Transferencia de estados cuánticos

Omar Osenda

Facultad de Matemática, Astronomía y Física
Universidad Nacional de Córdoba

11 de Octubre de 2011- GTMC

Información cuántica

- Información y computación cuántica
- Cómo se codifica la información en la naturaleza
- Cuál es el poder computacional de la misma

Una posible definición

La información cuántica trata al estado cuántico como su objeto, los observables o las propiedades espectrales pasan a un segundo plano

Información cuántica

- Información y computación cuántica
- Cómo se codifica la información en la naturaleza
- Cuál es el poder computacional de la misma

Una posible definición

La información cuántica trata al estado cuántico como su objeto, los observables o las propiedades espectrales pasan a un segundo plano

Información cuántica

- Información y computación cuántica
- Cómo se codifica la información en la naturaleza
- Cuál es el poder computacional de la misma

Una posible definición

La información cuántica trata al estado cuántico como su objeto, los observables o las propiedades espectrales pasan a un segundo plano

Información cuántica

- Información y computación cuántica
- Cómo se codifica la información en la naturaleza
- Cuál es el poder computacional de la misma

Una posible definición

La información cuántica trata al estado cuántico como su objeto, los observables o las propiedades espectrales pasan a un segundo plano

Cuándo comenzó?

- Algoritmo de factorización cuántico [Shor 93]
- Distribución de llaves seguras [Bennet-Brassard 84]
- Las computadoras cuánticas probablemente no resolverán problemas NP-completos [BBBV 94]

Cuándo comenzó?

- Algoritmo de factorización cuántico [Shor 93]
- Distribución de llaves seguras [Bennet-Brassard 84]
- Las computadoras cuánticas probablemente no resolverán problemas NP-completos [BBBV 94]

Cuándo comenzó?

- Algoritmo de factorización cuántico [Shor 93]
- Distribución de llaves seguras [Bennet-Brassard 84]
- Las computadoras cuánticas probablemente no resolverán problemas NP-completos [BBBV 94]

Bases de la Información Cuántica

- Bit Cuántico (qubit): lo que lleva la información
  - un sistema cuántico el cual puede estar en un estado $|0\rangle$, $|1\rangle$ o en cualquier combinación convexa de los mismos

$$a_0|0\rangle + a_1|1\rangle, \quad a_0, a_1 \in \mathcal{C}, \quad |a_0|^2 + |a_1|^2 = 1$$

- Ejemplos Físicos
  spin de un electrón, el spin de un núcleo, la polarización de un fotón, átomo de dos niveles
- En lo que nos concierne un qubit es un objeto matemático abstracto, es decir un vector unitario en un espacio de Hilbert 2D

Bases de la Información Cuántica

- Bit Cuántico (qubit): lo que lleva la información
  - un sistema cuántico el cual puede estar en un estado $|0\rangle$, $|1\rangle$ o en cualquier combinación convexa de los mismos

$$a_0|0\rangle + a_1|1\rangle, \quad a_0, a_1 \in \mathcal{C}, \quad |a_0|^2 + |a_1|^2 = 1$$

- Ejemplos Físicos
  spin de un electrón, el spin de un núcleo, la polarización de un fotón, átomo de dos niveles
- En lo que nos concierne un qubit es un objeto matemático abstracto, es decir un vector unitario en un espacio de Hilbert 2D

Bases de la Información Cuántica

- Bit Cuántico (qubit): lo que lleva la información
  - un sistema cuántico el cual puede estar en un estado $|0\rangle$, $|1\rangle$ o en cualquier combinación convexa de los mismos

$$a_0|0\rangle + a_1|1\rangle, \quad a_0, a_1 \in \mathcal{C}, \quad |a_0|^2 + |a_1|^2 = 1$$

- Ejemplos Físicos
  spin de un electrón, el spin de un núcleo, la polarización de un fotón, átomo de dos niveles
- En lo que nos concierne un qubit es un objeto matemático abstracto, es decir un vector unitario en un espacio de Hilbert 2D

Bases de la Información Cuántica

- Bit Cuántico (qubit): lo que lleva la información
  - un sistema cuántico el cual puede estar en un estado $|0\rangle$, $|1\rangle$ o en cualquier combinación convexa de los mismos

$$a_0|0\rangle + a_1|1\rangle, \quad a_0, a_1 \in \mathcal{C}, \quad |a_0|^2 + |a_1|^2 = 1$$

- Ejemplos Físicos
  spin de un electrón, el spin de un núcleo, la polarización de un fotón, átomo de dos niveles
- En lo que nos concierne un qubit es un objeto matemático abstracto, es decir un vector unitario en un espacio de Hilbert 2D

Porqué primero la criptografía?

- No se puede medir un sistema cuántico sin perturbarlo
- No se puede determinar simultáneamente la posición y el momento de una partícula con precisión arbitrariamente alta
- No se puede medir simultáneamente la polarización de un fotón en la base horizontal-vertical y simultáneamente en la base diagonal
- No se puede describir procesos cuánticos individuales
- No se puede duplicar un estado cuántico desconocido!!!!!

Porqué primero la criptografía?

- No se puede medir un sistema cuántico sin perturbarlo
- No se puede determinar simultáneamente la posición y el momento de una partícula con precisión arbitrariamente alta
- No se puede medir simultáneamente la polarización de un fotón en la base horizontal-vertical y simultáneamente en la base diagonal
- No se puede describir procesos cuánticos individuales
- No se puede duplicar un estado cuántico desconocido!!!!!

Porqué primero la criptografía?

- No se puede medir un sistema cuántico sin perturbarlo
- No se puede determinar simultáneamente la posición y el momento de una partícula con precisión arbitrariamente alta
- No se puede medir simultáneamente la polarización de un fotón en la base horizontal-vertical y simultáneamente en la base diagonal
- No se puede describir procesos cuánticos individuales
- No se puede duplicar un estado cuántico desconocido!!!!!

Porqué primero la criptografía?

- No se puede medir un sistema cuántico sin perturbarlo
- No se puede determinar simultáneamente la posición y el momento de una partícula con precisión arbitrariamente alta
- No se puede medir simultáneamente la polarización de un fotón en la base horizontal-vertical y simultáneamente en la base diagonal
- No se puede describir procesos cuánticos individuales
- No se puede duplicar un estado cuántico desconocido!!!!!

Porqué primero la criptografía?

- No se puede medir un sistema cuántico sin perturbarlo
- No se puede determinar simultáneamente la posición y el momento de una partícula con precisión arbitrariamente alta
- No se puede medir simultáneamente la polarización de un fotón en la base horizontal-vertical y simultáneamente en la base diagonal
- No se puede describir procesos cuánticos individuales
- No se puede duplicar un estado cuántico desconocido!!!!!

Porqué primero la criptografía?

- en criptografía se suele utilizar la convención de que Alice es el nombre del que envía la información, mientras que Bob es quien la recibe, y Eve es quien pretende robarla
- No hay perturbación => No hubo medición => no hubo espionaje
- Así, si la comunicación es cuántica, esto es, usando sistemas cuánticos, Eve no puede obtener información sin introducir perturbaciones que revelen su presencia

Porqué primero la criptografía?

- en criptografía se suele utilizar la convención de que Alice es el nombre del que envía la información, mientras que Bob es quien la recibe, y Eve es quien pretende robarla
- No hay perturbación => No hubo medición => no hubo espionaje
- Así, si la comunicación es cuántica, esto es, usando sistemas cuánticos, Eve no puede obtener información sin introducir perturbaciones que revelen su presencia

Porqué primero la criptografía?

- en criptografía se suele utilizar la convención de que Alice es el nombre del que envía la información, mientras que Bob es quien la recibe, y Eve es quien pretende robarla
- No hay perturbación => No hubo medición => no hubo espionaje
- Así, si la comunicación es cuántica, esto es, usando sistemas cuánticos, Eve no puede obtener información sin introducir perturbaciones que revelen su presencia

Información clásica

- Es discreta
- Unidad elemental : bit, con estados 0 y 1
- Codificación: ejemplo, se puede asignar a cada símbolo su código ASCII en forma binaria y agregarle un bit para checkear paridad. Por ejemplo quanta puede codificarse como 11100010 11101011 11000011 11011101 11101000 11000011
- Los bits son almacenadas físicamente y son estados macroscópicos distinguibles y son bastantes estables y robustos

Información clásica

- Es discreta
- Unidad elemental : bit, con estados 0 y 1
- Codificación: ejemplo, se puede asignar a cada símbolo su código ASCII en forma binaria y agregarle un bit para checkear paridad. Por ejemplo quanta puede codificarse como 11100010 11101011 11000011 11011101 11101000 11000011
- Los bits son almacenadas físicamente y son estados macroscópicos distinguibles y son bastantes estables y robustos

Información clásica

- Es discreta
- Unidad elemental : bit, con estados 0 y 1
- Codificación: ejemplo, se puede asignar a cada símbolo su código ASCII en forma binaria y agregarle un bit para checkear paridad. Por ejemplo quanta puede codificarse como 11100010 11101011 11000011 11011101 11101000 11000011
- Los bits son almacenadas físicamente y son estados macroscópicos distinguibles y son bastantes estables y robustos

Información clásica

- Es discreta
- Unidad elemental : bit, con estados 0 y 1
- Codificación: ejemplo, se puede asignar a cada símbolo su código ASCII en forma binaria y agregarle un bit para checkear paridad. Por ejemplo quanta puede codificarse como 11100010 11101011 11000011 11011101 11101000 11000011
- Los bits son almacenadas físicamente y son estados macroscópicos distinguibles y son bastantes estables y robustos

Información clásica

- los bits pueden ser copiados o clonados sin ningún problema
- La información es transmitida (comunicación) y/o procesada (computación)

Información clásica

- los bits pueden ser copiados o clonados sin ningún problema
- La información es transmitida (comunicación) y/o procesada (computación)

Estados y operadores

- Quantum bit o qubit (Shumacher, 1995). Sistema cuántico bidimensional (spin 1/2, polarización de un fotón, etc etc) con un espacio de Hilbert isomórfico a $\mathcal{C}^2$
- Estados base $|0\rangle \equiv \begin{pmatrix} 1 \\ 0 \end{pmatrix}, |1\rangle \equiv \begin{pmatrix} 0 \\ 1 \end{pmatrix},$
- Una quantum logic gate que actúa sobre un conjunto de registros cuánticos de k qubits es un operador unitario en el espacio de Hilbert asociado $\mathcal{C}^{2^k}$
- Ejemplo: para 1 qubit $U_{not} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \sigma_x$

Estados y operadores

- Quantum bit o qubit (Shumacher, 1995). Sistema cuántico bidimensional (spin 1/2, polarización de un fotón, etc etc) con un espacio de Hilbert isomórfico a $\mathcal{C}^2$
- Estados base $|0\rangle \equiv \begin{pmatrix} 1 \\ 0 \end{pmatrix}$, $|1\rangle \equiv \begin{pmatrix} 0 \\ 1 \end{pmatrix}$,
- Una quantum logic gate que actúa sobre un conjunto de registros cuánticos de k qubits es un operador unitario en el espacio de Hilbert asociado $\mathcal{C}^{2^k}$
- Ejemplo: para 1 qubit $U_{not} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \sigma_x$

Estados y operadores

- Quantum bit o qubit (Shumacher, 1995). Sistema cuántico bidimensional (spin 1/2, polarización de un fotón, etc etc) con un espacio de Hilbert isomórfico a $\mathcal{C}^2$
- Estados base $|0\rangle \equiv \begin{pmatrix} 1 \\ 0 \end{pmatrix}$, $|1\rangle \equiv \begin{pmatrix} 0 \\ 1 \end{pmatrix}$,
- Una quantum logic gate que actúa sobre un conjunto de registros cuánticos de k qubits es un operador unitario en el espacio de Hilbert asociado $\mathcal{C}^{2^k}$
- Ejemplo: para 1 qubit $U_{not} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \sigma_x$

Estados y operadores

- Quantum bit o qubit (Shumacher, 1995). Sistema cuántico bidimensional (spin 1/2, polarización de un fotón, etc etc) con un espacio de Hilbert isomórfico a $\mathcal{C}^2$
- Estados base $|0\rangle \equiv \begin{pmatrix} 1 \\ 0 \end{pmatrix}$, $|1\rangle \equiv \begin{pmatrix} 0 \\ 1 \end{pmatrix}$,
- Una quantum logic gate que actúa sobre un conjunto de registros cuánticos de k qubits es un operador unitario en el espacio de Hilbert asociado $\mathcal{C}^{2^k}$
- Ejemplo: para 1 qubit $U_{not} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \sigma_x$

Compuertas Cuánticas

- Ejemplo: para 2 qubit

$$\begin{aligned} U_{cnot} &= |0\rangle\langle 0| \otimes \mathbb{I} + |1\rangle\langle 1| \otimes U_{not} \\ &= \tfrac{1}{2}(\mathbb{I} + \sigma_z) \otimes \mathbb{I} + \tfrac{1}{2}(\mathbb{I} - \sigma_z) \otimes \sigma_x \end{aligned}$$

- $|0\rangle\langle 0| = \frac{1}{2}(\mathbb{I} + \sigma_z) = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 \end{pmatrix}$

Compuertas Cuánticas

- Ejemplo: para 2 qubit

$$\begin{aligned} U_{cnot} &= |0\rangle\langle 0| \otimes \mathbb{I} + |1\rangle\langle 1| \otimes U_{not} \\ &= \tfrac{1}{2}(\mathbb{I} + \sigma_z) \otimes \mathbb{I} + \tfrac{1}{2}(\mathbb{I} - \sigma_z) \otimes \sigma_x \end{aligned}$$

- $|0\rangle\langle 0| = \frac{1}{2}(\mathbb{I} + \sigma_z) = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 \end{pmatrix}$

Primera aplicación: no cloning theorem

- formulado por Wootters y Zurek (1982) como respuesta a la posibilidad de producir “signaling faster than light”
- $H = H_{orig} \otimes H_{copy}$
- definición de la copiadora cuántica
  $U_{QCM} : |\psi >_{orig} \otimes |\phi_0\rangle_{copy} \rightarrow |\psi >_{orig} \otimes |\psi\rangle_{copy}$
- $|\psi >_{orig} = \alpha_0|0\rangle + \alpha_1|1\rangle$
- $U_{QCM}|\psi >_{orig} |\phi_0\rangle_{copy} = \alpha_0|0\rangle|0\rangle + \alpha_1|1\rangle|1\rangle$
- pero, de acuerdo a la definición
- $U_{QCM}|\psi >_{orig} \otimes |\phi_0\rangle_{copy} = |\psi >_{orig} |\psi\rangle_{copy}$
- $|\psi >_{orig} |\psi\rangle_{copy} = \alpha_0^2|0\rangle|0\rangle + \alpha_0\alpha_1|0\rangle|1\rangle + \alpha_0\alpha_1|1\rangle|0\rangle + \alpha_1^2|1\rangle|1\rangle$

Primera aplicación: no cloning theorem

- formulado por Wootters y Zurek (1982) como respuesta a la posibilidad de producir “signaling faster than light”
- $H = H_{orig} \otimes H_{copy}$
- definición de la copiadora cuántica
  $U_{QCM} : |\psi >_{orig} \otimes |\phi_0\rangle_{copy} \rightarrow |\psi >_{orig} \otimes |\psi\rangle_{copy}$
- $|\psi >_{orig} = \alpha_0|0\rangle + \alpha_1|1\rangle$
- $U_{QCM}|\psi >_{orig} |\phi_0\rangle_{copy} = \alpha_0|0\rangle|0\rangle + \alpha_1|1\rangle|1\rangle$
- pero, de acuerdo a la definición
- $U_{QCM}|\psi >_{orig} \otimes |\phi_0\rangle_{copy} = |\psi >_{orig} |\psi\rangle_{copy}$
- $|\psi >_{orig} |\psi\rangle_{copy} = \alpha_0^2|0\rangle|0\rangle + \alpha_0\alpha_1|0\rangle|1\rangle + \alpha_0\alpha_1|1\rangle|0\rangle + \alpha_1^2|1\rangle|1\rangle$

Primera aplicación: no cloning theorem

- formulado por Wootters y Zurek (1982) como respuesta a la posibilidad de producir “signaling faster than light”
- $H = H_{orig} \otimes H_{copy}$
- definición de la copiadora cuántica
  $U_{QCM} : |\psi >_{orig} \otimes |\phi_0\rangle_{copy} \rightarrow |\psi >_{orig} \otimes |\psi\rangle_{copy}$
- $|\psi >_{orig} = \alpha_0|0\rangle + \alpha_1|1\rangle$
- $U_{QCM}|\psi >_{orig} |\phi_0\rangle_{copy} = \alpha_0|0\rangle|0\rangle + \alpha_1|1\rangle|1\rangle$
- pero, de acuerdo a la definición
- $U_{QCM}|\psi >_{orig} \otimes |\phi_0\rangle_{copy} = |\psi >_{orig} |\psi\rangle_{copy}$
- $|\psi >_{orig} |\psi\rangle_{copy} = \alpha_0^2|0\rangle|0\rangle + \alpha_0\alpha_1|0\rangle|1\rangle + \alpha_0\alpha_1|1\rangle|0\rangle + \alpha_1^2|1\rangle|1\rangle$

Primera aplicación: no cloning theorem

- formulado por Wootters y Zurek (1982) como respuesta a la posibilidad de producir “signaling faster than light”
- $H = H_{orig} \otimes H_{copy}$
- definición de la copiadora cuántica
  $U_{QCM} : |\psi >_{orig} \otimes |\phi_0\rangle_{copy} \rightarrow |\psi >_{orig} \otimes |\psi\rangle_{copy}$
- $|\psi >_{orig} = \alpha_0|0\rangle + \alpha_1|1\rangle$
- $U_{QCM}|\psi >_{orig} |\phi_0\rangle_{copy} = \alpha_0|0\rangle|0\rangle + \alpha_1|1\rangle|1\rangle$
- pero, de acuerdo a la definición
- $U_{QCM}|\psi >_{orig} \otimes |\phi_0\rangle_{copy} = |\psi >_{orig} |\psi\rangle_{copy}$
- $|\psi >_{orig} |\psi\rangle_{copy} = \alpha_0^2|0\rangle|0\rangle + \alpha_0\alpha_1|0\rangle|1\rangle + \alpha_0\alpha_1|1\rangle|0\rangle + \alpha_1^2|1\rangle|1\rangle$

Primera aplicación: no cloning theorem

- formulado por Wootters y Zurek (1982) como respuesta a la posibilidad de producir “signaling faster than light”
- $H = H_{orig} \otimes H_{copy}$
- definición de la copiadora cuántica
  $U_{QCM} : |\psi >_{orig} \otimes |\phi_0\rangle_{copy} \rightarrow |\psi >_{orig} \otimes |\psi\rangle_{copy}$
- $|\psi >_{orig} = \alpha_0|0\rangle + \alpha_1|1\rangle$
- $U_{QCM}|\psi >_{orig} |\phi_0\rangle_{copy} = \alpha_0|0\rangle|0\rangle + \alpha_1|1\rangle|1\rangle$
- pero, de acuerdo a la definición
- $U_{QCM}|\psi >_{orig} \otimes |\phi_0\rangle_{copy} = |\psi >_{orig} |\psi\rangle_{copy}$
- $|\psi >_{orig} |\psi\rangle_{copy} = \alpha_0^2|0\rangle|0\rangle + \alpha_0\alpha_1|0\rangle|1\rangle + \alpha_0\alpha_1|1\rangle|0\rangle + \alpha_1^2|1\rangle|1\rangle$

Primera aplicación: no cloning theorem

- formulado por Wootters y Zurek (1982) como respuesta a la posibilidad de producir “signaling faster than light”
- $H = H_{orig} \otimes H_{copy}$
- definición de la copiadora cuántica
  $U_{QCM} : |\psi >_{orig} \otimes |\phi_0\rangle_{copy} \rightarrow |\psi >_{orig} \otimes |\psi\rangle_{copy}$
- $|\psi >_{orig} = \alpha_0|0\rangle + \alpha_1|1\rangle$
- $U_{QCM}|\psi >_{orig} |\phi_0\rangle_{copy} = \alpha_0|0\rangle|0\rangle + \alpha_1|1\rangle|1\rangle$
- pero, de acuerdo a la definición
- $U_{QCM}|\psi >_{orig} \otimes |\phi_0\rangle_{copy} = |\psi >_{orig} |\psi\rangle_{copy}$
- $|\psi >_{orig} |\psi\rangle_{copy} = \alpha_0^2|0\rangle|0\rangle + \alpha_0\alpha_1|0\rangle|1\rangle + \alpha_0\alpha_1|1\rangle|0\rangle + \alpha_1^2|1\rangle|1\rangle$

Primera aplicación: no cloning theorem

- formulado por Wootters y Zurek (1982) como respuesta a la posibilidad de producir “signaling faster than light”
- $H = H_{orig} \otimes H_{copy}$
- definición de la copiadora cuántica
  $U_{QCM} : |\psi >_{orig} \otimes |\phi_0\rangle_{copy} \rightarrow |\psi >_{orig} \otimes |\psi\rangle_{copy}$
- $|\psi >_{orig} = \alpha_0|0\rangle + \alpha_1|1\rangle$
- $U_{QCM}|\psi >_{orig} |\phi_0\rangle_{copy} = \alpha_0|0\rangle|0\rangle + \alpha_1|1\rangle|1\rangle$
- pero, de acuerdo a la definición
- $U_{QCM}|\psi >_{orig} \otimes |\phi_0\rangle_{copy} = |\psi >_{orig} |\psi\rangle_{copy}$
- $|\psi >_{orig} |\psi\rangle_{copy} = \alpha_0^2|0\rangle|0\rangle + \alpha_0\alpha_1|0\rangle|1\rangle + \alpha_0\alpha_1|1\rangle|0\rangle + \alpha_1^2|1\rangle|1\rangle$

Primera aplicación: no cloning theorem

- formulado por Wootters y Zurek (1982) como respuesta a la posibilidad de producir “signaling faster than light”
- $H = H_{orig} \otimes H_{copy}$
- definición de la copiadora cuántica
  $U_{QCM} : |\psi >_{orig} \otimes |\phi_0\rangle_{copy} \rightarrow |\psi >_{orig} \otimes |\psi\rangle_{copy}$
- $|\psi >_{orig} = \alpha_0|0\rangle + \alpha_1|1\rangle$
- $U_{QCM}|\psi >_{orig} |\phi_0\rangle_{copy} = \alpha_0|0\rangle|0\rangle + \alpha_1|1\rangle|1\rangle$
- pero, de acuerdo a la definición
- $U_{QCM}|\psi >_{orig} \otimes |\phi_0\rangle_{copy} = |\psi >_{orig} |\psi\rangle_{copy}$
- $|\psi >_{orig} |\psi\rangle_{copy} = \alpha_0^2|0\rangle|0\rangle + \alpha_0\alpha_1|0\rangle|1\rangle + \alpha_0\alpha_1|1\rangle|0\rangle + \alpha_1^2|1\rangle|1\rangle$

Segunda aplicación: teleportación

- Bennett *et al.* (1993), formulada para que el Capitán James T. Kirk pueda decir “Beam me up, Scotty!”
- Reglas del juego: Alice quiere teleportar un estado $|\psi\rangle$ a su amigo Bob. Alice posee a $|\psi\rangle$ y la mitad de un par de Bell $|\Phi\rangle$. Bob posee la otra mitad del par de Bell. Ambos operan solo localmente.
- $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$
- $|\Phi\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$
- Estado inicial: $|\psi\rangle \otimes |\Phi\rangle$

Segunda aplicación: teleportación

- Bennett *et al.* (1993), formulada para que el Capitán James T. Kirk pueda decir “Beam me up, Scotty!”
- Reglas del juego: Alice quiere teleportar un estado $|\psi\rangle$ a su amigo Bob. Alice posee a $|\psi\rangle$ y la mitad de un par de Bell $|\Phi\rangle$. Bob posee la otra mitad del par de Bell. Ambos operan solo localmente.
- $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$
- $|\Phi\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$
- Estado inicial: $|\psi\rangle \otimes |\Phi\rangle$

Segunda aplicación: teleportación

- Bennett *et al.* (1993), formulada para que el Capitán James T. Kirk pueda decir “Beam me up, Scotty!”
- Reglas del juego: Alice quiere teleportar un estado $|\psi\rangle$ a su amigo Bob. Alice posee a $|\psi\rangle$ y la mitad de un par de Bell $|\Phi\rangle$. Bob posee la otra mitad del par de Bell. Ambos operan solo localmente.
- $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$
- $|\Phi\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$
- Estado inicial: $|\psi\rangle \otimes |\Phi\rangle$

Segunda aplicación: teleportación

- Bennett *et al.* (1993), formulada para que el Capitán James T. Kirk pueda decir “Beam me up, Scotty!”
- Reglas del juego: Alice quiere teleportar un estado $|\psi\rangle$ a su amigo Bob. Alice posee a $|\psi\rangle$ y la mitad de un par de Bell $|\Phi\rangle$. Bob posee la otra mitad del par de Bell. Ambos operan solo localmente.
- $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$
- $|\Phi\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$
- Estado inicial: $|\psi\rangle \otimes |\Phi\rangle$

Segunda aplicación: teleportación

- Bennett *et al.* (1993), formulada para que el Capitán James T. Kirk pueda decir “Beam me up, Scotty!”
- Reglas del juego: Alice quiere teleportar un estado $|\psi\rangle$ a su amigo Bob. Alice posee a $|\psi\rangle$ y la mitad de un par de Bell $|\Phi\rangle$. Bob posee la otra mitad del par de Bell. Ambos operan solo localmente.
- $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$
- $|\Phi\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$
- Estado inicial: $|\psi\rangle \otimes |\Phi\rangle$

teleportación continuación

Primer paso: Alice aplica

$$U := [(U_H \otimes \mathbb{I})U_{cnot}] \otimes \mathbb{I}$$

lo que da

$$\frac{1}{2}\left[|00\rangle \otimes |\psi\rangle + |01\rangle \otimes X|\psi\rangle + |10\rangle \otimes Z|\psi\rangle + |11\rangle \otimes Y|\psi\rangle\right]$$

donde

$$X = \sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \; Y = \sigma_y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \; Z = \sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

$$U_H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

teleportación continuación

Segundo paso: Alice mide los dos primeros qubits, y obtiene equiprobablemente

$$|00\rangle \quad |01\rangle \quad |10\rangle \quad |11\rangle$$

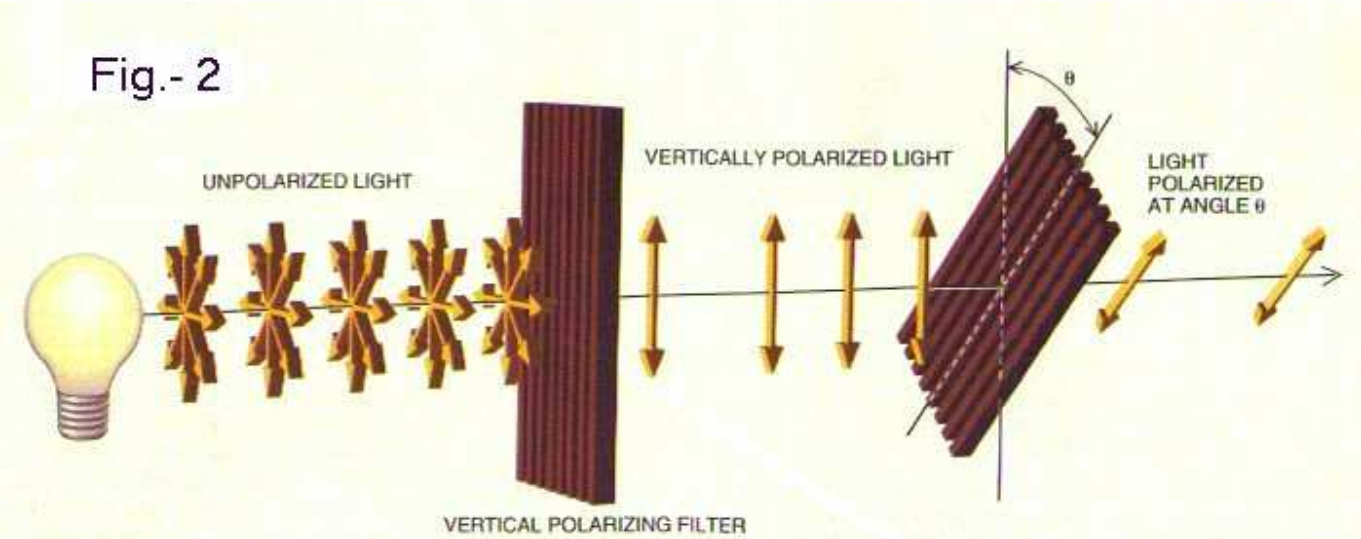
Alice le comunica clásicamente a Bob que ha medido, el estado del tercer bit es

$$|\psi\rangle \quad X|\psi\rangle \quad Z|\psi\rangle \quad Y|\psi\rangle$$

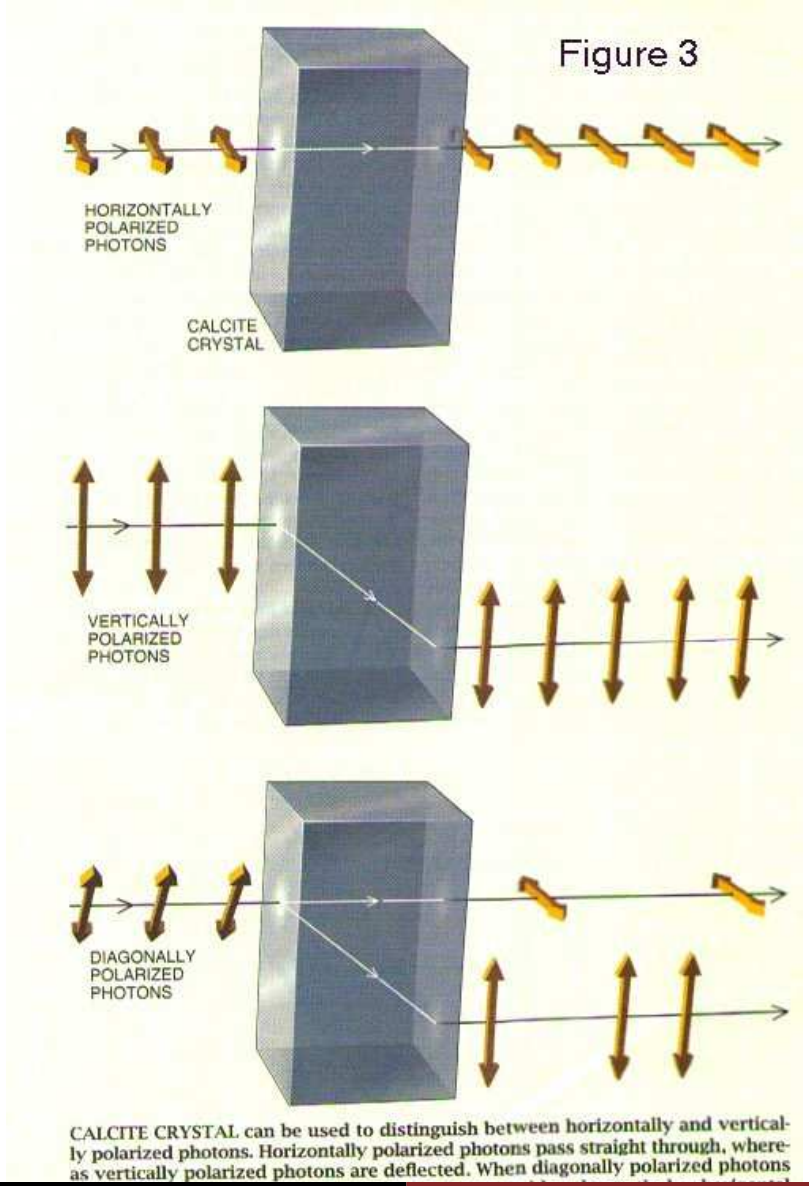
Tercer paso: Bob ha recibido los bits clásicos 0 0, 0 1, 1 0 o 1 1, como $X^2 = Y^2 = Z^2 = \mathbb{I}$ si aplica $\mathbb{I}, X, Z$ o Y, respectivamente, en todos los casos obtiene

$$|\psi\rangle \quad \text{teleportado!!!!}$$

Criptografía: obtención de los estados base



Criptografía: detectando la polarización



CALCITE CRYSTAL can be used to distinguish between horizontally and vertically polarized photons. Horizontally polarized photons pass straight through, whereas vertically polarized photons are deflected. When diagonally polarized photons

Criptografía: protocolo BB84

Quantum Key Distribution

A quantum cryptographic system will allow two people, say, Alice and Bob, to exchange a secret key. The system includes a transmitter and a receiver. Alice uses the transmitter to send photons in one of four polarizations: 0, 45, 90 or 135 degrees. Bobs uses the receiver to measure the polarization. According to the laws of quantum mechanics, the receiver can distinguish between rectilinear polarizations (0 and 90), or it can quickly be reconfigured to discriminate between diagonal polarizations (45 and 135); it can never, however, distinguish both types. The key distribution requires several steps. Alice sends photons with one of four polarizations, which she has chosen at random.

For each photon, Bob chooses at random the type of measurement: either the rectilinear type (+) or the diagonal type (×).

Bob records the result of his measurement but keeps it a secret.

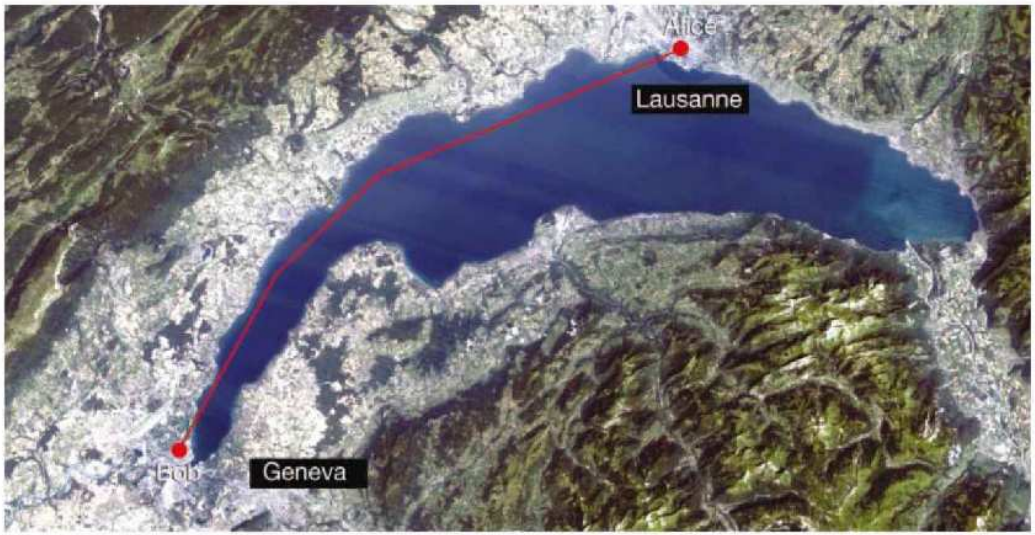
Bob publicly announces the type of measurements he made, and Alice tells him which measurements were of the correct type.

Alice and Bob keep all cases in which Bob measured the correct type. These cases are then translated into bits (1's and 0's) and thereby become the key.

Criptografía: implementación

Photon experiments

Light work: keys encoded using polarized photons have been sent between Alice and Bob (left) through 67 km of fibre-optic cable under Lake Geneva.



Un poco de publicidad

Quantum Security... at last

Quantum Cryptography System

Communicating over optical fiber networks with absolute security

Main features

- Security guaranteed by quantum physics
- Encryption with AES or One-time pad
- Transmission distance up to 100 km
- Automated key management
- High transmission speed

Quantum cryptography exploits a fundamental principle of quantum physics - observation causes perturbation - to distribute cryptographic keys with absolute security and implement secure transmission links over optical fiber networks.

The id Quantique quantum cryptography system can be used to transmit securely information between two sites located in a metropolitan area network.

Applications include connection of remote local area networks, storage area networks, and file servers.

id Quantique
Ch. de la Marbrerie, 3 1227 Carouge Switzerland
Tel. +41 (0)22 301 83 71 Fax +41 (0)22 301 83 79
info@idquantique.com
www.idquantique.com

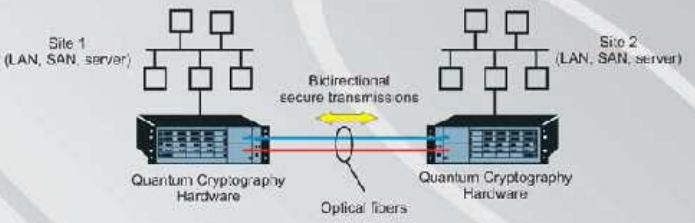
id Quantique
Pi Quantum leaps for Cryptography

Features

Maximum distance[1]	100	Km
Encryption algorithms	AES, One-time pad	

Notes
[1]: Maximum distance varies with actual fiber attenuation.

Deployment scenario



General information

Optical connector[2]	FC/PC	
Data input/output	Ethernet port	
Operating temperature	+10 to +30	°C
Dimension (LxWxH)	32 x 48 x 16	cm
Weight	10	kg
Power supply	110 - 230	VAC

Notes
[2]: Other connector types available upon request

Sales Contact

For further information on this or other products, please contact *id Quantique* by phone: +41 (0)22 301 83 71, fax: +41 (0)22 301 83 79 or email: info@idquantique.com

Disclaimer

The information and specification set forth above are subject to change at any time by *id Quantique* without prior notice. Copyright © id Quantique SA 2004.

algun paper

PRL 98, 010504 (2007) PHYSICAL REVIEW LETTERS week ending 5 JANUARY 2007

Experimental Demonstration of Free-Space Decoy-State Quantum Key Distribution over 144 km

Tobias Schmitt-Manderbach,[1,2,*] Henning Weier,[2] Martin Fürst,[2] Rupert Ursin,[3] Felix Tiefenbacher,[4,3] Thomas Scheidl,[4,3] Josep Perdigues,[5] Zoran Sodnik,[5] Christian Kurtsiefer,[6] John G. Rarity,[7] Anton Zeilinger,[4,3] and Harald Weinfurter[1,2]

[1]*Max-Planck-Institute for Quantum Optics, D-85748 Garching, Germany*
[2]*Department of Physics, Ludwig-Maximilians-University, D-80799 Munich, Germany*
[3]*Institute for Experimental Physics, University of Vienna, A-1090 Vienna, Austria*
[4]*Institute for Quantum Optics and Quantum Information, Austrian Academy of Sciences, A-1090 Vienna, Austria*
[5]*European Space Agency, NL-2200 AG Noordwijk, The Netherlands*
[6]*Department of Physics, National University of Singapore, Singapore 117542, Singapore*
[7]*Department of Electrical and Electronic Engineering, University of Bristol, Bristol BS8 1UB, United Kingdom*

(Received 23 August 2006; published 5 January 2007)

Criterios para computación

1. Well-defined qubits

2. Initialization to a pure state

$|00\ldots0\rangle$

3. Universal set of quantum gates

4. Qubit-specific measurement

5. Long coherence times

$|0\ldots0\rangle + |1\ldots1\rangle$

Criterios para transmisión

6. Interconvert stationary and flying qubits

   Repeater stations
   Distributed quantum computing

7. Transmit flying qubits between distant location

   Quantum communication
   Error correction (communication between differer
   the computer)

...los fotones son buenos

- La tecnología de fibras ópticas, lásers, amplificadores, etc, esta MUY desarrollada
- Todas las compuertas cuánticas de un qubit necesarias se implementan con medios físicos sencillos
- Los modelos teóricos están muy desarrollados
- Los estados base son fácilmente distinguibles
- Las trampas ópticas pueden mantener un número pequeño de fotones atrapados sin perdidas durante décimas de segundo!!!!

...los fotones son buenos

- La tecnología de fibras ópticas, lásers, amplificadores, etc, esta MUY desarrollada
- Todas las compuertas cuánticas de un qubit necesarias se implementan con medios físicos sencillos
- Los modelos teóricos están muy desarrollados
- Los estados base son fácilmente distinguibles
- Las trampas ópticas pueden mantener un número pequeño de fotones atrapados sin perdidas durante décimas de segundo!!!!

...los fotones son buenos

- La tecnología de fibras ópticas, lásers, amplificadores, etc, esta MUY desarrollada
- Todas las compuertas cuánticas de un qubit necesarias se implementan con medios físicos sencillos
- Los modelos teóricos están muy desarrollados
- Los estados base son fácilmente distinguibles
- Las trampas ópticas pueden mantener un número pequeño de fotones atrapados sin perdidas durante décimas de segundo!!!!

...los fotones son buenos

- La tecnología de fibras ópticas, lásers, amplificadores, etc, esta MUY desarrollada
- Todas las compuertas cuánticas de un qubit necesarias se implementan con medios físicos sencillos
- Los modelos teóricos están muy desarrollados
- Los estados base son fácilmente distinguibles
- Las trampas ópticas pueden mantener un número pequeño de fotones atrapados sin perdidas durante décimas de segundo!!!!

...los fotones son buenos

- La tecnología de fibras ópticas, lásers, amplificadores, etc, esta MUY desarrollada
- Todas las compuertas cuánticas de un qubit necesarias se implementan con medios físicos sencillos
- Los modelos teóricos están muy desarrollados
- Los estados base son fácilmente distinguibles
- Las trampas ópticas pueden mantener un número pequeño de fotones atrapados sin perdidas durante décimas de segundo!!!!

...pero no tanto!

- Los tiempos de decoherencia escalean como $1/N$ o más rápido
- La óptica es básicamente lineal! operaciones de dos (o más fotones) son muy difíciles de implementar - se necesita un camino óptico distinto por cada resultado posible $\Rightarrow$ 2^N caminos!!!!!!
- ... es decir, los sistemas de fotones escalean mal!

...pero no tanto!

- Los tiempos de decoherencia escalean como $1/N$ o más rápido
- La óptica es básicamente lineal! operaciones de dos (o más fotones) son muy difíciles de implementar - se necesita un camino óptico distinto por cada resultado posible $\Rightarrow$ 2^N caminos!!!!!!
- ... es decir, los sistemas de fotones escalean mal!

...pero no tanto!

- Los tiempos de decoherencia escalean como $1/N$ o más rápido
- La óptica es básicamente lineal! operaciones de dos (o más fotones) son muy difíciles de implementar - se necesita un camino óptico distinto por cada resultado posible $\Rightarrow$ 2^N caminos!!!!!!
- ... es decir, los sistemas de fotones escalean mal!

Sistemas físicos que escalean mejor

- Sistemas de “estado sólido”: qubits superconductores, spins nucleares de impurezas en semiconductores ....
- Atomos atrapados: en redes ópticas, en Pening traps, ó átomos de Rydberg (átomos excitados con electrones con número cuántico principal muy alto)
- Todos estos sistemas tienen en comun que en algun régimen son descriptos adecuadamente por Hamiltonianos de spin

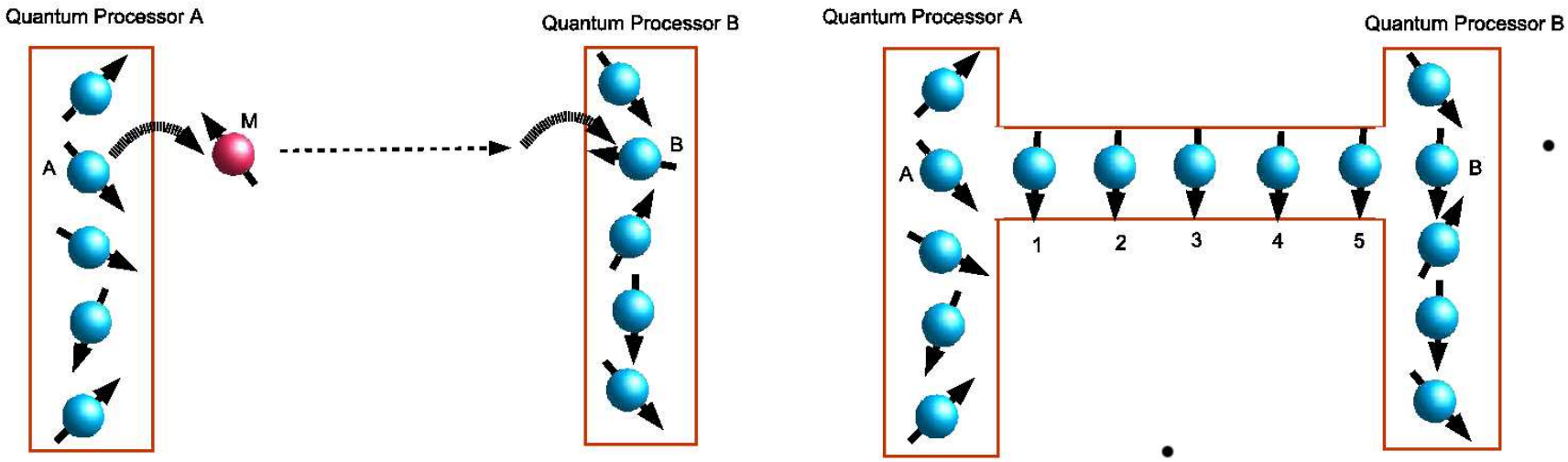
Sistemas físicos que escalean mejor

- Sistemas de “estado sólido”: qubits superconductores, spins nucleares de impurezas en semiconductores ....
- Atomos atrapados: en redes ópticas, en Pening traps, ó átomos de Rydberg (átomos excitados con electrones con número cuántico principal muy alto)
- Todos estos sistemas tienen en comun que en algun régimen son descriptos adecuadamente por Hamiltonianos de spin

Sistemas físicos que escalean mejor

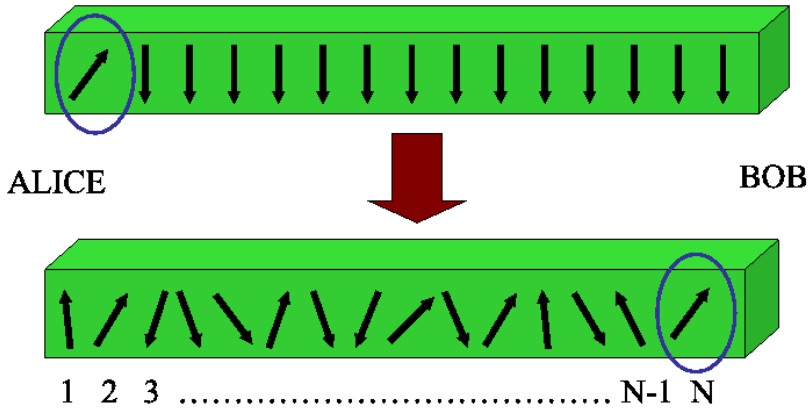
- Sistemas de “estado sólido”: qubits superconductores, spins nucleares de impurezas en semiconductores ....
- Atomos atrapados: en redes ópticas, en Pening traps, ó átomos de Rydberg (átomos excitados con electrones con número cuántico principal muy alto)
- Todos estos sistemas tienen en comun que en algun régimen son descriptos adecuadamente por Hamiltonianos de spin

Conectando procesadores



La forma usual de conectar procesadores cuánticos. La información almacenada en un registro es mapeada a un qubit móvil. Este qubit vuela hacia el otro registro donde la información almacenada en él es mapeada al segundo registro. La figura de la derecha muestra cuando la información es transportada a través de una cadena de qubits estacionaria

El protocolo más simple



El protocolo de comunicación más simple a través de una cadena de spins. Una cadena de spins $1/2$ ferromagnética con todos sus spins down es el canal de comunicación. Alice pone la información en un extremos y, después de cierto tiempo, Bob recoge en el otro extremo información aproximada.

El protocolo más simple 2

VOLUME 91, NUMBER 20 PHYSICAL REVIEW LETTERS week ending 14 NOVEMBER 2003

Quantum Communication through an Unmodulated Spin Chain

Sougato Bose

Institute for Quantum Information, MC 107-81, California Institute of Technology, Pasadena, California 91125-8100, USA and Department of Physics and Astronomy, University College London, Gower Street, London WC1E 6BT, United Kingdom

(Received 15 January 2003; revised manuscript received 24 June 2003; published 10 November 2003)

We propose a scheme for using an unmodulated and unmeasured spin chain as a channel for short distance quantum communications. The state to be transmitted is placed on one spin of the chain and received later on a distant spin with some fidelity. We first obtain simple expressions for the fidelity of quantum state transfer and the amount of entanglement sharable between any two sites of an arbitrary Heisenberg ferromagnet using our scheme. We then apply this to the realizable case of an open ended chain with nearest neighbor interactions. The fidelity of quantum state transfer is obtained as an inverse discrete cosine transform and as a Bessel function series. We find that in a reasonable time, a qubit can be directly transmitted with better than classical fidelity across the full length of chains of up to 80 spins. Moreover, our channel allows distillable entanglement to be shared over arbitrary distances.

DOI: 10.1103/PhysRevLett.91.207901 PACS numbers: 03.67.Hk, 05.50.+q, 32.80.Lg

La fidelidad

Llamemos $|\mathbf{0}\rangle = |0000\ldots0\rangle$, y $|\mathbf{j}\rangle = |000\ldots010\ldots0\rangle$ y preparemos el estado inicial

$$|\Psi(0)\rangle = \cos\frac{\theta}{2}|\mathbf{0}\rangle + e^{i\phi}\sin\frac{\theta}{2}|\mathbf{1}\rangle,$$

si $\left[H, \sum_{i=1}^{N}\sigma_z^i\right] = 0$, entonces

$$|\Psi(t)\rangle = \cos\frac{\theta}{2}|\mathbf{0}\rangle + e^{i\phi}\sin\frac{\theta}{2}\sum_{i=1}^{N}\langle\mathbf{j}|e^{-iHt}|\mathbf{1}\rangle|\mathbf{j}\rangle.$$

Entonces

$$\rho_{out}(t) = \mathrm{Tr}_{1,2,\ldots,N-1}|\Psi(t)\rangle\langle\Psi(t)|,$$

y $F(t) = \langle\Psi(0)|\rho_{out}(t)|\Psi(0)\rangle$.

Fidelidad promedio

Promediando sobre todos los estados de entrada puros en la esfera de Bloch

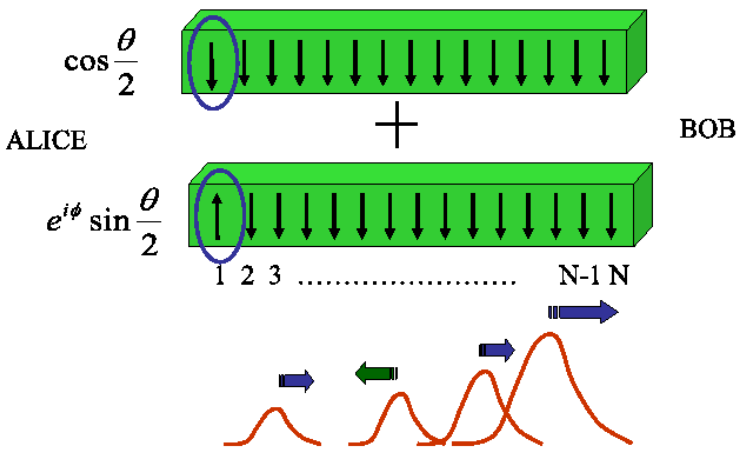
$$\frac{1}{4\pi}\int \langle\Psi(0)|\rho_{out}(t)|\Psi(0)\rangle\, d\Omega = \frac{|f_{N,1}(t)|\cos\gamma}{3} + \frac{|f_{N,1}(t)|^2}{6} + \frac{1}{2},$$

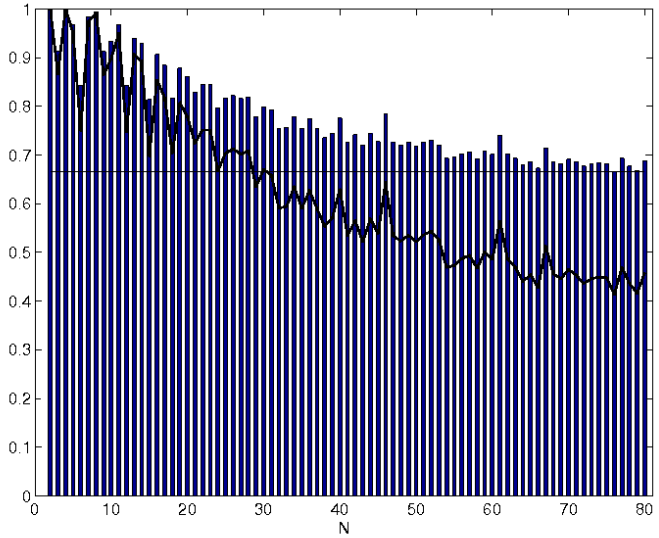
donde $\gamma = \arg\{f_{N,1}(t)\}$, y

$$f_{N,1}(t) = \langle \mathbf{N}|e^{-iHt}|\mathbf{1}\rangle,$$

es la amplitud de transición de una excitación del estado $|\mathbf{1}\rangle$ al estado $|\mathbf{N}\rangle$

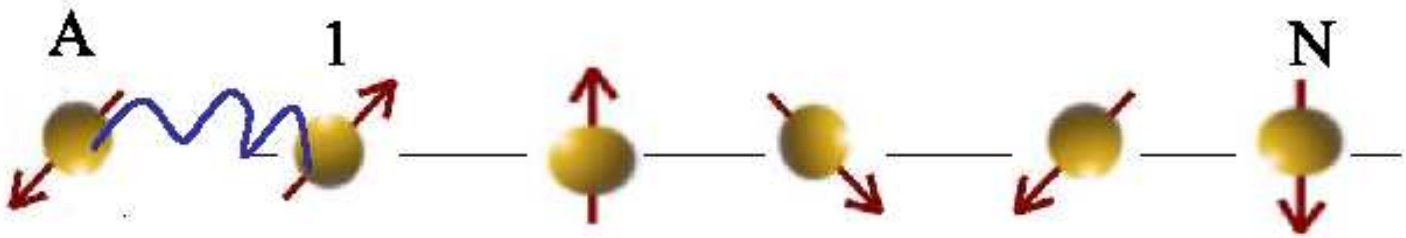
La fidelidad del protocolo más simle





La cadena va a una superposición del estado fundamental y la evolución temporal del estado con un spin up. La evolución temporal transmite un spin flip el cual viaja como una serie de paquetes de onda al mismo tiempo que se dispersa. (barras) máxima fidelidad; (curva) máximo entrelazamiento

El protocolo más simple para entrelazamiento



El mecanismo para transferir entrelazamiento por una cadena. Alice produce un par entrelazado entre un spin (A) que mantiene con ella y el spin en el primer sitio de la cadena. Después de un tiempo el spin de Bob (B) estará entrelazado con el qubit de Alice

Propuestas para mejorar la transmisión

- cadenas con acoples especiales (rotación de un spinotote)
- cadenas con campos externos modulados
- cadenas con arquitecturas más complejas (doble riel)
- distinta codificación del estado inicial
- teoría de control

Propuestas para mejorar la transmisión

- cadenas con acoples especiales (rotación de un spinotote)
- cadenas con campos externos modulados
- cadenas con arquitecturas más complejas (doble riel)
- distinta codificación del estado inicial
- teoría de control

Propuestas para mejorar la transmisión

- cadenas con acoples especiales (rotación de un spinotote)
- cadenas con campos externos modulados
- cadenas con arquitecturas más complejas (doble riel)
- distinta codificación del estado inicial
- teoría de control

Propuestas para mejorar la transmisión

- cadenas con acoples especiales (rotación de un spinotote)
- cadenas con campos externos modulados
- cadenas con arquitecturas más complejas (doble riel)
- distinta codificación del estado inicial
- teoría de control

Propuestas para mejorar la transmisión

- cadenas con acoples especiales (rotación de un spinotote)
- cadenas con campos externos modulados
- cadenas con arquitecturas más complejas (doble riel)
- distinta codificación del estado inicial
- teoría de control

cadenas especiales

PRL 93, 230502 (2004) PHYSICAL REVIEW LETTERS week ending 3 DECEMBER 2004

Mirror Inversion of Quantum States in Linear Registers

Claudio Albanese,[1,2,*] Matthias Christandl,[3,†] Nilanjana Datta,[4,‡] and Artur Ekert[3,5,§]

[1]*Department of Mathematics, Imperial College, London, SW7 2AZ, United Kingdom*
[2]*Department of Mathematics, National University of Singapore, Singapore 117543, Singapore*
[3]*Centre for Quantum Computation, DAMTP, University of Cambridge, Cambridge CB3 0WA, United Kingdom*
[4]*Statistical Laboratory, DPMMS, University of Cambridge, Cambridge CB3 0WB, United Kingdom*
[5]*Department of Physics, National University of Singapore, Singapore 117542, Singapore*

(Received 6 May 2004; published 30 November 2004)

Transfer of data in linear quantum registers can be significantly simplified with preengineered but not dynamically controlled interqubit couplings. We show how to implement a mirror inversion of the state of the register in each excitation subspace with respect to the center of the register. Our construction is especially appealing as it requires no dynamical control over individual interqubit interactions. If, however, individual control of the interactions is available then the mirror inversion operation can be performed on any substring of qubits in the register. In this case, a sequence of mirror inversions can generate any permutation of a quantum state of the involved qubits.

DOI: 10.1103/PhysRevLett.93.230502 PACS numbers: 03.67.Hk, 05.50.+q

control

PHYSICAL REVIEW A, VOLUME 63, 063410

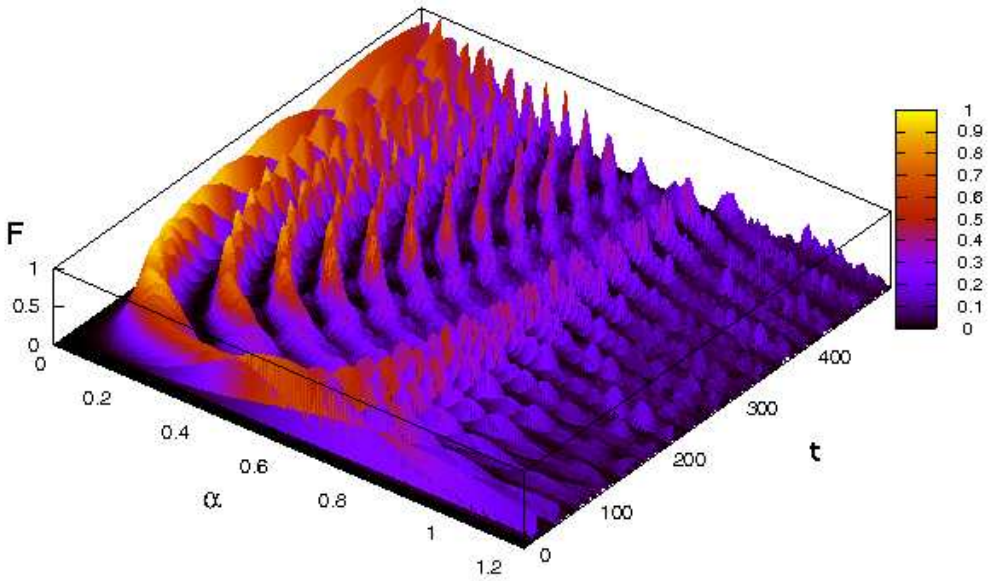
Complete controllability of quantum systems

S. G. Schirmer, H. Fu, and A. I. Solomon
Quantum Processes Group, The Open University, Milton Keynes, MK7 6AA, United Kingdom
(Received 2 September 2000; published 15 May 2001)

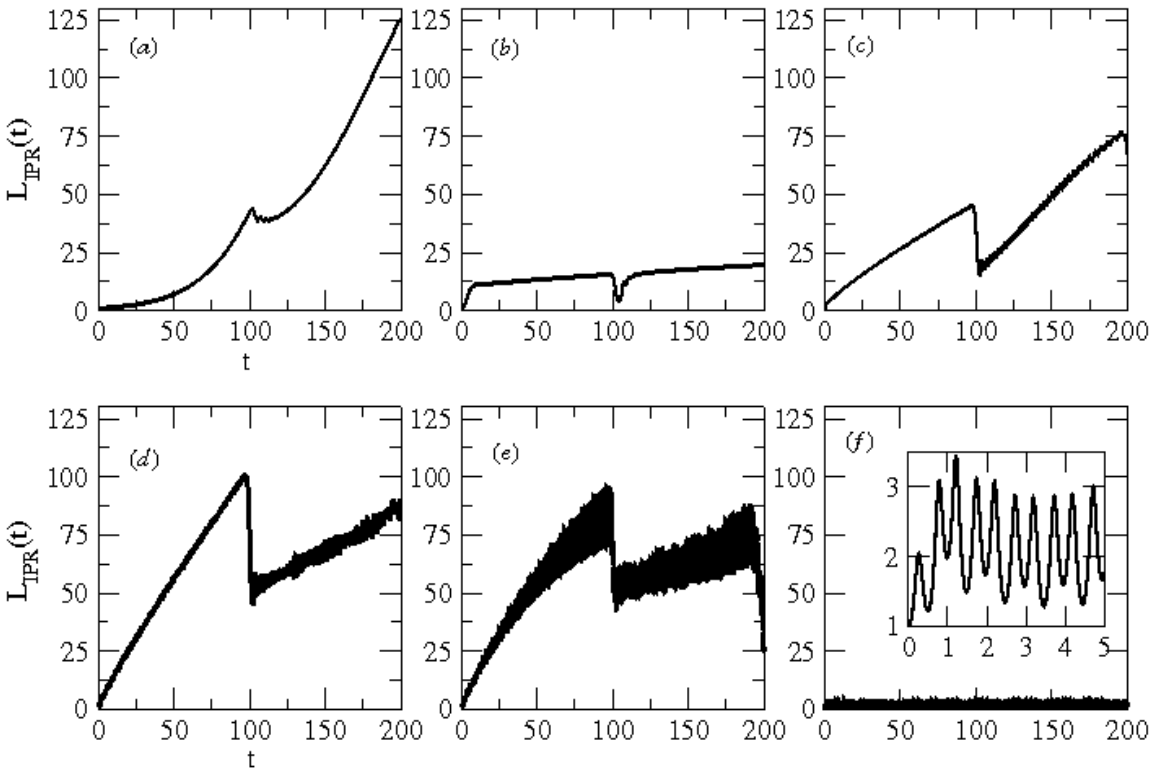
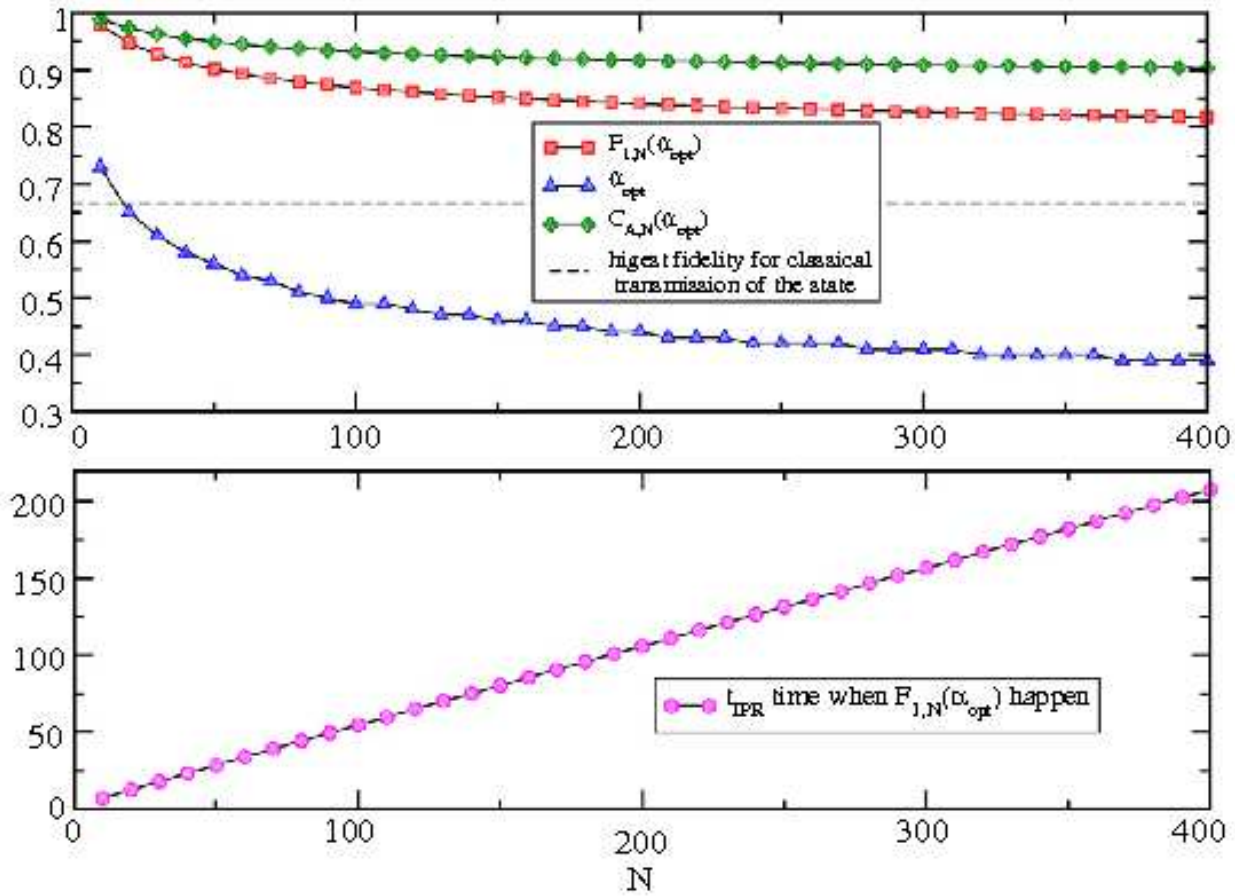
Sufficient conditions for complete controllability of N-level quantum systems subject to a single control pulse that addresses multiple allowed transitions concurrently are established. The results are applied in particular to Morse and harmonic-oscillator systems, as well as some systems with degenerate energy levels. Controllability of these model systems is of special interest since they have many applications in physics, e.g., Morse and harmonic oscillators serve as models for molecular bonds, and the standard control approach of using a sequence of frequency-selective pulses to address a single transition at a time is either not applicable or only of limited utility for such systems.

DOI: 10.1103/PhysRevA.63.063410 PACS number(s): 32.80.Qk, 05.30.−d, 07.05.Dz, 02.20.Sv

Modulando los acoples: landscape



Modulando los acoples: localización



Mejoras obtenidas