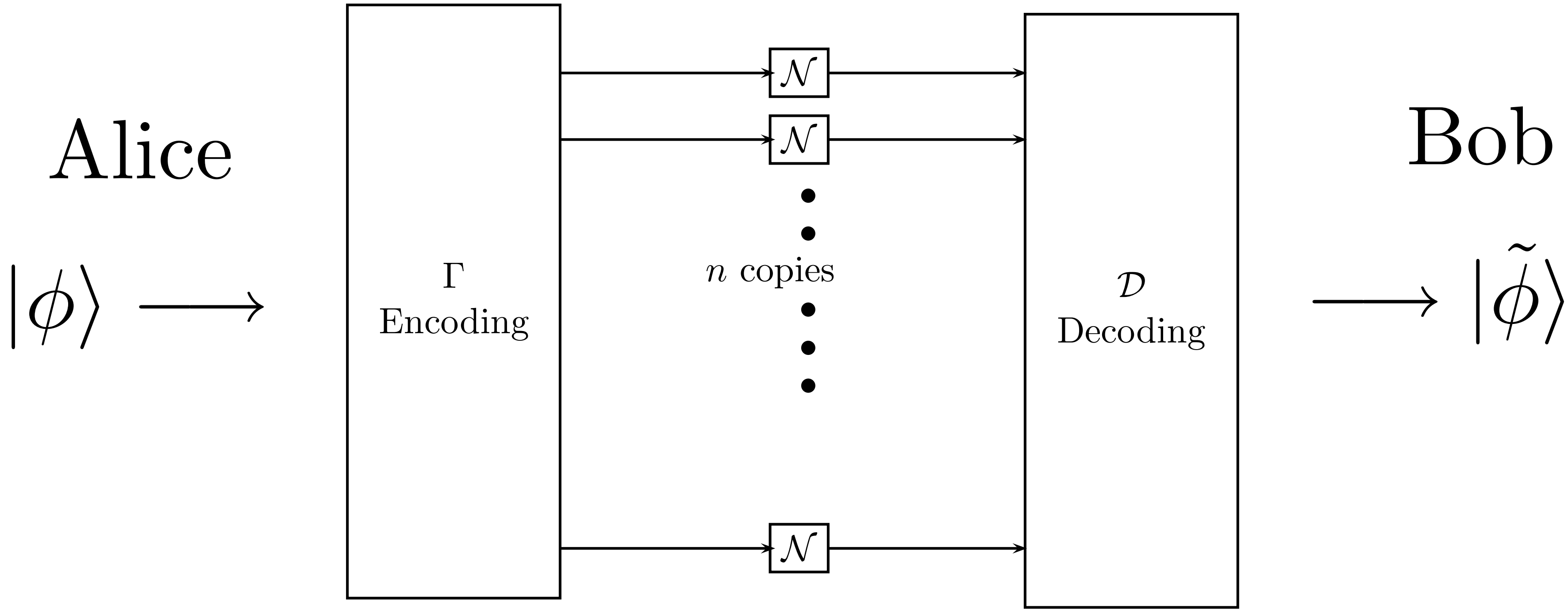
Bob

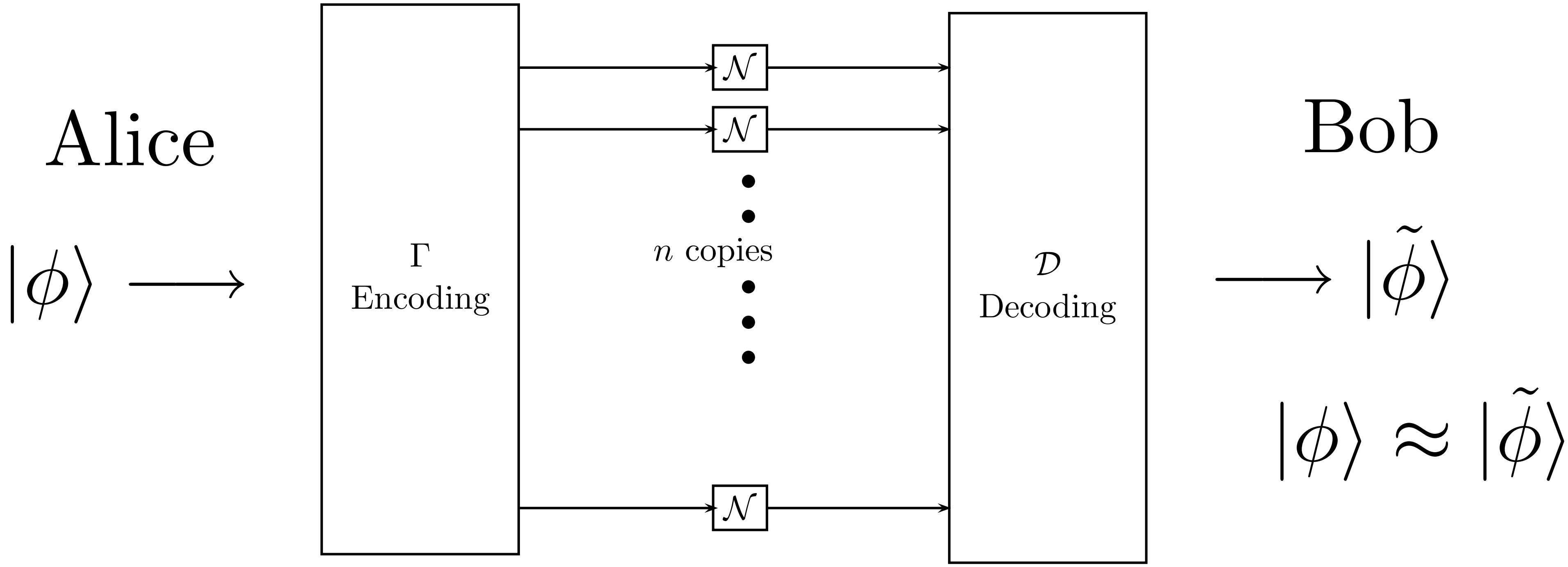
Alice

Bob

$|\phi\rangle \longrightarrow$

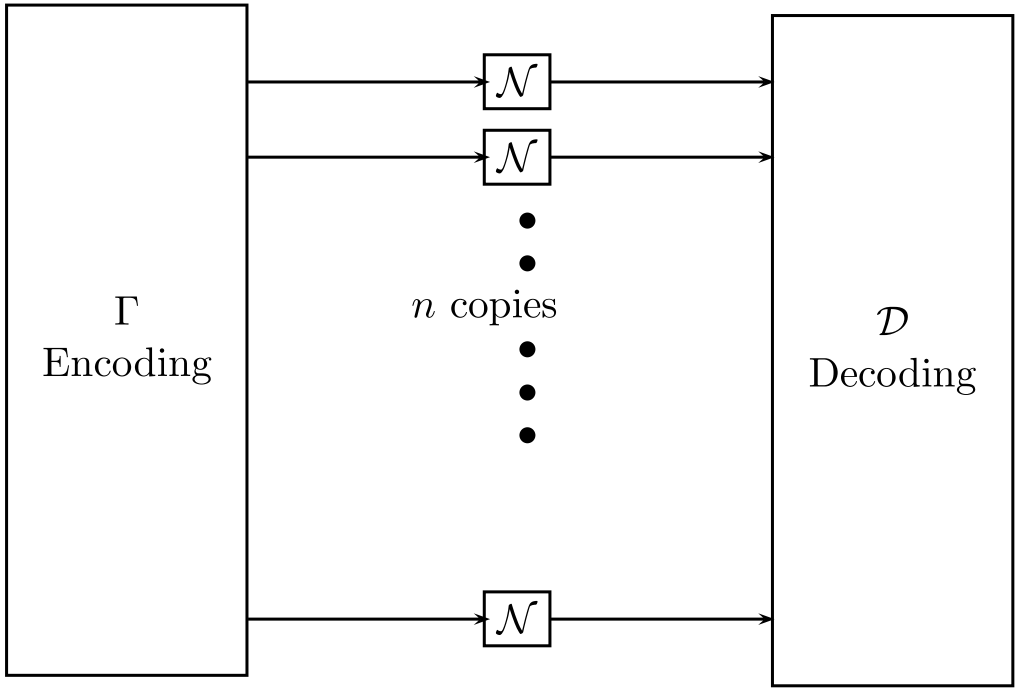

Alice
Bob
$|\phi\rangle \longrightarrow$
Γ
Encoding
$\mathcal{N}$
$\mathcal{N}$
n copies
$\mathcal{N}$
$\mathcal{D}$
Decoding


Alice
$|\phi\rangle \longrightarrow$
Γ
Encoding
$\mathcal{N}$
$\mathcal{N}$
n copies
$\mathcal{N}$
$\mathcal{D}$
Decoding
Bob
$\longrightarrow |\tilde{\phi}\rangle$


Alice
$|\phi\rangle \longrightarrow$
Γ
Encoding
$\mathcal{N}$
$\mathcal{N}$
n copies
$\mathcal{N}$
$\mathcal{D}$
Decoding
Bob
$\longrightarrow |\tilde{\phi}\rangle$
$|\phi\rangle \approx |\tilde{\phi}\rangle$

Alice

$$|\phi\rangle \longrightarrow$$



Bob

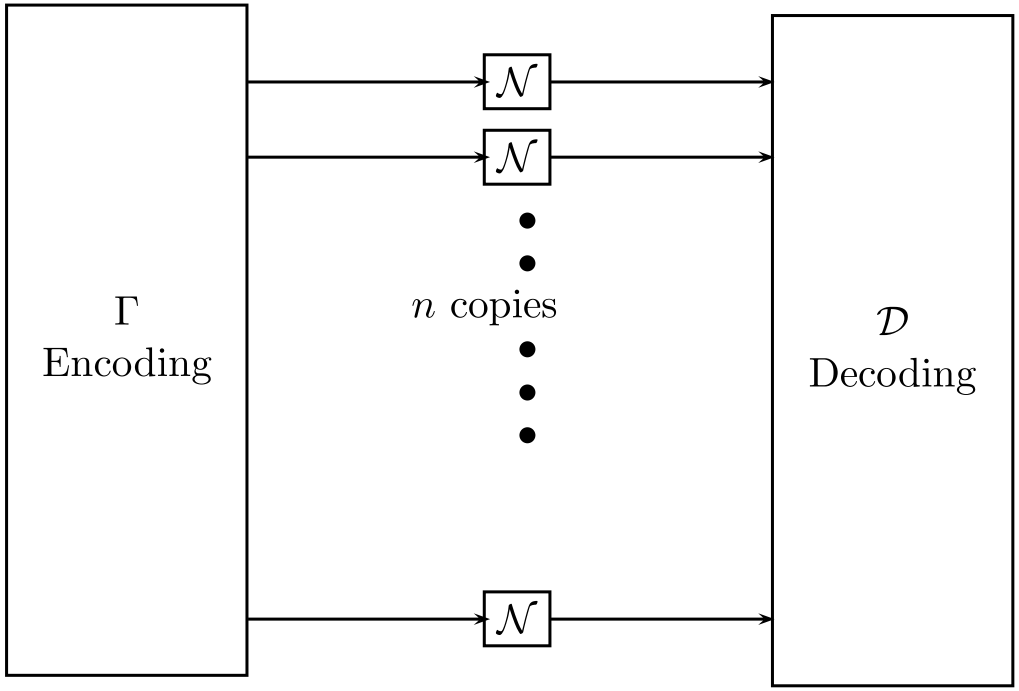
$$\longrightarrow |\tilde{\phi}\rangle$$

$$|\phi\rangle \approx |\tilde{\phi}\rangle$$

Alice

Alice

$|\phi\rangle \longrightarrow$



Bob

$\longrightarrow |\tilde{\phi}\rangle$

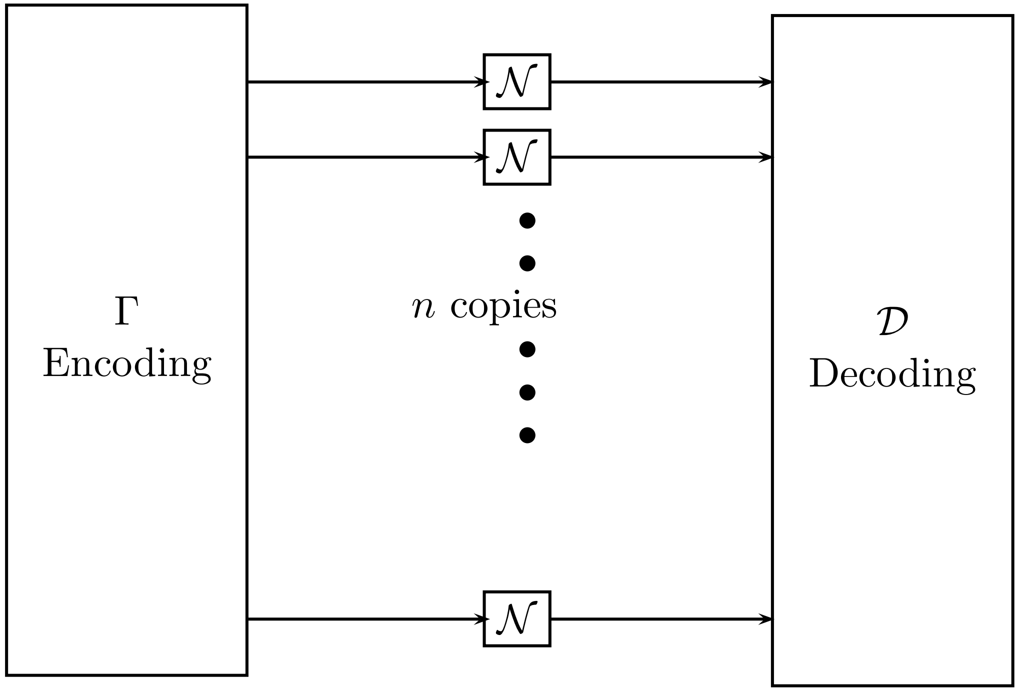
$|\phi\rangle \approx |\tilde{\phi}\rangle$

Alice

$|\phi\rangle \longrightarrow$

Alice

$|\phi\rangle \longrightarrow$



Bob

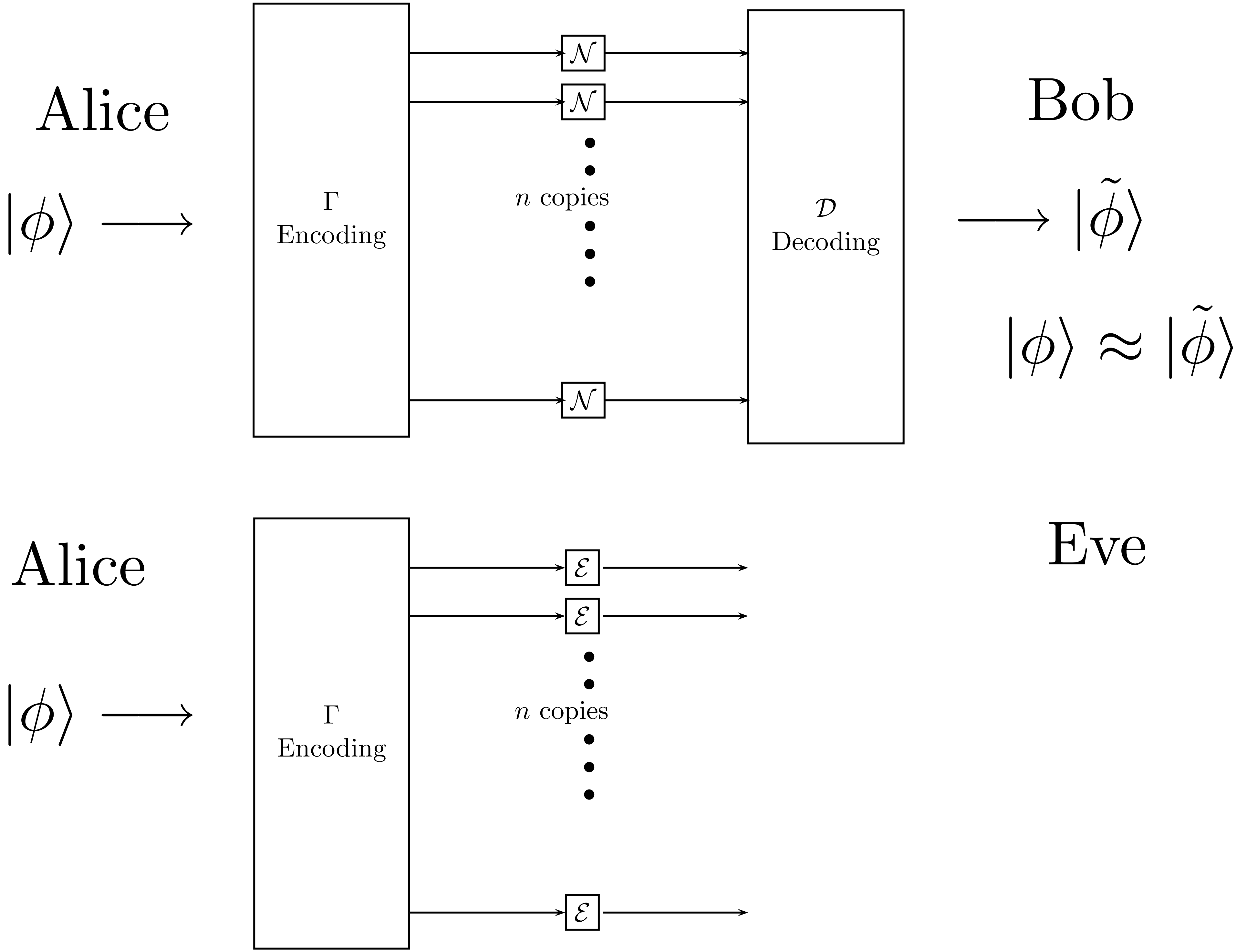
$\longrightarrow |\tilde{\phi}\rangle$

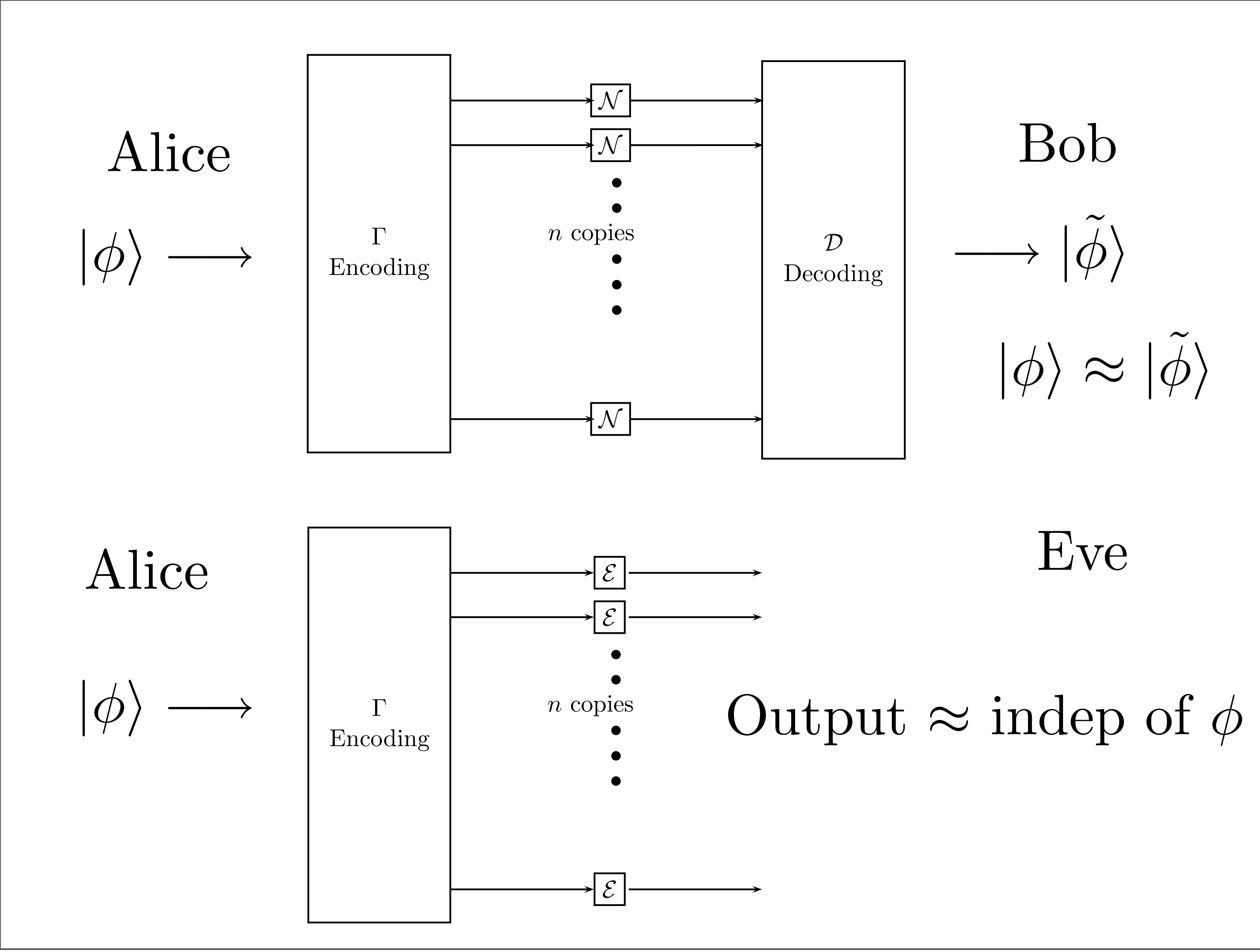
$|\phi\rangle \approx |\tilde{\phi}\rangle$

Alice

Eve

$|\phi\rangle \longrightarrow$


Alice
$|\phi\rangle \longrightarrow$
Γ
Encoding
$\mathcal{N}$
$\mathcal{N}$
n copies
$\mathcal{N}$
$\mathcal{D}$
Decoding
Bob
$\longrightarrow |\tilde{\phi}\rangle$
$|\phi\rangle \approx |\tilde{\phi}\rangle$
Alice
$|\phi\rangle \longrightarrow$
Γ
Encoding
$\mathcal{E}$
$\mathcal{E}$
n copies
$\mathcal{E}$
Eve



Alice
$|\phi\rangle \longrightarrow$
Γ
Encoding
$\mathcal{N}$
$\mathcal{N}$
n copies
$\mathcal{N}$
$\mathcal{D}$
Decoding
Bob
$\longrightarrow |\tilde{\phi}\rangle$
$|\phi\rangle \approx |\tilde{\phi}\rangle$
Alice
$|\phi\rangle \longrightarrow$
Γ
Encoding
$\mathcal{E}$
$\mathcal{E}$
n copies
$\mathcal{E}$
Eve
Output $\approx$ indep of ϕ

Regularization

Quantum informatic quantities are usually computed by:

allowing n uses of the channel and computing

Regularization

Quantum informatic quantities are usually computed by:

allowing n uses of the channel and computing

$$\lim_{n\to\infty} \frac{1}{n} Q(n)$$

Regularization

Quantum informatic quantities are usually computed by:

allowing n uses of the channel and computing

$$\lim_{n\to\infty} \frac{1}{n} Q(n)$$

where Q is the quantity of interest.

Regularization

Quantum informatic quantities are usually computed by:

allowing n uses of the channel and computing

$$\lim_{n\to\infty} \frac{1}{n} Q(n)$$

where Q is the quantity of interest.

1. Easier to compute
2. Essentially using the law of large numbers to get better behaviour

Private classical capacity

of a quantum channel.

Private classical capacity

of a quantum channel.

Alice sends to Bob on id a noiseless channel

Private classical capacity

of a quantum channel.

Alice sends to Bob on id a noiseless channel

Eve receives on a noisy channel $\mathcal{NC}$

Private classical capacity

of a quantum channel.

Alice sends to Bob on id a noiseless channel

Eve receives on a noisy channel $\mathcal{NC}$

We allow n uses of the channel and measure the optimal rate, in bits per channel use, that Alice can send to Bob in such a way that Eve cannot read the messages,

Private classical capacity

of a quantum channel.

Alice sends to Bob on id a noiseless channel

Eve receives on a noisy channel $\mathcal{NC}$

We allow n uses of the channel and measure the optimal rate, in bits per channel use, that Alice can send to Bob in such a way that Eve cannot read the messages,

$$C_p(\mathrm{id}, \mathcal{NC}) = \lim_{n \to \infty} \frac{1}{n} C_p^{(1)}(\mathrm{id}^{\otimes n}, \mathcal{NC}^{\otimes n})$$

Private classical capacity

of a quantum channel.

Alice sends to Bob on id a noiseless channel

Eve receives on a noisy channel $\mathcal{NC}$

We allow n uses of the channel and measure the optimal rate, in bits per channel use, that Alice can send to Bob in such a way that Eve cannot read the messages,

$$C_p(\mathrm{id}, \mathcal{NC}) = \lim_{n \to \infty} \frac{1}{n} C_p^{(1)}(\mathrm{id}^{\otimes n}, \mathcal{NC}^{\otimes n})$$

$$C_p^{(1)}(\mathrm{id}^{\otimes n}, \mathcal{NC}^{\otimes n}) = \max_{\mathcal{Q}} [\chi(\mathcal{Q}) - \chi(\mathcal{NC}^{\otimes n}(\mathcal{Q}))].$$

Private classical capacity

of a quantum channel.

Alice sends to Bob on id a noiseless channel

Eve receives on a noisy channel $\mathcal{NC}$

We allow n uses of the channel and measure the optimal rate, in bits per channel use, that Alice can send to Bob in such a way that Eve cannot read the messages,

$$C_p(\mathrm{id}, \mathcal{NC}) = \lim_{n\to\infty} \frac{1}{n} C_p^{(1)}(\mathrm{id}^{\otimes n}, \mathcal{NC}^{\otimes n})$$

$$C_p^{(1)}(\mathrm{id}^{\otimes n}, \mathcal{NC}^{\otimes n}) = \max_{\mathcal{Q}}[\chi(\mathcal{Q}) - \chi(\mathcal{NC}^{\otimes n}(\mathcal{Q}))].$$

where $\mathcal{Q}$ in an ensemble of pure states on n copies of the channel.

Formalizing Private Quantum Capacity

Given $\mathcal{N}_1$ from Alice to Bob
Given $\mathcal{N}_2$ from Alice to Eve.

Formalizing Private Quantum Capacity

Given $\mathcal{N}_1$ from Alice to Bob
Given $\mathcal{N}_2$ from Alice to Eve.

An (n, k, δ, ϵ) private code is an encoding channel Γ taking k qubits to the input of $\mathcal{N}_1^{\otimes n}$

Formalizing Private Quantum Capacity

Given $\mathcal{N}_1$ from Alice to Bob
Given $\mathcal{N}_2$ from Alice to Eve.

An (n, k, δ, ϵ) private code is an encoding channel Γ taking k qubits to the input of $\mathcal{N}_1^{\otimes n}$

and a decoding channel $\mathcal{D}$ taking Bob's output back to k qubits, such that:

Formalizing Private Quantum Capacity

Given $\mathcal{N}_1$ from Alice to Bob
Given $\mathcal{N}_2$ from Alice to Eve.

An (n, k, δ, ϵ) private code is an encoding channel Γ taking k qubits to the input of $\mathcal{N}_1^{\otimes n}$

and a decoding channel $\mathcal{D}$ taking Bob's output back to k qubits, such that:

$$||(\mathrm{id} \otimes \mathcal{D} \circ \mathcal{N}_1^{\otimes n} \circ \Gamma)(\Phi) - \Phi||_1 \leq \delta$$

Formalizing Private Quantum Capacity

Given $\mathcal{N}_1$ from Alice to Bob
Given $\mathcal{N}_2$ from Alice to Eve.

An (n, k, δ, ϵ) private code is an encoding channel Γ taking k qubits to the input of $\mathcal{N}_1^{\otimes n}$

and a decoding channel $\mathcal{D}$ taking Bob's output back to k qubits, such that:

$$||(\mathrm{id} \otimes \mathcal{D} \circ \mathcal{N}_1^{\otimes n} \circ \Gamma)(\Phi) - \Phi||_1 \leq \delta$$

Φ is the maximally entangled state

Formalizing Private Quantum Capacity

Given $\mathcal{N}_1$ from Alice to Bob
Given $\mathcal{N}_2$ from Alice to Eve.

An (n, k, δ, ϵ) private code is an encoding channel Γ taking k qubits to the input of $\mathcal{N}_1^{\otimes n}$

and a decoding channel $\mathcal{D}$ taking Bob's output back to k qubits, such that:

$$||(\mathrm{id} \otimes \mathcal{D} \circ \mathcal{N}_1^{\otimes n} \circ \Gamma)(\Phi) - \Phi||_1 \leq \delta$$

Φ is the maximally entangled state

$$|| \ldots ||_1 \leq \epsilon$$

Formalizing Private Quantum Capacity

Given $\mathcal{N}_1$ from Alice to Bob
Given $\mathcal{N}_2$ from Alice to Eve.

An (n, k, δ, ϵ) private code is an encoding channel Γ taking k qubits to the input of $\mathcal{N}_1^{\otimes n}$

and a decoding channel $\mathcal{D}$ taking Bob's output back to k qubits, such that:

$$||(\mathrm{id} \otimes \mathcal{D} \circ \mathcal{N}_1^{\otimes n} \circ \Gamma)(\Phi) - \Phi||_1 \leq \delta$$

Φ is the maximally entangled state

$$|| \ldots ||_1 \leq \epsilon$$

Uses $\mathcal{N}_2$ and compares the output with the maximally *mixed* state.

A rate Q is *achievable* if for all δ, ϵ and sufficiently large n there exists an $(n, \lfloor nQ \rfloor, \delta, \epsilon)$ code.

The private quantum capacity is the sup over all achievable rates.

A rate Q is *achievable* if for all δ, ϵ and sufficiently large n there exists an $(n, \lfloor nQ \rfloor, \delta, \epsilon)$ code.

The private quantum capacity is the sup over all achievable rates.

Achievable rates: *Given any pure state* $|\varphi\rangle^{AA'}$, *the rate* $\min(I(A\rangle B)_\rho, H(A|E)_\sigma)$ *is achievable, where* $\rho = (\mathrm{id} \otimes \mathcal{N}_1)(\varphi)$, $\sigma = (\mathrm{id} \otimes \mathcal{N}_2)(\varphi)$, $I(A\rangle B)_\rho = H(B)_\rho - H(AB)_\rho$ *is the coherent information and* $H(A|E)_\sigma = H(AE)_\sigma - H(E)_\sigma$ *the conditional entropy.*

A rate Q is *achievable* if for all δ, ϵ and sufficiently large n there exists an $(n, \lfloor nQ \rfloor, \delta, \epsilon)$ code.

The private quantum capacity is the sup over all achievable rates.

Achievable rates: *Given any pure state* $|\varphi\rangle^{AA'}$, *the rate* $\min(I(A\rangle B)_\rho, H(A|E)_\sigma)$ *is achievable, where* $\rho = (\mathrm{id} \otimes \mathcal{N}_1)(\varphi)$, $\sigma = (\mathrm{id} \otimes \mathcal{N}_2)(\varphi)$, $I(A\rangle B)_\rho = H(B)_\rho - H(AB)_\rho$ *is the coherent information and* $H(A|E)_\sigma = H(AE)_\sigma - H(E)_\sigma$ *the conditional entropy.*

So calculating the private capacity involves computing conditional entropies and then minimzing.

The Unruh Channel

The Unruh Channel

Alice and Bob have the same Fock space.

The Unruh Channel

Alice and Bob have the same Fock space.

Alice uses two different modes of the quantum field to encode qubits.

The Unruh Channel

Alice and Bob have the same Fock space.

Alice uses two different modes of the quantum field to encode qubits.

Let the annihilation operators for the two modes be a and b.

The Unruh Channel

Alice and Bob have the same Fock space.

Alice uses two different modes of the quantum field to encode qubits.

Let the annihilation operators for the two modes be a and b.

A Bogolioubov transformation will change the modes to Eve's Fock space.

The Unruh Channel

Alice and Bob have the same Fock space.

Alice uses two different modes of the quantum field to encode qubits.

Let the annihilation operators for the two modes be a and b.

A Bogolioubov transformation will change the modes to Eve's Fock space.

$$
\begin{aligned}
U_{abcd}(r) = U_{ac}(r) \otimes U_{bd}(r) &= e^{r(a^\dagger c^\dagger + b^\dagger d^\dagger) - r(ac+bd)} \\
&= \frac{1}{\cosh^2 r} e^{\tanh r (a^\dagger c^\dagger + b^\dagger d^\dagger)} \\
&\times e^{-\ln \cosh r (a^\dagger a + b^\dagger b + c^\dagger c + d^\dagger d)} e^{-\tanh r (ac+bd)}.
\end{aligned}
$$

The Unruh Channel

Alice and Bob have the same Fock space.

Alice uses two different modes of the quantum field to encode qubits.

Let the annihilation operators for the two modes be a and b.

A Bogolioubov transformation will change the modes to Eve's Fock space.

$$\begin{aligned} U_{abcd}(r) = U_{ac}(r) \otimes U_{bd}(r) &= e^{r(a^\dagger c^\dagger + b^\dagger d^\dagger) - r(ac+bd)} \\ &= \frac{1}{\cosh^2 r} e^{\tanh r(a^\dagger c^\dagger + b^\dagger d^\dagger)} \\ &\times e^{-\ln\cosh r(a^\dagger a + b^\dagger b + c^\dagger c + d^\dagger d)} e^{-\tanh r(ac+bd)}. \end{aligned}$$

The output density matrix is infinite dimensional and block diagonal.

The Unruh Channel

Alice and Bob have the same Fock space.

Alice uses two different modes of the quantum field to encode qubits.

Let the annihilation operators for the two modes be a and b.

A Bogolioubov transformation will change the modes to Eve's Fock space.

$$
\begin{aligned}
U_{abcd}(r) = U_{ac}(r) \otimes U_{bd}(r) &= e^{r(a^\dagger c^\dagger + b^\dagger d^\dagger) - r(ac+bd)} \\
&= \frac{1}{\cosh^2 r} e^{\tanh r (a^\dagger c^\dagger + b^\dagger d^\dagger)} \\
&\times e^{-\ln \cosh r (a^\dagger a + b^\dagger b + c^\dagger c + d^\dagger d)} e^{-\tanh r (ac+bd)}.
\end{aligned}
$$

The output density matrix is infinite dimensional and block diagonal.

The only hope: deal with it block by block.

Hayden's black magic

Hayden's black magic

Aha!

The blocks are irreducible representations of $SU(2)$!!

Hayden's black magic

Aha!
The blocks are irreducible representations of $SU(2)$!!

So we can use some simple Lie theory to diagonalize all the blocks at once!

Hayden's black magic

Aha!
The blocks are irreducible representations of $SU(2)$!!

So we can use some simple Lie theory to diagonalize all the blocks at once!

$\sigma = \mathcal{N}(\rho)$ with $\rho = \mathbb{1}/2 + \vec{n} \cdot J^{(2)}$ arbitrary, then

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

Hayden's black magic

Aha!
The blocks are irreducible representations of $SU(2)$!!

So we can use some simple Lie theory to diagonalize all the blocks at once!

$\sigma = \mathcal{N}(\rho)$ with $\rho = \mathbb{1}/2 + \vec{n} \cdot J^{(2)}$ arbitrary, then

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

Now we can calculate the entropies and

Hayden's black magic

Aha!
The blocks are irreducible representations of $SU(2)$!!

So we can use some simple Lie theory to diagonalize all the blocks at once!

$$\sigma = \mathcal{N}(\rho) \text{ with } \rho = \mathbb{1}/2 + \vec{n} \cdot J^{(2)} \text{ arbitrary, then}$$

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

Now we can calculate the entropies and with a bit of work

Hayden's black magic

Aha!
The blocks are irreducible representations of $SU(2)$!!

So we can use some simple Lie theory to diagonalize all the blocks at once!

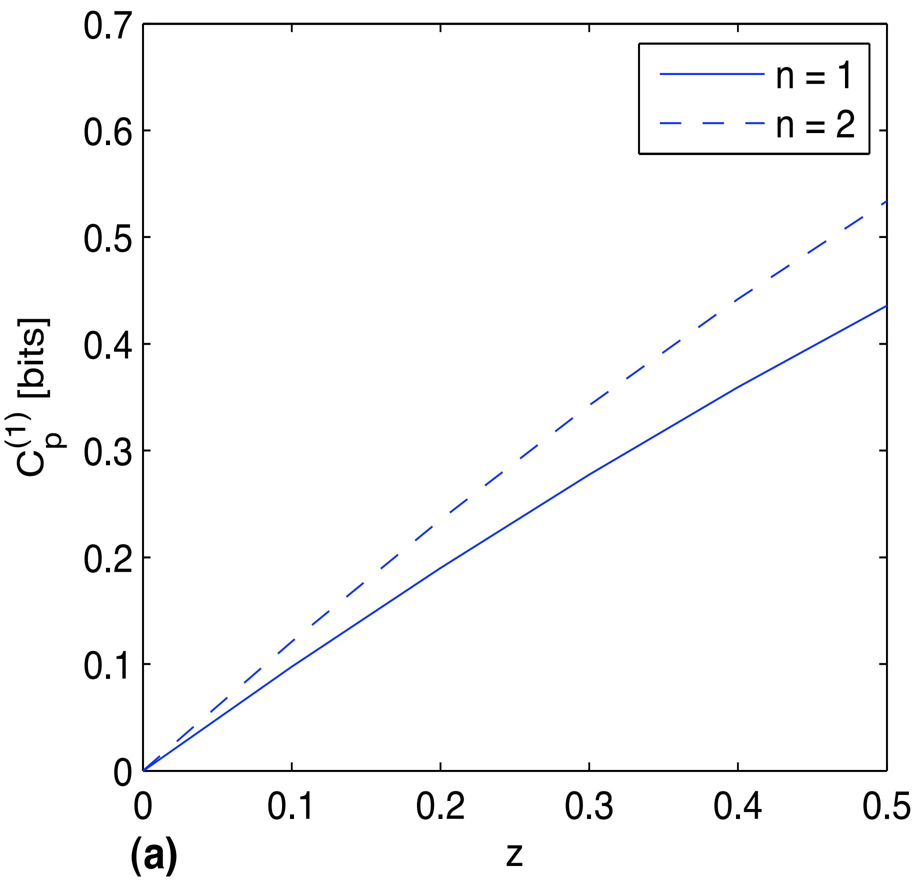
$$\sigma = \mathcal{N}(\rho) \text{ with } \rho = \mathbb{1}/2 + \vec{n} \cdot J^{(2)} \text{ arbitrary, then}$$

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

Now we can calculate the entropies and the private capacities.

with a bit of work

The classical private capacitiy is not zero and depends on the acceleration.



The quantum private capacitiy is zero!?

The quantum private capacitiy is zero!?

Only if we assume isometric encodings.

The quantum private capacitiy is zero!?

Only if we assume isometric encodings.

A non-isometric encoding.

The quantum private capacitiy is zero!?

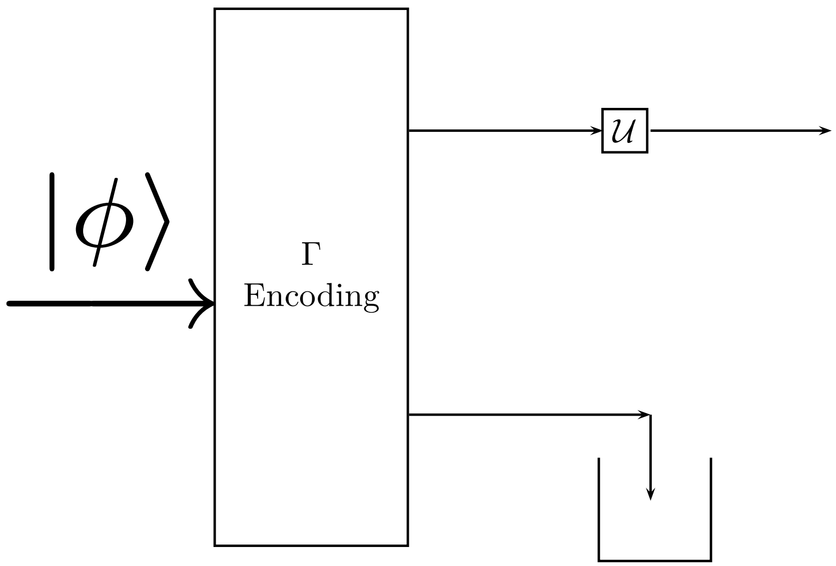
Only if we assume isometric encodings.

$$\xrightarrow{|\phi\rangle}$$

A non-isometric encoding.

The quantum private capacitiy is zero!?

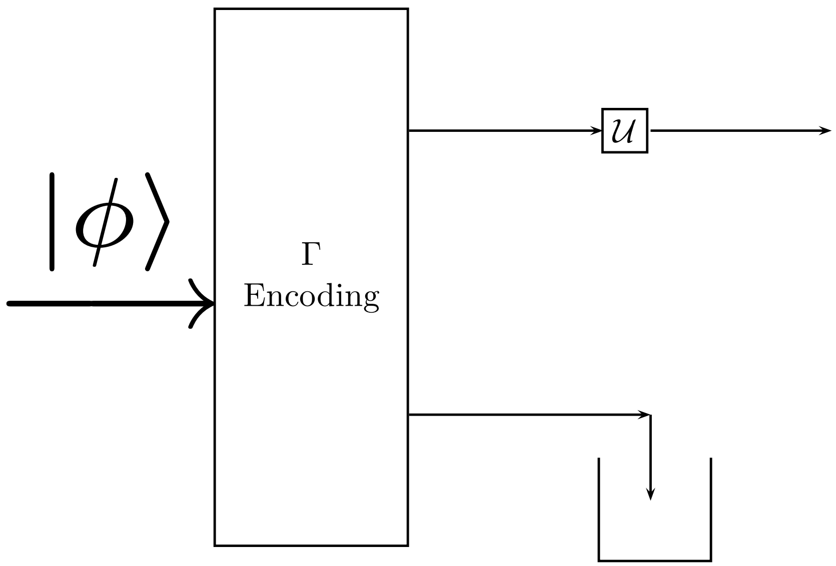
Only if we assume isometric encodings.



A non-isometric encoding.

The quantum private capacitiy is zero!?

Only if we assume isometric encodings.



Part of the output is discarded

A non-isometric encoding.

Conclusions

Conclusions

Quantum information theory is affected in non-trivial ways by relativistic effects.

Conclusions

Quantum information theory is affected in non-trivial ways by relativistic effects.

The effect of horizons is particularly interesting.

Conclusions

Quantum information theory is affected in non-trivial ways by relativistic effects.

The effect of horizons is particularly interesting.

First nontrivial example where quantum private capacity has been calculated

Conclusions

Quantum information theory is affected in non-trivial ways by relativistic effects.

The effect of horizons is particularly interesting.

First nontrivial example where quantum private capacity has been calculated

Calculations used symmetry (representation theory of $SU(2)$).

Conclusions

Quantum information theory is affected in non-trivial ways by relativistic effects.

The effect of horizons is particularly interesting.

First nontrivial example where quantum private capacity has been calculated

Calculations used symmetry (representation theory of $SU(2)$).

We can deal with n-ary states (are they really called "nits?")
using representation theory of $SU(N)$.

Conclusions

Quantum information theory is affected in non-trivial ways by relativistic effects.

The effect of horizons is particularly interesting.

First nontrivial example where quantum private capacity has been calculated

Calculations used symmetry (representation theory of $SU(2)$).

We can deal with n-ary states (are they really called "nits?") using representation theory of $SU(N)$.

Next stop: Hawking radiation from black holes.