



BENEMÉRITA UNIVERSIDAD AUTÓNOMA DE PUEBLA

Facultad de Ciencias
Físico Matemáticas

Criptografía y teleportación cuántica imperfecta

Tesis que para obtener el título de:

Licenciatura en Física

Presenta:

Julián Antonio Díaz Ayón

Director de Tesis:

Dr. Juan Mauricio Torres González

Puebla, Pue.
Diciembre 2019

CRIPTOGRAFÍA Y TELEPORTACIÓN CUÁNTICA IMPERFECTA

Julián Antonio Díaz Ayón
Asesor: Juan Mauricio Torres Gonzalez

8 de diciembre de 2019

Índice general

1. Introducción	2
2. Conceptos básicos	4
2.1. Bits y Qubits	4
2.1.1. Bit Clásico	4
2.1.2. Bit Cuántico	4
2.1.3. Qubits múltiples	5
2.2. Computación cuántica	6
2.2.1. Compuertas cuánticas	6
2.2.2. Circuitos cuánticos	8
2.3. Postulados de la mecánica cuántica	9
2.4. Operador de densidad	9
2.4.1. Operador de densidad reducido	10
3. Comunicación cuántica	12
3.1. Entrelazamiento cuántico	12
3.2. Teleportación cuántica	16
3.3. Teleportación cuántica con ruido	17
4. Criptografía Clásica	28
4.1. Definiciones	28
4.1.1. Terminología básica	28
4.1.2. Privacidad perfecta	29
4.2. One time pad	30
4.3. Distribución de llaves	31
5. Criptografía Cuántica	32
5.1. Protocolo BB84	32
5.2. Protocolo BB84 con ruido	34
5.2.1. Primer modelo: desfasamiento	35
5.2.2. Segundo modelo: Jaynes-Cummings no markoviano	40
6. Conclusiones	46

Capítulo 1

Introducción

Durante el siglo XX se vivió una revolución científica y tecnológica que cambió el mundo de manera incontestable. Esta revolución, la cual estuvo basada en el desarrollo de la mecánica cuántica nos entregó una tecnología crucial, la electrónica de semiconductores [1]. Esta, le dió la posibilidad a un campo científico emergente de esos tiempos, la computación, para desarrollarse a tal nivel, que ahora sería imposible imaginarse la civilización sin las computadoras. Al mismo tiempo, la ciencia y la tecnología han recibido un impulso inmenso gracias al desarrollo de la computación, incluso habiendo conseguido avances teóricos importantes, que sin las computadoras no hubiesen sido posibles [2].

En el siglo XXI, se está dando una nueva revolución científica y tecnológica, también basada en la mecánica cuántica [2]. Esta revolución se diferencia de la primera en que ahora se pretende controlar sistemas cuánticos individuales, utilizando este control para crear tecnologías que nos permitan medir con una precisión hasta ahora imposible, transmitir información totalmente segura, y resolver problemas computacionales que ahora mismo son imposibles utilizando una supercomputadora clásica.

De las tecnologías de esta nueva revolución, la computación cuántica es una de las más interesantes, ya que parece ser el siguiente paso natural de la computación. Durante los 70's Robert Solovay y Volker Strassen mostraron que era posible probar si un entero era primo o no, usando un algoritmo probabilista [3]. Este resultado es importante porque hasta ahora no hay forma de probar si un entero es primo de manera eficiente utilizando un algoritmo determinista. Esto hizo evidente que una computadora probabilista podía resolver un conjunto más grande de problemas que una computadora determinista. Esto, y la clara dificultad de las computadoras clásicas para simular sistemas físicos cuánticos eficientemente, llevaron a David Deutsch en 1985, a proponer un modelo de computación basado ya no en la física clásica, sino en la física cuántica, que debería ser en principio más general que el modelo de Turing o cualquier otro modelo existente basado en la física clásica [4].

Estas ideas llegaron a un punto de máxima atención, cuando en 1994, Peter Shor demostró que era posible resolver el problema de hallar los factores primos

de un entero utilizando un algoritmo cuántico ejecutado en una computadora cuántica teórica [2]. Desde ese momento los desarrollos en computación cuántica no se han detenido, y aunque su despliegue comercial total está todavía a décadas de ser real, las computadoras cuánticas darán un impulso gigantesco a la ciencia y la tecnología, permitiendonos diseñar medicamentos más eficientes, entender mejor la mecánica cuántica al ser capaces de simular sistemas cuánticos eficientemente, resolver problemas computacionales importantes, entre otros [5].

Uno de los obstáculos para llevar a cabo tareas de computación cuántica es el entorno que rodea los sistemas cuánticos. Debido a la imposibilidad de aislar a los sistemas cuánticos de manera perfecta en situaciones reales, es importante el estudio de la mecánica cuántica ante agentes externos que producen ruido en el sistema. En este contexto el área de estudio de sistemas cuánticos abiertos ha desarrollado modelos teóricos que describen de manera más precisa a los sistemas cuánticos ya que toman en cuenta el efecto de su entorno [6].

En esta tesis abordamos el problema de imperfecciones en los protocolos de teleportación y criptografía cuántica y estudiamos como se ve afectado el protocolo original ante estas imperfecciones. Para ello consideramos modelos sencillos de ruido motivados de la teoría de sistemas cuánticos abiertos pero sin hacer énfasis en su derivación microscópica. El enfoque se centra en modelos simples de ruido que ayudan a entender las complicaciones a las que se enfrentan las tecnologías cuánticas para ser implementadas experimentalmente.

Este trabajo está dividido de la siguiente manera: el capítulo 2 introduce los conceptos básicos necesarios para hablar de información cuántica, como los qubits, las compuertas cuánticas y el operador de densidad. El capítulo 3 introduce el entrelazamiento cuántico y como la teleportación cuántica lo utiliza como recurso para transmitir información, y analiza lo que ocurre cuando se intenta transmitir un estado impuro. El capítulo 4 discute los conceptos básicos de la criptografía clásica, el criptosistema One-time-pad, y el problema de la distribución de llaves privadas clásicamente. El capítulo 5 expone una aplicación de la información cuántica a la distribución de llaves criptográficas mediante el protocolo BB84 y finalmente analiza que ocurre con la comunicación cuando el canal cuántico tiene cierto tipo de ruido. El capítulo 6 concluye esta tesis.

Capítulo 2

Conceptos básicos

Este capítulo expone los conceptos necesarios para hablar de información cuántica, primero definiendo lo que es un qubit. Después, trata las compuertas cuánticas, que representan las operaciones que se pueden realizar sobre ellos. Finalmente, muestra el operador de densidad, que sirve para describir a los estados cuánticos de una forma más general y será de gran utilidad más adelante.

2.1. Bits y Qubits

2.1.1. Bit Clásico

Bit es el acrónimo de Binary Digit [7]. Un bit es un dígito en sistema binario. Para el caso que nos interesa (teoría informática), un bit es la mínima unidad de información que podemos procesar y posee dos estados, 0 y 1. El sistema binario es importante porque es la forma en la que las computadoras clásicas representan toda la información que procesan [7]. Una representación física de los dos valores de un bit puede ser dos niveles diferentes de carga de un capacitor [7].

2.1.2. Bit Cuántico

El *bit cuántico*, *cúbit* o *qubit*, es la mínima unidad de información cuántica, al igual que el bit clásico es la mínima unidad de información clásica, con una diferencia muy importante. Mientras que un bit está en todo momento, ya sea en el estado 0 o en el estado 1, un qubit puede estar en una superposición de los estados 0 y 1, ya que el estado de un qubit es cuántico.

Un estado cuántico es un vector de un espacio vectorial complejo, y de acuerdo a Dirac, este vector se llama ket y se denota por $|\alpha\rangle$ [8]. Dos kets se pueden sumar y el resultado es otro ket

$$|\alpha\rangle + |\beta\rangle = |\gamma\rangle. \quad (2.1)$$

Los qubits son kets de dos dimensiones y se pueden expresar como

$$|\psi\rangle = \alpha |0\rangle + \beta |1\rangle. \quad (2.2)$$

Donde $|0\rangle$ corresponde al estado 0 y $|1\rangle$ corresponde al estado 1, los cuales son conocidos como *los estados de la base computacional*. Estos kets se pueden representar como

$$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \text{ y } |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}. \quad (2.3)$$

Otra diferencia importante entre un bit y un qubit es que cuando queremos conocer el estado de un bit, simplemente lo observamos y vemos si está en 0 o en 1. Además, antes y después de medirlo su estado era y sigue siendo ese mismo 0 o 1. Por otro lado, si queremos conocer el estado de un qubit, digamos $|\psi\rangle = \alpha |0\rangle + \beta |1\rangle$, también debemos observarlo. Pero, cuando lo medimos en la base computacional, no obtenemos el resultado $\alpha |0\rangle + \beta |1\rangle$. Lo que obtenemos, es 0 con probabilidad $|\alpha|^2$ o 1 con probabilidad $|\beta|^2$. Por lo tanto, como $|\alpha|^2$ y $|\beta|^2$ son probabilidades, se debe cumplir: $|\alpha|^2 + |\beta|^2 = 1$. Finalmente, a menos que se diga lo contrario, un qubit se mide en la base computacional.

2.1.3. Qubits múltiples

Si tenemos dos bits, podemos tener las combinaciones 00, 01, 10 y 11. De la misma manera, un par de qubits podrían estar en los estados $|0\rangle_A \otimes |0\rangle_B$, $|0\rangle_A \otimes |1\rangle_B$, $|1\rangle_A \otimes |0\rangle_B$ y $|1\rangle_A \otimes |1\rangle_B$, las cuales forman la base computacional del estado de dos qubits, el símbolo $\otimes$ significa producto tensorial y los subíndices A y B marcan el primer y segundo qubit respectivamente. Es posible expresar los qubits múltiples de forma más compacta como $|00\rangle$, $|01\rangle$, $|10\rangle$ y $|11\rangle$. Además, si el estado de un qubit es un vector en dos dimensiones, entonces el estado de dos qubits es un vector en cuatro dimensiones, es decir

$$|\Psi\rangle = \alpha_{00} |00\rangle + \alpha_{01} |01\rangle + \alpha_{10} |10\rangle + \alpha_{11} |11\rangle. \quad (2.4)$$

Al igual que para un qubit, cuando se miden dos qubits, se obtiene 00, 01, 10 o 11, con probabilidad $|\alpha_{00}|^2$, $|\alpha_{01}|^2$, $|\alpha_{10}|^2$ o $|\alpha_{11}|^2$ respectivamente. Donde se debe cumplir que $|\alpha_{00}|^2 + |\alpha_{01}|^2 + |\alpha_{10}|^2 + |\alpha_{11}|^2 = 1$.

En general, el estado de n -qubits es generado por la base:

$$\begin{aligned} |0\rangle \otimes |0\rangle \dots \otimes |0\rangle &= |00\dots 0\rangle \\ |0\rangle \otimes |0\rangle \dots \otimes |1\rangle &= |00\dots 1\rangle \\ &\vdots \\ |1\rangle \otimes |1\rangle \dots \otimes |1\rangle &= |11\dots 1\rangle. \end{aligned} \quad (2.5)$$

Los cuales son 2^n estados que se pueden representar por números binarios. Entonces, el estado total es

$$|\Psi\rangle = \sum_x \alpha_x |x\rangle, \quad (2.6)$$

donde x es una cadena de bits y la suma se realiza sobre todas las cadenas de bits $x \in \{0, 1\}^n$, con n siendo el número de qubits.

2.2. Computación cuántica

2.2.1. Compuertas cuánticas

De manera similar en que la información clásica se procesa usando compuertas clásicas, la información cuántica se procesa usando compuertas cuánticas. Como ejemplo de compuerta clásica, tenemos la compuerta AND, la cual toma dos bits como entrada y entrega un bit de salida. Solo si los dos bits de entrada son iguales 1, la salida es 1, y en cualquier otro caso la salida es 0.

Una compuerta cuántica es un operador unitario actuando sobre uno o más qubits, y podemos representarlo como una matriz actuando sobre un vector. Por ejemplo, si representamos el qubit $|\psi\rangle$ como

$$|\psi\rangle = \alpha |0\rangle + \beta |1\rangle = \begin{pmatrix} \alpha \\ \beta \end{pmatrix}. \quad (2.7)$$

Después, hacemos actuar la matriz de Pauli σ_x , también conocida como compuerta X sobre $|\psi\rangle$, tenemos

$$\sigma_x |\psi\rangle = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} \alpha \\ \beta \end{pmatrix} = \begin{pmatrix} \beta \\ \alpha \end{pmatrix} = \beta |0\rangle + \alpha |1\rangle. \quad (2.8)$$

Es decir, σ_x cambia α por β y viceversa.

Otros ejemplos de compuertas cuánticas incluyendo a X , son:

$$H \equiv \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \quad (2.9)$$

$$X \equiv \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \quad (2.10)$$

$$Y \equiv \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \quad (2.11)$$

$$Z \equiv \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \quad (2.12)$$

$$U_{CN} \equiv \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}. \quad (2.13)$$

La compuerta Hadamard H es importante y la utilizaremos más adelante, así que examinemos como actúa sobre los estados de la base computacional. Para $|0\rangle$, tenemos

$$\begin{aligned} H|0\rangle &= \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} \\ &= \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 1 \end{pmatrix} = \frac{1}{\sqrt{2}} \left[\begin{pmatrix} 1 \\ 0 \end{pmatrix} + \begin{pmatrix} 0 \\ 1 \end{pmatrix} \right] \\ &= \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle). \end{aligned} \quad (2.14)$$

Ahora sobre $|1\rangle$, se tiene

$$\begin{aligned} H|1\rangle &= \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} 0 \\ 1 \end{pmatrix} \\ &= \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ -1 \end{pmatrix} = \frac{1}{\sqrt{2}} \left[\begin{pmatrix} 1 \\ 0 \end{pmatrix} - \begin{pmatrix} 0 \\ 1 \end{pmatrix} \right] \\ &= \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle). \end{aligned} \quad (2.15)$$

También utilizaremos la compuerta CNOT U_{CN} , así que la analizaremos. Esta es una compuerta de dos qubits. El primer qubit es llamado el qubit de control, y el segundo se conoce como qubit objetivo. El estado del qubit de

control no es afectado por la compuerta, y el cambio en el estado del qubit objetivo depende del estado del qubit de control. En particular, si el qubit de control es $|0\rangle$, nada pasa con el qubit objetivo, pero si el bit de control es $|1\rangle$, entonces el qubit objetivo es invertido. Teniendo los casos:

$$|00\rangle \rightarrow |00\rangle$$

$$|01\rangle \rightarrow |01\rangle$$

$$|10\rangle \rightarrow |11\rangle$$

$$|11\rangle \rightarrow |10\rangle$$

2.2.2. Circuitos cuánticos

Un circuito cuántico es una representación gráfica de una serie de procesos que afectan a uno o más qubits. Se leen de izquierda a derecha, los cables (líneas simples) representan el desplazamiento en el espacio o el tiempo de un qubit y los cuadrados representan las compuertas cuánticas. Entonces, un qubit empieza su recorrido del circuito desde el extremo izquierdo y va atravesando cada compuerta que encuentra sufriendo la operación correspondiente. Un ejemplo de circuito cuántico se muestra a continuación

$$|\psi_1\rangle \text{ --- } \boxed{H} \text{ --- } \boxed{Z} \text{ --- } \boxed{Y} \text{ --- } |\psi_2\rangle$$

En el circuito anterior el qubit pasa primero por una compuerta Hadamard, después por una Z y finalmente por una Y. En este caso, si $|\psi_1\rangle = \alpha|0\rangle + \beta|1\rangle$, después de realizar todas las operaciones obtenemos $|\psi_2\rangle = i[(\alpha - \beta)|0\rangle + (\alpha + \beta)|1\rangle]/\sqrt{2}$.

La compuerta U_{CN} , o CNOT, se representa como



donde el qubit de control es el que está en la línea superior y el qubit objetivo en la línea inferior.

Una medición sobre un qubit se representa como



donde la línea doble representa un bit clásico. El concepto de medición se recordará al revisar los postulados de la mecánica cuántica en la siguiente sección.

2.3. Postulados de la mecánica cuántica

Los protocolos revisados en esta tesis utilizarán el concepto de medición en mecánica cuántica. Por lo que es conveniente enunciar los postulados de la mecánica cuántica de la siguiente manera.

1. El estado de una partícula es representado por un vector $|\psi(t)\rangle$ en un espacio de Hilbert.
2. Las observables, tales como la posición, el momento o el spin, son representadas por operadores Hermitianos que actúan sobre los kets.
3. Si una partícula está en el estado $|\psi\rangle$, la medición de una observable Ω , entregará uno de sus eigenvalores ω con probabilidad $P(\omega) = |\langle\omega|\psi\rangle|^2$. El estado del sistema cambiará de $|\psi\rangle$ al eigenestado $|\omega\rangle$ como resultado de la medición. Esto último se conoce como colapso de la función de onda.
4. El ket de estado $|\psi(t)\rangle$ obedece la *ecuación de Schrödinger*

$$i\hbar \frac{d}{dt} |\psi(t)\rangle = H |\psi(t)\rangle, \quad (2.16)$$

donde H es el Hamiltoniano cuántico.

El postulado cuatro no se utiliza en esta tesis, sin embargo se incluye por completés.

2.4. Operador de densidad

El operador de densidad es una forma más general en la que se pueden representar a los qubits, solo que ahora hay que pensar en que se tiene un conjunto o ensamble de qubits en vez de uno solo, los cuales pueden estar, cada uno, en diferentes estados $|\psi_i\rangle$; y donde, si se elige al azar uno de esos qubits, estará en el estado $|\psi_i\rangle$ con probabilidad p_i .

El operador de densidad tiene la forma

$$\rho = \sum_{i=1}^N p_i |\psi_i\rangle \langle\psi_i|, \quad (2.17)$$

donde p_i es la probabilidad de hallar un qubit en el estado $|\psi_i\rangle$.

Por ejemplo, si tenemos un ensamble con la mitad de qubits en el estado $|0\rangle$ y la otra mitad en el estado $|1\rangle$, el operador de densidad es

$$\rho = \frac{1}{2} |0\rangle \langle 0| + \frac{1}{2} |1\rangle \langle 1|. \quad (2.18)$$

Si tenemos un ensamble de qubits múltiples, digamos, un tercio de qubits en el estado $|01\rangle$, un tercio de $|10\rangle$, y un tercio de $|11\rangle$, el operador de densidad es

$$\rho = \frac{1}{3} |01\rangle \langle 01| + \frac{1}{3} |10\rangle \langle 10| + \frac{1}{3} |11\rangle \langle 11|. \quad (2.19)$$

El operador de densidad también puede ser representado por una matriz en la base computacional, donde cada entrada $\rho_{ij} = \langle i|\rho|j\rangle$. Para el segundo ejemplo esto es

$$\begin{aligned} \rho &= \begin{pmatrix} \langle 00|\rho|00\rangle & \langle 00|\rho|01\rangle & \langle 00|\rho|10\rangle & \langle 00|\rho|11\rangle \\ \langle 01|\rho|00\rangle & \langle 01|\rho|01\rangle & \langle 01|\rho|10\rangle & \langle 01|\rho|11\rangle \\ \langle 10|\rho|00\rangle & \langle 10|\rho|01\rangle & \langle 10|\rho|10\rangle & \langle 10|\rho|11\rangle \\ \langle 11|\rho|00\rangle & \langle 11|\rho|01\rangle & \langle 11|\rho|10\rangle & \langle 11|\rho|11\rangle \end{pmatrix} \\ &= \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & \frac{1}{3} & 0 & 0 \\ 0 & 0 & \frac{1}{3} & 0 \\ 0 & 0 & 0 & \frac{1}{3} \end{pmatrix} \end{aligned} \quad (2.20)$$

Un estado es puro cuando existe una base donde todas las $p_i = 0$ excepto una, esto es $\rho = |\psi_j\rangle\langle\psi_j|$, con $p_j = 1$. Es decir, si existe un eigenvalor igual a uno y por consiguiente todos los demás iguales a cero, se tiene un estado puro, de otra manera se tiene estado mezclado.

Como la traza de una matriz es la suma de los elementos de su diagonal. La traza de un operador de densidad es

$$\text{tr}(\rho) = \sum_i \langle i|\rho|i\rangle \quad (2.21)$$

Además, la traza de un operador de densidad es igual a uno. Ya que

$$\text{tr}(\rho) = \sum_{i=i}^N p_i \text{tr}(|\psi_i\rangle\langle\psi_i|) = \sum_i p_i = 1. \quad (2.22)$$

Finalmente, si ρ es un operador de densidad, existe la manera de cuantificar que tan fielmente se parece a un estado puro con la cantidad conocida como pureza calculando la traza del operador de densidad al cuadrado. Esto es

$$\text{tr}(\rho^2) \leq 1, \quad (2.23)$$

con la igualdad si y solo si ρ es un estado puro.

2.4.1. Operador de densidad reducido

Cuando se tiene un sistema compuesto por dos subsistemas A y B , cuyo estado es descrito por el operador ρ^{AB} , donde los superíndices A y B se refieren a cada sistema individual. El operador de densidad reducido del sistema A se define como

$$\rho^A \equiv \text{tr}_B(\rho^{AB}) = \sum_i \langle i|^B \rho^{AB} |i\rangle^B, \quad (2.24)$$

donde tr_B es la traza parcial sobre el sistema B . Esto es

$$\text{tr}(\rho^B) = \sum_i \langle i|^B \rho^B |i\rangle^B. \quad (2.25)$$

Para el ejemplo de la sección anterior, se tiene

$$\begin{aligned} \rho^{AB} &= \frac{1}{3} |01\rangle \langle 01| + \frac{1}{3} |10\rangle \langle 10| + \frac{1}{3} |11\rangle \langle 11| \\ &= \frac{1}{3} |0\rangle \langle 0|^A |1\rangle \langle 1|^B + \frac{1}{3} |1\rangle \langle 1|^A |0\rangle \langle 0|^B + \frac{1}{3} |1\rangle \langle 1|^A |1\rangle \langle 1|^B. \end{aligned} \quad (2.26)$$

Por lo que el operador de densidad de A es

$$\begin{aligned} \rho^A &= \text{tr}_B(\rho^{AB}) = \frac{1}{3} |0\rangle \langle 0|^A + \frac{1}{3} |1\rangle \langle 1|^A + \frac{1}{3} |1\rangle \langle 1|^A \\ &= \frac{1}{3} |0\rangle \langle 0|^A + \frac{2}{3} |1\rangle \langle 1|^A. \end{aligned} \quad (2.27)$$

La traza parcial cobra importancia en el contexto de sistemas cuánticos abiertos, ya que tomando traza parcial sobre los grados de libertad del entorno, se obtiene la matriz de densidad del sistema de interés.

Capítulo 3

Comunicación cuántica

Este capítulo trata de dos aplicaciones de la información cuántica. Primero, el entrelazamiento cuántico, el cual es una propiedad de los sistemas cuánticos. Después, la teleportación cuántica, la cual es una técnica para transmitir estados cuánticos utilizando el entrelazamiento como un recurso. Finalmente, se muestra que ocurre con la teleportación cuando no se tiene un estado inicial ideal.

3.1. Entrelazamiento cuántico

El entrelazamiento cuántico es un fenómeno físico que ocurre cuando dos o más partículas interactúan entre sí, de tal manera que el estado cuántico de una partícula no puede ser descrito independientemente de los estados de las otras. Aquí solo se tratará el caso del entrelazamiento de dos qubits. Un estado cuántico puro que está en un espacio producto de Hilbert $\mathcal{H} = \mathcal{H}_A \otimes \mathcal{H}_B$ no está entrelazado si es un estado producto de la forma

$$|\Psi\rangle_{AB} = |\phi_1\rangle_A \otimes |\phi_2\rangle_B,$$

de otra manera, está entrelazado. Por ejemplo, $|0\rangle_A |0\rangle_B$ no está entrelazado, mientras que los estados de Bell

$$\begin{aligned} |\Psi^\pm\rangle &= \frac{1}{\sqrt{2}}(|01\rangle_{AB} \pm |10\rangle_{AB}) \\ |\Phi^\pm\rangle &= \frac{1}{\sqrt{2}}(|00\rangle_{AB} \pm |11\rangle_{AB}) \end{aligned}$$

sí lo están.

Una manera de medir el entrelazamiento entre dos qubits es utilizando la entropía de Von Neumann, que se escribe como

$$S \equiv -\text{tr}(\rho \log_2 \rho). \quad (3.1)$$

donde ρ es un operador de densidad reducido de alguno de los dos qubits.

Si el operador de densidad está escrito en terminos de sus eigenvectores, S toma la forma

$$\rho = \sum_j \eta_j |j\rangle \langle j|, \quad (3.2)$$

entonces, la entropía de Von Neumann se puede escribir como

$$S = - \sum_j \eta_j \log_2 \eta_j. \quad (3.3)$$

con $0 \log(0) \equiv 0$, y donde el entrelazamiento es máximo si $S = 1$ y no hay entrelazamiento si $S = 0$.

Por ejemplo, para $|0\rangle_A |0\rangle_B$, tenemos

$$\begin{aligned} \rho^{AB} &= |0\rangle_A |0\rangle_B \langle 0|_A \langle 0|_B \\ &= |0\rangle \langle 0|_A |0\rangle \langle 0|_B. \end{aligned} \quad (3.4)$$

Por lo que

$$\rho^A = |0\rangle \langle 0|_A, \quad (3.5)$$

que está en términos de sus eigenvalores, por lo tanto

$$S = -1 \log_2 1 - 0 \log_2 0 = 0. \quad (3.6)$$

Es decir, $|0\rangle_A |0\rangle_B$ no está entrelazado.

Por otro lado, si tenemos

$$|\Psi^+\rangle = \frac{1}{\sqrt{2}}(|01\rangle_{AB} + |10\rangle_{AB}), \quad (3.7)$$

entonces

$$\rho^{AB} = |\Psi^+\rangle \langle \Psi^+|, \quad (3.8)$$

por lo tanto, el operador de densidad reducido es

$$\rho^A = \frac{1}{2}(|0\rangle \langle 0| + |1\rangle \langle 1|), \quad (3.9)$$

que está en términos de sus eigenvectores, por lo tanto

$$S = \frac{1}{2} \log_2 2 + \frac{1}{2} \log_2 2 = 1. \quad (3.10)$$

Por lo tanto $|\Psi^+\rangle$ está máximamente entrelazado.

Por otro lado podríamos tener un estado como

$$|\psi\rangle = \sqrt{1 - \alpha^2} |00\rangle + \alpha |11\rangle. \quad (3.11)$$

Cuyo operador de densidad reducido del primer qubit es

$$\rho^A = (1 - \alpha^2) |0\rangle\langle 0| + \alpha^2 |1\rangle\langle 1|. \quad (3.12)$$

Por lo tanto, su entropía es

$$S = -(1 - \alpha^2)\log_2(1 - \alpha^2) - \alpha^2\log_2(\alpha^2). \quad (3.13)$$

Es decir, el entrelazamiento de $|\psi\rangle$ depende de α , que va desde el estado separable para $S = 0$, hasta el entrelazamiento máximo $S = 1$. La forma de S se muestra en la figura 3.1.

En la siguiente sección veremos como se puede utilizar el entrelazamiento cuántico como recurso para el protocolo de teleportación cuántica.

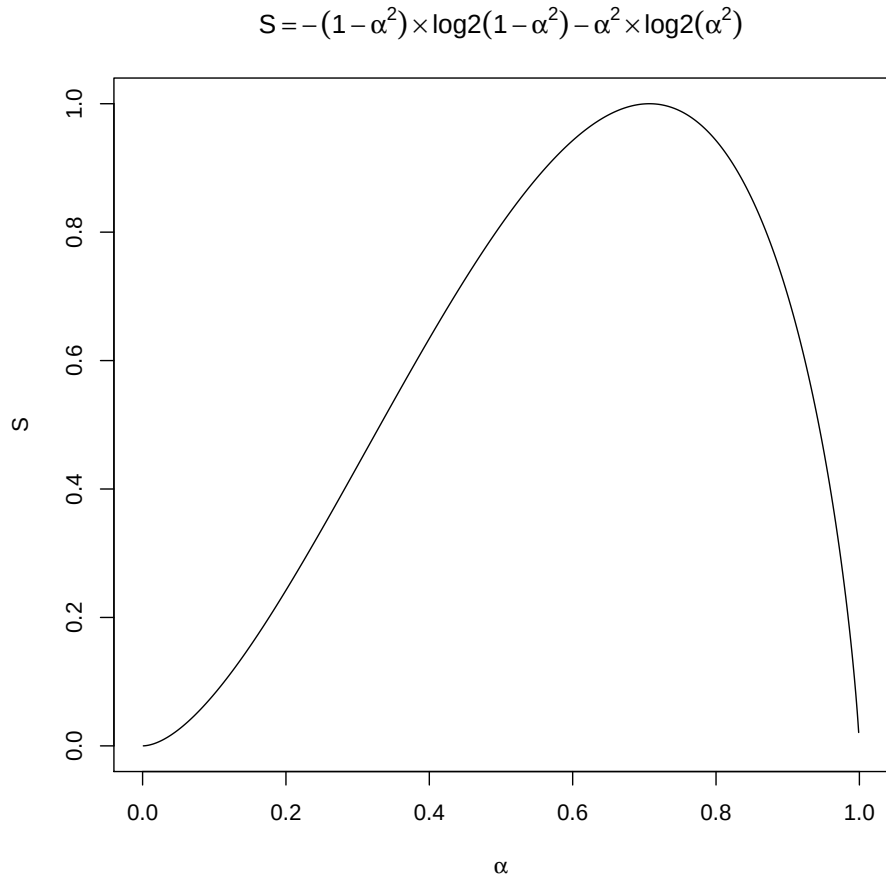


Figura 3.1: La entropía de Von Neumann S , de $|\psi\rangle = \sqrt{1 - \alpha^2} |00\rangle + \alpha |11\rangle$ como función de α .

3.2. Teleportación cuántica

La teleportación cuántica es una técnica para trasportar estados cuánticos cuando tenemos disponible un canal de comunicación clásico y el entrelazamiento cuántico como un recurso adicional [2]. Tiempo atrás Alice y Bob generaron un par de qubits entrelazados. El día de hoy mucho tiempo después de su encuentro, Alice posee un qubit y quiere enviar su estado $|\psi\rangle$ a Bob, pero solo puede enviarle información clásica. Afortunadamente, pueden utilizar el par entrelazado para lograr esta tarea.

El estado a ser teleportado es $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$, donde α y β son desconocidos. El estado inicial total es

$$\begin{aligned} |\psi_0\rangle &= |\psi\rangle |\Phi^+\rangle \\ &= \frac{1}{\sqrt{2}}[\alpha|0\rangle(|00\rangle + |11\rangle) + \beta|1\rangle(|00\rangle + |11\rangle)], \end{aligned} \quad (3.14)$$

donde los dos primeros qubits de la izquierda pertenecen a Alice, y el tercero a Bob. Alice manda sus qubits por una compuerta CNOT, obteniendo

$$|\psi_1\rangle = \frac{1}{\sqrt{2}}[\alpha|0\rangle(|00\rangle + |11\rangle) + \beta|1\rangle(|10\rangle + |01\rangle)]. \quad (3.15)$$

Después manda el primer qubit por una compuerta Hadamard, obteniendo

$$|\psi_2\rangle = \frac{1}{2}[\alpha(|0\rangle + |1\rangle)(|00\rangle + |11\rangle) + \beta(|0\rangle - |1\rangle)(|10\rangle + |01\rangle)]. \quad (3.16)$$

Este estado se puede reescribir como

$$\begin{aligned} |\psi_2\rangle &= \frac{1}{2} \left[|00\rangle (\alpha|0\rangle + \beta|1\rangle) + |01\rangle (\alpha|1\rangle + \beta|0\rangle) \right. \\ &\quad \left. + |10\rangle (\alpha|0\rangle - \beta|1\rangle) + |11\rangle (\alpha|1\rangle - \beta|0\rangle) \right]. \end{aligned} \quad (3.17)$$

Esta expresión tiene cuatro términos. El primero tiene a los qubits de Alice en el estado $|00\rangle$, y el qubit de Bob en el estado $\alpha|0\rangle + \beta|1\rangle$. Si Alice hace una medición en la base computacional y obtiene 00 entonces el sistema de Bob será $|\psi\rangle$. Similarmente, de la expresión anterior podemos saber que estado tiene Bob dependiendo del resultado de la medición de Alice:

$$00 \rightarrow |\psi_3(00)\rangle \equiv [\alpha|0\rangle + \beta|1\rangle]$$

$$01 \rightarrow |\psi_3(01)\rangle \equiv [\alpha|1\rangle + \beta|0\rangle]$$

$$10 \rightarrow |\psi_3(10)\rangle \equiv [\alpha|0\rangle - \beta|1\rangle]$$

$$11 \rightarrow |\psi_3(11)\rangle \equiv [\alpha |1\rangle - \beta |0\rangle].$$

Dependiendo del resultado de Alice, el qubit de Bob estará en uno de estos cuatro estados. Por supuesto, para saber cual es, Bob tiene que ser informado del resultado de la medición. Una vez que Bob conoce el resultado, simplemente tiene que usar la compuerta cuántica correcta para recuperar el estado original. Por ejemplo, si el resultado de la medición fué 00, Bob no tiene que hacer nada. Si el resultado es 01 Bob puede usar la compuerta X . Si el resultado es 10 Bob puede usar la compuerta Z . Y, si el resultado es 11 entonces Bob puede usar X y luego Z . Recuperando el estado $|\psi\rangle$.

Es posible reescribir el protocolo de teleportación usando el operador de densidad, lo cual será útil para la siguiente sección donde se tratan sistemas con ruido. El estado inicial es

$$\begin{aligned} |\psi_0\rangle &= |\psi\rangle_A |\Phi^+\rangle_{BC} \\ \Rightarrow \rho_0 &= |\psi\rangle\langle\psi|_A |\Phi^+\rangle\langle\Phi^+|_{BC}, \end{aligned} \quad (3.18)$$

donde los subíndices A,B y C se refieren al primero, segundo y tercer qubit respectivamente. El estado después de CNOT y Hadamard es:

$$\begin{aligned} |\psi_2\rangle &= \frac{1}{2} \sum_{ij} |ij\rangle_{AB} |\psi_{ij}\rangle_C \\ \Rightarrow \rho_2 &= \frac{1}{4} \sum_{ij} |ij\rangle_{AB} |\psi_{ij}\rangle_C \sum_{kl} \langle kl|_{AB} \langle\psi_{kl}|_C \\ &= \frac{1}{4} \sum_{ijkl} |ij\rangle\langle kl|_{AB} |\psi_{ij}\rangle\langle\psi_{kl}|_C, \end{aligned} \quad (3.19)$$

donde $i, j, k, l = 0, 1$, y

$$\begin{aligned} |\psi_{00}\rangle &= \alpha |0\rangle + \beta |1\rangle \\ |\psi_{01}\rangle &= \alpha |1\rangle + \beta |0\rangle \\ |\psi_{10}\rangle &= \alpha |0\rangle - \beta |1\rangle \\ |\psi_{11}\rangle &= \alpha |1\rangle - \beta |0\rangle \end{aligned}$$

3.3. Teleportación cuántica con ruido

Primer modelo de ruido

En el caso ideal tenemos $\rho = |\psi\rangle\langle\psi|_A |\Phi^+\rangle\langle\Phi^+|_{BC}$ como estado inicial, y podemos transmitir $|\psi\rangle$ exitosamente. Sin embargo, en un escenario donde nuestros qubits están interactuando con su entorno debido a la imposibilidad de

aislarlos perfectamente, esto podría resultar en un estado inicial imperfecto de la forma

$$\begin{aligned}\rho_0 &= F\rho_0^{(1)} + (1-F)\rho_0^{(2)} \\ &= F|\psi\rangle\langle\psi|_A|\Phi^+\rangle\langle\Phi^+|_{BC} + (1-F)|\psi\rangle\langle\psi|_A|00\rangle\langle 00|_{BC}\end{aligned}\quad (3.20)$$

donde F es la fidelidad del estado inicial, esto es, su cercanía al estado ideal.

Ahora, teniendo un estado de la forma anterior, el estado transmitido ya no será $|\psi\rangle$ exactamente. Para analizar que ocurre en este caso, primero se debe notar que el estado $\rho_0^{(1)}$ es igual al estado inicial del protocolo sin ruido, y aprovechando la linealidad de los componentes de ρ , se puede analizar $\rho^{(1)}$ y $\rho^{(2)}$ por separado. Por lo tanto, usando el último resultado de la sección anterior, el estado final de $\rho_0^{(1)}$ es

$$\rho_2^{(1)} = \frac{1}{4} \sum_{ijkl} |ij\rangle\langle kl|_{AB} |\psi_{ij}\rangle\langle\psi_{kl}|_C. \quad (3.21)$$

Para encontrar $\rho_2^{(2)}$, veamos primero lo que le ocurre al estado $|\psi\rangle|00\rangle$ al atravesar el protocolo, entonces el estado inicial es

$$\begin{aligned}|\psi_0^{(2)}\rangle &= |\psi\rangle|00\rangle \\ &= (\alpha|0\rangle + \beta|1\rangle)|00\rangle \\ &= \alpha|000\rangle + \beta|100\rangle.\end{aligned}\quad (3.22)$$

Al mandar los primeros dos qubits por la compuerta CNOT, tenemos

$$|\psi_1^{(2)}\rangle = \alpha|000\rangle + \beta|110\rangle. \quad (3.23)$$

Después mandamos el primer qubit por la compuerta Hadamard, obteniendo

$$\begin{aligned}|\psi_2^{(2)}\rangle &= \frac{1}{\sqrt{2}} \left[\alpha(|0\rangle + |1\rangle)|00\rangle + \beta(|0\rangle - |1\rangle)|10\rangle \right] \\ &= \frac{1}{\sqrt{2}} \left[\alpha|000\rangle + \alpha|100\rangle + \beta|010\rangle - \beta|110\rangle \right] \\ &= \frac{1}{\sqrt{2}} \sum_{ij} c_{ij} |ij\rangle_{AB} |0\rangle_C,\end{aligned}\quad (3.24)$$

con $i, j = 0, 1$ y

$$c_{00} = c_{10} = \alpha \quad (3.25)$$

$$c_{01} = \beta \quad (3.26)$$

$$c_{11} = -\beta. \quad (3.27)$$

Entonces, el operador de densidad de la parte que representa el ruido es

$$\begin{aligned}\rho_2^{(2)} &= \frac{1}{2} \sum_{ij} c_{ij} |ij\rangle_{AB} |0\rangle_C \sum_{kl} c_{kl}^* \langle kl|_{AB} |0\rangle_C \\ &= \frac{1}{2} \sum_{ijkl} c_{ij} c_{kl}^* |ij\rangle \langle kl|_{AB} |0\rangle \langle 0|_C.\end{aligned}\quad (3.28)$$

Por lo tanto, el operador de densidad total después de las compuertas CNOT y Hadamard, es

$$\rho_2 = \frac{F}{4} \sum_{ijkl} |ij\rangle \langle kl|_{AB} |\psi_{ij}\rangle \langle \psi_{kl}|_C + \frac{1-F}{2} \sum_{ijkl} c_{ij} c_{kl}^* |ij\rangle \langle kl|_{AB} |0\rangle \langle 0|_C. \quad (3.29)$$

Ahora, al proyectar ρ_2 sobre el estado $|nm\rangle_{AB}$, obtenemos la matriz de densidad no normalizada del qubit de Bob, después de que Alice ha medido sus dos qubits. Esto es

$$\begin{aligned}\hat{\rho}_C &= \frac{F}{4} \langle nm|_{AB} \left[\sum_{ijkl} |ij\rangle \langle kl|_{AB} |\psi_{ij}\rangle \langle \psi_{kl}|_C \right. \\ &\quad \left. + \frac{1-F}{2} \sum_{ijkl} c_{ij} c_{kl}^* |ij\rangle \langle kl|_{AB} |0\rangle \langle 0|_C \right] |nm\rangle_{AB}.\end{aligned}\quad (3.30)$$

Que resulta en

$$\hat{\rho}_C = \frac{F}{4} |\psi_{ij}\rangle \langle \psi_{ij}|_C + \frac{(1-F)|c_{ij}|^2}{2} |0\rangle \langle 0|_C. \quad (3.31)$$

Ahora. Calculando la traza de $\hat{\rho}_C$, tenemos

$$\begin{aligned}\text{tr}\{\hat{\rho}_C\} &= \sum_k \langle k| \left[\frac{F}{4} |\psi_{ij}\rangle \langle \psi_{ij}| + \frac{(1-F)|c_{ij}|^2}{2} |0\rangle \langle 0| \right] |k\rangle \\ &= \frac{F}{4} (|\alpha|^2 + |\beta|^2) + \frac{(1-F)|c_{ij}|^2}{2} \\ &= \frac{F}{4} + \frac{(1-F)|c_{ij}|^2}{2}.\end{aligned}\quad (3.32)$$

Por lo tanto, el operador de densidad normalizado del qubit de Bob, es

$$\rho_C = \left[\frac{F}{4} |\psi_{ij}\rangle \langle \psi_{ij}| + \frac{(1-F)|c_{ij}|^2}{2} |0\rangle \langle 0| \right] \left[\frac{F}{4} + \frac{(1-F)|c_{ij}|^2}{2} \right]^{-1}. \quad (3.33)$$

Al igual que en el caso ideal, Bob debe realizar la transformación correspondiente de acuerdo al resultado de la medición de Alice. Sin embargo, aún cuando Bob use la transformación correcta, no siempre tendrá el estado $|\psi\rangle$ que Alice quería transmitir debido a que el estado inicial que ella envió no era ideal. Finalmente, la fidelidad F_{ij} del estado $|\psi_{ij}\rangle$ al ser transmitido, es

$$\begin{aligned} F_{ij} &= \langle \psi_{ij} | \rho_{(C)} | \psi_{ij} \rangle \\ &= \left[\frac{F}{4} + \frac{(1-F)|c_{ij}|^4}{2} \right] \left[\frac{F}{4} + \frac{(1-F)|c_{ij}|^2}{2} \right]^{-1}. \end{aligned} \quad (3.34)$$

La fidelidad del estado teleportado depende del estado inicial y del resultado de la medición de Alice debido a la presencia de $|c_{ij}|$. Por lo tanto, en general, estos estados no son deseables para ser teleportados. Se muestra F_{ij} en la figura 3.2.

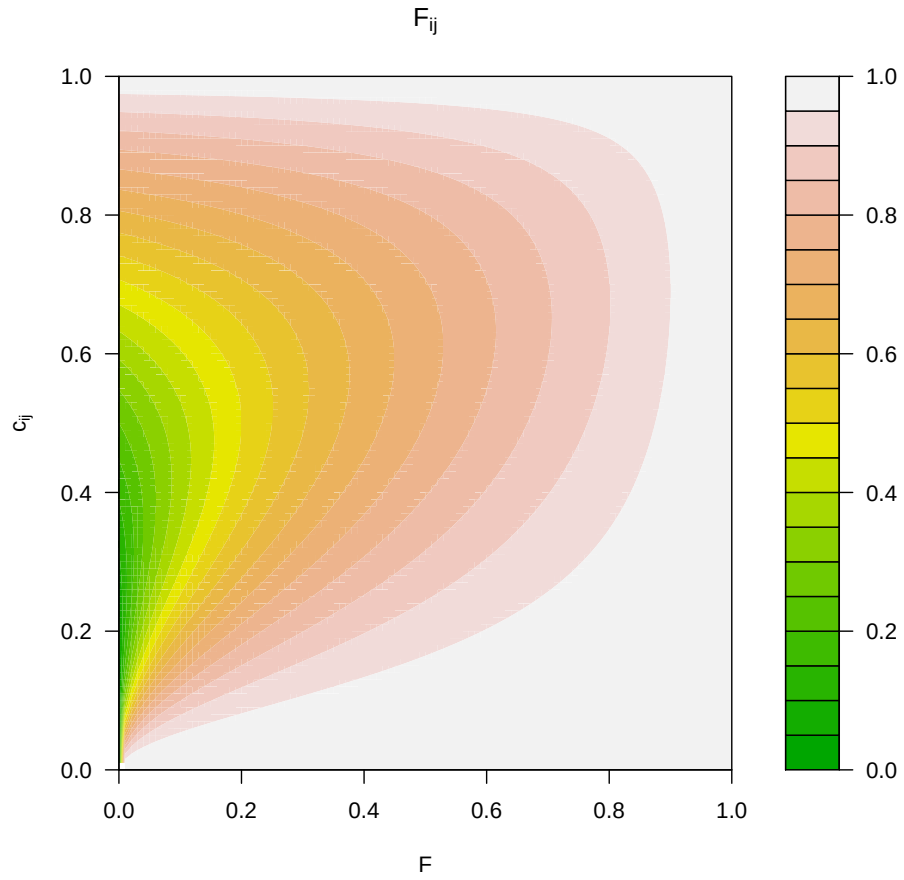


Figura 3.2: La fidelidad de F_{ij} como función de c_{ij} y F . El color verde representa el valor mínimo 0 y el rosa el valor máximo 1. F_{ij} es máxima cuando $F = 1$ y para cualquier valor de c_{ij} . Cuando $F < 1$, F_{ij} empeora especialmente para valores de $c_{ij} \simeq 0,4$ y para valores de F cercanos a 0.

Segundo modelo de ruido

El estado inicial que consideraremos en este caso es

$$\rho_0 = |\psi\rangle\langle\psi| \rho_w, \quad (3.35)$$

donde ρ_w es

$$\rho_w = F |\Phi^+\rangle\langle\Phi^+| + \frac{1-F}{3} \left[|\Phi^-\rangle\langle\Phi^-| + |\Psi^+\rangle\langle\Psi^+| + |\Psi^-\rangle\langle\Psi^-| \right], \quad (3.36)$$

el cual es conocido como estado de Werner. Este tipo de estados se utilizaron en el primer protocolo de purificación de entrelazamiento [9].

Antes de analizar que ocurre con este estado al ser teleportado, recordemos a los estados de Bell

$$|\Psi^\pm\rangle = \frac{1}{\sqrt{2}}(|01\rangle_{AB} \pm |10\rangle_{AB})$$

$$|\Phi^\pm\rangle = \frac{1}{\sqrt{2}}(|00\rangle_{AB} \pm |11\rangle_{AB}),$$

y consideremos las siguientes transformaciones entre estados de Bell y operadores de Pauli, las cuales serán de gran utilidad en los cálculos posteriores.

$$\sigma_x^A |\Phi^+\rangle_{AB} = \sigma_x^B |\Phi^+\rangle_{AB} = |\Psi^+\rangle, \quad (3.37)$$

$$-\sigma_z^A \sigma_x^A |\Phi^+\rangle_{AB} = \sigma_z^B \sigma_x^B |\Phi^+\rangle_{AB} = |\Psi^-\rangle, \quad (3.38)$$

$$\sigma_z^A |\Phi^+\rangle_{AB} = \sigma_z^B |\Phi^+\rangle_{AB} = |\Phi^-\rangle, \quad (3.39)$$

$$-\sigma_x^A |\Phi^-\rangle_{AB} = \sigma_x^B |\Phi^-\rangle_{AB} = |\Psi^-\rangle, \quad (3.40)$$

$$\sigma_z^A \sigma_x^A |\Phi^-\rangle_{AB} = \sigma_z^B \sigma_x^B |\Phi^-\rangle_{AB} = |\Psi^+\rangle, \quad (3.41)$$

$$\sigma_z^A |\Phi^-\rangle_{AB} = \sigma_z^B |\Phi^-\rangle_{AB} = |\Phi^+\rangle, \quad (3.42)$$

$$\sigma_x^A |\Psi^+\rangle_{AB} = \sigma_x^B |\Psi^+\rangle_{AB} = |\Phi^+\rangle, \quad (3.43)$$

$$-\sigma_z^A \sigma_x^A |\Psi^+\rangle_{AB} = \sigma_z^B \sigma_x^B |\Psi^+\rangle_{AB} = |\Phi^-\rangle, \quad (3.44)$$

$$\sigma_z^A |\Psi^+\rangle_{AB} = \sigma_z^B |\Psi^+\rangle_{AB} = |\Psi^-\rangle, \quad (3.45)$$

$$-\sigma_x^A |\Psi^-\rangle_{AB} = \sigma_x^B |\Psi^-\rangle_{AB} = |\Phi^-\rangle, \quad (3.46)$$

$$\sigma_z^A \sigma_x^A |\Psi^-\rangle_{AB} = \sigma_z^B \sigma_x^B |\Psi^-\rangle_{AB} = |\Phi^+\rangle, \quad (3.47)$$

$$\sigma_z^A |\Psi^-\rangle_{AB} = \sigma_z^B |\Psi^-\rangle_{AB} = |\Psi^+\rangle. \quad (3.48)$$

Adicionalmente, reescribiré el circuito de teleportación notando que las compuertas CNOT y Hadamard y las mediciones en la base computacional representan una

medición de Bell sobre los qubits de Alice. Una medición de Bell mide los cuatro estados de Bell de manera análoga a la medición de la base computacional. De esta manera se puede ver que el protocolo de teleportación esta basado en una sola medición de Bell.

Aprovechando la linealidad de los operadores que actúan sobre los kets, podemos analizar cada parte de ρ_0 por separado. Para $|\psi\rangle |\Phi^+\rangle$ el cual es igual al estado ideal que ya habíamos analizado, tenemos

$$|\psi\rangle |\Phi^+\rangle = \frac{\alpha |00\rangle + \alpha |01\rangle + \beta |10\rangle + \beta |11\rangle}{\sqrt{2}}. \quad (3.49)$$

Podemos reescribir este estado empleando los estados de Bell notando que

$$\begin{aligned} |00\rangle &= |\Phi^+\rangle + |\Phi^-\rangle \\ |01\rangle &= |\Psi^+\rangle + |\Psi^-\rangle \\ |10\rangle &= |\Psi^+\rangle - |\Psi^-\rangle \\ |11\rangle &= |\Phi^+\rangle - |\Phi^-\rangle. \end{aligned} \quad (3.50)$$

Esto es

$$|\psi\rangle |\Phi^+\rangle = \frac{1}{2} \left[\alpha (|\Phi^+\rangle + |\Phi^-\rangle) |0\rangle + \alpha (|\Psi^+\rangle + |\Psi^-\rangle) |1\rangle \right. \quad (3.51)$$

$$\left. + \beta (|\Psi^+\rangle - |\Psi^-\rangle) |0\rangle + \beta (|\Phi^+\rangle - |\Phi^-\rangle) |1\rangle \right]. \quad (3.52)$$

Factorizando los estados de Bell, obtenemos

$$|\psi\rangle |\Phi^+\rangle = \frac{1}{2} \left[|\Phi^+\rangle (\alpha |0\rangle + \beta |1\rangle) + |\Phi^-\rangle (\alpha |0\rangle - \beta |1\rangle) \right. \quad (3.53)$$

$$\left. + |\Psi^+\rangle (\alpha |1\rangle + \beta |0\rangle) + |\Psi^-\rangle (\alpha |1\rangle - \beta |0\rangle) \right]. \quad (3.54)$$

Que podemos escribir de forma más compacta como

$$\begin{aligned} |\psi\rangle_A |\Phi^+\rangle_{BC} &= \frac{1}{2} \left[|\Phi^+\rangle_{AB} |\psi\rangle_C + |\Phi^-\rangle_{AB} \sigma_z^C |\psi\rangle_C \right. \\ &\quad \left. + |\Psi^+\rangle_{AB} \sigma_x^C |\psi\rangle_C + |\Psi^-\rangle_{AB} \sigma_z^C \sigma_x^C |\psi\rangle_C \right]. \end{aligned} \quad (3.55)$$

Este es el estado inicial al cual no se le ha hecho ninguna operación, ya que simplemente se ha reescrito reagrupando las etiquetas de tal manera que el qubit de Bob quede separado. Se ve que Alice solo debe realizar una medición de Bell y comunicar su resultado a Bob, luego él debe usar la transformación correspondiente para obtener $|\psi\rangle$. Por ejemplo, si Alice mide $|\Phi^-\rangle$, Bob debe emplear σ_z para recuperar $|\psi\rangle$.

Continuando con las otras partes de el estado con ruido. Podemos reescribir $|\psi\rangle|\Psi^+\rangle$ usando la ecuación (3.37), es decir

$$|\psi\rangle_A |\Psi^+\rangle_{BC} = \sigma_x^B |\psi\rangle_A |\Phi^+\rangle_{BC} \quad (3.56)$$

$$\begin{aligned} &= \sigma_x^B \frac{1}{2} \left[|\Phi^+\rangle_{AB} |\psi\rangle_C + |\Phi^-\rangle_{AB} \sigma_z^C |\psi\rangle_C \right. \\ &\quad \left. + |\Psi^+\rangle_{AB} \sigma_x^C |\psi\rangle_C + |\Psi^-\rangle_{AB} \sigma_z^C \sigma_x^C |\psi\rangle_C \right]. \end{aligned} \quad (3.57)$$

Multiplicando σ_x^B por cada estado de Bell dentro del paréntesis y empleando las ecuaciones (3.37), (3.40), (3.43) y (3.46), obtenemos

$$\begin{aligned} |\psi\rangle_A |\Psi^+\rangle_{BC} &= \frac{1}{2} \left[|\Psi^+\rangle_{AB} |\psi\rangle_C + |\Psi^-\rangle_{AB} \sigma_z^C |\psi\rangle_C \right. \\ &\quad \left. + |\Phi^+\rangle_{AB} \sigma_x^C |\psi\rangle_C + |\Phi^-\rangle_{AB} \sigma_z^C \sigma_x^C |\psi\rangle_C \right]. \end{aligned} \quad (3.58)$$

En seguida, podemos reescribir $|\psi\rangle|\Phi^-\rangle$ usando la ec (3.39), esto es

$$\begin{aligned} |\psi\rangle_A |\Phi^-\rangle_{BC} &= \sigma_z^B |\psi\rangle_A |\Phi^+\rangle_{BC} \\ &= \sigma_z^B \frac{1}{2} \left[|\Phi^+\rangle_{AB} |\psi\rangle_C + |\Phi^-\rangle_{AB} \sigma_z^C |\psi\rangle_C \right. \\ &\quad \left. + |\Psi^+\rangle_{AB} \sigma_x^C |\psi\rangle_C + |\Psi^-\rangle_{AB} \sigma_z^C \sigma_x^C |\psi\rangle_C \right]. \end{aligned} \quad (3.59)$$

Multiplicando σ_z^B por cada estado de Bell dentro del paréntesis y empleando las ecuaciones (3.39), (3.42), (3.45) y (3.48), obtenemos

$$\begin{aligned} |\psi\rangle_A |\Phi^-\rangle_{BC} &= \frac{1}{2} \left[|\Phi^-\rangle_{AB} |\psi\rangle_C + |\Phi^+\rangle_{AB} \sigma_z^C |\psi\rangle_C \right. \\ &\quad \left. + |\Psi^-\rangle_{AB} \sigma_x^C |\psi\rangle_C + |\Psi^+\rangle_{AB} \sigma_z^C \sigma_x^C |\psi\rangle_C \right]. \end{aligned} \quad (3.60)$$

Finalmente, reescribiendo $|\psi\rangle|\Psi^-\rangle$ usando la ec (3.38), tenemos

$$\begin{aligned} |\psi\rangle_A |\Psi^-\rangle_{BC} &= \sigma_z^B \sigma_x^B |\psi\rangle_A |\Phi^+\rangle_{BC} \\ &= \sigma_z^B \sigma_x^B \frac{1}{2} \left[|\Phi^+\rangle_{AB} |\psi\rangle_C + |\Phi^-\rangle_{AB} \sigma_z^C |\psi\rangle_C \right. \\ &\quad \left. + |\Psi^+\rangle_{AB} \sigma_x^C |\psi\rangle_C + |\Psi^-\rangle_{AB} \sigma_z^C \sigma_x^C |\psi\rangle_C \right]. \end{aligned} \quad (3.61)$$

Multiplicando $\sigma_z^B \sigma_x^B$ por cada estado de Bell dentro del paréntesis y empleando las ecuaciones (3.38), (3.41), (3.44) y (3.47), obtenemos

$$\begin{aligned} |\psi\rangle_A |\Psi^-\rangle_{BC} &= \frac{1}{2} \left[-|\Psi^-\rangle_{AB} |\psi\rangle_C + |\Psi^+\rangle_{AB} \sigma_z^C |\psi\rangle_C \right. \\ &\quad \left. - |\Phi^-\rangle_{AB} \sigma_x^C |\psi\rangle_C + |\Phi^+\rangle_{AB} \sigma_z^C \sigma_x^C |\psi\rangle_C \right]. \end{aligned} \quad (3.62)$$

Tenemos todas las partes de ρ_0 . Ahora, proyectemos el estado $\rho_0 = |\psi\rangle\langle\psi| \rho_w$ en cada estado de Bell obteniendo el operador de densidad no normalizado del qubit de Bob. Comencemos proyectando sobre $|\Phi^+\rangle$. De las ecuaciones (3.36), (3.55), (3.58), (3.60) y (3.62), tenemos

$$\begin{aligned}\hat{\rho}_C(|\Phi^+\rangle) &= \langle\Phi^+|_{AB} |\psi\rangle\langle\psi|_A \rho_w^{BC} |\Phi^+\rangle_{AB} \\ &= \frac{F}{4} |\psi\rangle\langle\psi| + \frac{1-F}{12} \left[\sigma_x |\psi\rangle\langle\psi| \sigma_x + \sigma_z |\psi\rangle\langle\psi| \sigma_z \right. \\ &\quad \left. + \sigma_z \sigma_x |\psi\rangle\langle\psi| \sigma_x \sigma_z \right].\end{aligned}\quad (3.63)$$

Proyectando sobre $|\Phi^-\rangle$. De las ecuaciones (3.36), (3.55), (3.58), (3.60) y (3.62), tenemos

$$\begin{aligned}\hat{\rho}_C(|\Phi^-\rangle) &= \langle\Phi^-|_{AB} |\psi\rangle\langle\psi|_A \rho_w^{BC} |\Phi^-\rangle_{AB} \\ &= \frac{F}{4} \sigma_z |\psi\rangle\langle\psi| \sigma_z + \frac{1-F}{12} \left[\sigma_x |\psi\rangle\langle\psi| \sigma_x + |\psi\rangle\langle\psi| \right. \\ &\quad \left. + \sigma_z \sigma_x |\psi\rangle\langle\psi| \sigma_x \sigma_z \right].\end{aligned}\quad (3.64)$$

Proyectando sobre $|\Psi^+\rangle$. De las ecuaciones (3.36), (3.55), (3.58), (3.60) y (3.62), tenemos

$$\begin{aligned}\hat{\rho}_C(|\Psi^+\rangle) &= \langle\Psi^+|_{AB} |\psi\rangle\langle\psi|_A \rho_w^{BC} |\Psi^+\rangle_{AB} \\ &= \frac{F}{4} \sigma_x |\psi\rangle\langle\psi| \sigma_x + \frac{1-F}{12} \left[\sigma_z |\psi\rangle\langle\psi| \sigma_z + |\psi\rangle\langle\psi| \right. \\ &\quad \left. + \sigma_z \sigma_x |\psi\rangle\langle\psi| \sigma_x \sigma_z \right].\end{aligned}\quad (3.65)$$

Finalmente, proyectando sobre $|\Psi^-\rangle$. De las ecuaciones (3.36), (3.55), (3.58), (3.60) y (3.62), tenemos

$$\begin{aligned}\hat{\rho}_C(|\Psi^-\rangle) &= \langle\Psi^-|_{AB} |\psi\rangle\langle\psi|_A \rho_w^{BC} |\Psi^-\rangle_{AB} \\ &= \frac{F}{4} \sigma_z \sigma_x |\psi\rangle\langle\psi| \sigma_x \sigma_z + \frac{1-F}{12} \left[\sigma_z |\psi\rangle\langle\psi| \sigma_z + |\psi\rangle\langle\psi| \right. \\ &\quad \left. + \sigma_x |\psi\rangle\langle\psi| \sigma_x \right].\end{aligned}\quad (3.66)$$

Calculando la traza en la base computacional de cualquiera de los $\hat{\rho}_C$, que en todos los casos es la misma, se obtiene

$$\begin{aligned}\text{tr}\{\hat{\rho}_C\} &= \sum_i \langle i | \hat{\rho}_C | i \rangle \\ &= \frac{F}{4} (|\alpha|^2 + |\beta|^2) + \frac{1-F}{12} 3(|\alpha|^2 + |\beta|^2) = \frac{1}{4}.\end{aligned}\quad (3.67)$$

Por lo tanto, los operadores de densidad normalizados del qubit de Bob son

$$\rho_C(|\Phi^+\rangle) = F|\psi\rangle\langle\psi| + \frac{1-F}{3} \left[\sigma_x |\psi\rangle\langle\psi| \sigma_x + \sigma_z |\psi\rangle\langle\psi| \sigma_z + \sigma_z \sigma_x |\psi\rangle\langle\psi| \sigma_x \sigma_z \right], \quad (3.68)$$

$$\rho_C(|\Phi^-\rangle) = F\sigma_z |\psi\rangle\langle\psi| \sigma_z + \frac{1-F}{3} \left[\sigma_x |\psi\rangle\langle\psi| \sigma_x + |\psi\rangle\langle\psi| + \sigma_z \sigma_x |\psi\rangle\langle\psi| \sigma_x \sigma_z \right], \quad (3.69)$$

$$\rho_C(|\Psi^+\rangle) = F\sigma_x |\psi\rangle\langle\psi| \sigma_x + \frac{1-F}{3} \left[\sigma_z |\psi\rangle\langle\psi| \sigma_z + |\psi\rangle\langle\psi| + \sigma_z \sigma_x |\psi\rangle\langle\psi| \sigma_x \sigma_z \right] \quad (3.70)$$

y finalmente

$$\rho_C(|\Psi^-\rangle) = F\sigma_z \sigma_x |\psi\rangle\langle\psi| \sigma_x \sigma_z + \frac{1-F}{3} \left[\sigma_x |\psi\rangle\langle\psi| \sigma_x + |\psi\rangle\langle\psi| + \sigma_z |\psi\rangle\langle\psi| \sigma_z \right]. \quad (3.71)$$

Cuando Alice mide sus dos qubits en la base de Bell, si ha medido $|\Phi^+\rangle$, Bob no debe hacer ninguna operación, ya que el estado que quiere encontrar es $|\psi\rangle$. La fidelidad del estado $|\psi\rangle$ en la teleportación, es

$$\begin{aligned} F_{|\Phi^+\rangle} &= \langle\psi| \rho_C(|\Phi^+\rangle) |\psi\rangle \\ &= F + \frac{1-F}{3} [|\langle\psi| \sigma_x |\psi\rangle|^2 + |\langle\psi| \sigma_z \sigma_x |\psi\rangle|^2 + |\langle\psi| \sigma_z |\psi\rangle|^2] \\ &= F + \frac{1-F}{3} [\text{Re}[2\alpha^* \beta]^2 + |\text{Im}[2i\alpha^* \beta]|^2 + |\alpha|^2 + |\beta|^2] \\ &= F + \frac{1-F}{3} [2\alpha^* \beta + |\alpha|^2 + |\beta|^2] \\ &= F + \frac{1-F}{3} [4|\alpha|^2 |\beta|^2 + |\alpha|^4 - 2|\alpha|^2 |\beta|^2 + |\beta|^4] \\ &= F + \frac{1-F}{3} [|\alpha|^2 + |\beta|^2] \\ &= F + \frac{1-F}{3} \end{aligned} \quad (3.72)$$

Si Alice mide $|\Phi^-\rangle$, Bob tiene que usar una compuerta σ_z , ya que el estado que quiere encontrar es $\sigma_z |\psi\rangle$. Utilizando la igualdad

$$\sigma_z \sigma_x = -\sigma_x \sigma_z \quad (3.73)$$

La fidelidad del estado $\sigma_z |\psi\rangle$ es

$$\begin{aligned} F_{|\Phi^-\rangle} &= \langle \psi | \sigma_z \rho_C(|\Phi^-\rangle) \sigma_z | \psi \rangle \\ &= F + \frac{1-F}{3} [|\langle \psi | \sigma_x | \psi \rangle|^2 + |\langle \psi | \sigma_z \sigma_x | \psi \rangle|^2 + |\langle \psi | \sigma_z | \psi \rangle|^2] \\ &= F + \frac{1-F}{3} \end{aligned} \quad (3.74)$$

Cuando Alice mide $|\Psi^+\rangle$, Bob debe encontrar $\sigma_x |\psi\rangle$. Entonces, empleando (3.73) nuevamente tenemos

$$\begin{aligned} F_{|\Psi^+\rangle} &= \langle \psi | \sigma_x \rho_C(|\Psi^+\rangle) \sigma_x | \psi \rangle \\ &= F + \frac{1-F}{3} [|\langle \psi | \sigma_x | \psi \rangle|^2 + |\langle \psi | \sigma_z \sigma_x | \psi \rangle|^2 + |\langle \psi | \sigma_z | \psi \rangle|^2] \\ &= F + \frac{1-F}{3} \end{aligned} \quad (3.75)$$

Finalmente, si Alice mide $|\Psi^-\rangle$, Bob debe tener $\sigma_z \sigma_x |\psi\rangle$. Por lo tanto

$$\begin{aligned} F_{|\Psi^-\rangle} &= \langle \psi | \sigma_z \sigma_x \rho_C(|\Psi^-\rangle) \sigma_x \sigma_z | \psi \rangle \\ &= F + \frac{1-F}{3} [|\langle \psi | \sigma_x | \psi \rangle|^2 + |\langle \psi | \sigma_z \sigma_x | \psi \rangle|^2 + |\langle \psi | \sigma_z | \psi \rangle|^2] \\ &= F + \frac{1-F}{3} \end{aligned} \quad (3.76)$$

El desempeño del protocolo es el mismo independientemente del estado inicial. Es decir, la fidelidad del estado teleportado es independiente de su condición inicial. Aún más interesante resulta ser que la fidelidad del estado teleportado es mayor que la fidelidad del estado inicial. Es decir, un pequeño deterioro en el recurso (entrelazamiento) implica también un deterioro en el protocolo de teleportación pero en menor proporción. En consecuencia, este sería un escenario interesante para estudiar corrección de errores cuánticos [2] como una alternativa al costoso método de purificación de entrelazamiento [9].

Capítulo 4

Criptografía Clásica

Historicamente, la criptografía fué el arte codificar mensajes que a pesar de ser interceptados no revelaran la información contenida en ellos. Básicamente, se transformaba un mensaje ordinario mediante algún algoritmo para dejarlo ilegible, se enviaba, y el receptor realizaba la transformación inversa para obtener el mensaje original. Para garantizar la secrecía de la comunicación, al menos una parte del proceso de transformación se mantenía en secreto entre el emisor y el receptor. Así que sin esta pieza de información no era posible entender la comunicación entre ellos [10].

En la actualidad, la criptografía se puede definir como el estudio de las técnicas matemáticas relacionadas con los aspectos de la seguridad informática tales como la privacidad o confidencialidad, la integridad de la información, la autenticación del origen y la no repudiación [10]. El único aspecto del que hablaremos aquí es la privacidad de la información la cual se refiere a mantener inaccesible el contenido de la información a las partes no autorizadas.

Al proceso de transformar un mensaje ordinario en uno ilegible, se le llama encriptación o cifrado, al proceso inverso, desencriptación o decifrado, y a la pieza de información que deben mantener en secreto las partes legítimas, se le llama llave.

4.1. Definiciones

4.1.1. Terminología básica

- Un diseño de encriptación o primitivo criptográfico es definido por tres algoritmos Gen, Enc, y Dec, y la especificación de un espacio finito de mensajes $\mathcal{M}$, con $|\mathcal{M}| > 1$. $|\mathcal{M}|$ es el número de elementos que contiene $\mathcal{M}$.
- El algoritmo que genera la llave, Gen, es un algoritmo probabilístico que entrega una llave k elegida de acuerdo a cierta distribución de probabilidad.

Denotamos como $\mathcal{K}$ al espacio finito de las llaves que pueden ser seleccionadas por Gen.

- El algoritmo de encriptación Enc toma como entrada una llave $k \in \mathcal{K}$, y un mensaje $m \in \mathcal{M}$, y entrega un texto cifrado $c \in \mathcal{C}$. Es decir, $c := \text{Enc}_k(m)$. Aquí asumimos que Enc es determinista (aunque podría ser probabilístico), esto se denota por $:=$. $\mathcal{C}$ denota el conjunto de todos los posibles textos cifrados que pueden ser producidos por $\text{Enc}_k(m)$ para todas la posibles combinaciones de $k \in \mathcal{K}$ y $m \in \mathcal{M}$.
- El algoritmo de descryptación Dec toma como entrada una llave $k \in \mathcal{K}$ y un texto cifrado $c \in \mathcal{C}$, y entrega un mensaje $m \in \mathcal{M}$. Dec siempre es determinista, es decir, $\forall k \in \mathcal{K}, \forall m \in \mathcal{M}$ y $\forall c \in \mathcal{C}$ producido por $\text{Enc}_k(m)$. Se cumple $\text{Dec}_k(c) := m$.

También es posible que la llave de encriptación sea distinta a la llave de descryptación, en este caso tendríamos que $c := \text{Enc}_e(m)$, y $m := \text{Dec}_d(c)$. Es decir, $\forall e, d \in \mathcal{K}, \forall m \in \mathcal{M}$ y $\forall c \in \mathcal{C}$ producido por $\text{Enc}_e(m)$, se cumple $\text{Dec}_d(c) := m$. A un primitivo que funcione de esta forma se le llama *asimétrico* o *de llave pública*, mientras que uno donde las llaves sean iguales, se le llama *simétrico* o *de llave privada*.

Llamaremos a las partes legítimas Alice y Bob, y a la parte ilegítima o *Adversario* que intenta atacar nuestro criptosistema, la llamaremos Eve.

4.1.2. Privacidad perfecta

Supongamos que un adversario conoce la distribución de probabilidad de $\mathcal{M}$, esto es, el adversario sabe con que frecuencia se encriptan distintos mensajes sobre todo el espacio de mensajes posibles. Por ejemplo, el espacio de mensajes podría ser $\mathcal{M} = \{\text{Atacar}, \text{No atacar}\}$, con probabilidad 0.3 y 0.7 respectivamente. Supongamos además que el adversario también conoce el primitivo criptográfico usado; lo único que no conoce es la llave que comparten las partes legítimas. Un mensaje $m \in \mathcal{M}$ es elegido y encriptado por una de las partes honestas, y el texto cifrado resultante es enviado a la otra parte. Adicionalmente, el adversario puede mirar la comunicación y observar el texto cifrado. Bajo estas circunstancias, el adversario tiene bastante conocimiento de la comunicación. Para que un primitivo criptográfico sea considerado perfectamente seguro, observar el texto cifrado no debe afectar el conocimiento del adversario sobre que mensaje fué enviado [10]. En otras palabras la probabilidad de que el mensaje m se haya enviado, dado que se ha observado el texto cifrado c , es igual a la probabilidad de que el mismo mensaje m sea enviado, independientemente de ver texto cifrado c . En el ejemplo anterior, esto es, las probabilidades de cada mensaje siguen siendo 0.3 y 0.7 respectivamente, independientemente del texto cifrado que encuentre el atacante. Esto significa que el texto cifrado no revela absolutamente ninguna información acerca del mensaje que fué encriptado, por lo tanto, el adversario no puede seguir ninguna estrategia de análisis basandose en esta información.

4.2. One time pad

En 1917, Gilbert Vernam patentó un primitivo criptográfico que satisface la definición de privacidad perfecta, llamado *one-time-pad* (OTP) [10].

Construcción de One-time-pad Dado un entero $\ell > 0$. El espacio de mensajes $\mathcal{M}$, el espacio de llaves $\mathcal{K}$, y el espacio de textos cifrados $\mathcal{C}$ son iguales a $\{0, 1\}^\ell$ (el conjunto de todas las cadenas de bits con ℓ elementos).

- Gen: el algoritmo de generación elige una llave k de $\mathcal{K} = \{0, 1\}^\ell$ de acuerdo a la distribución de probabilidad uniforme.
- Enc: dada una llave $k \in \{0, 1\}^\ell$ y un mensaje $m \in \{0, 1\}^\ell$, el algoritmo de cifrado entrega $c := k \oplus m$.
- Dec: dada una llave $k \in \{0, 1\}^\ell$ y un texto cifrado $c \in \{0, 1\}^\ell$, el algoritmo de decifrado entrega el mensaje $m := k \oplus c$.

El símbolo $\oplus$ representa la suma módulo 2 de números binarios. Esto es:

$$\begin{aligned} 0 \oplus 0 &= 0 \\ 0 \oplus 1 &= 1 \\ 1 \oplus 0 &= 1 \\ 1 \oplus 1 &= 0, \end{aligned}$$

y cuando se suman cadenas de binarios, se suman los bits que tienen la misma posición, por ejemplo:

$$\begin{array}{r} 10110 \\ 01100 \\ \hline 11010 \end{array}$$

Entonces, lo que *one-time-pad* hace para encriptar es: tomar la llave k , hacer la suma módulo dos con m . Para desencriptar: toma la llave k y hace la suma módulo dos con c para obtener m nuevamente. Por ejemplo, supongamos que la llave es $k = 01010111010100010111$, y el mensaje $m = 01000111001010100101$, entonces $\text{Enc}_k(m)$ entrega:

$$\begin{array}{r} k = 01010111010100010111 \\ m = 01000111001010100101 \\ \hline c = 00010000011110110010 \end{array}.$$

Ahora, para desencriptar tomamos el texto cifrado $c = 00010000011110110010$ y le sumamos $k = 01010111010100010111$. Entonces, $\text{Dec}_k(c)$ entrega:

$$\begin{array}{r} k = 01010111010100010111 \\ c = 00010000011110110010 \\ \hline m = 01000111001010100101 \end{array},$$

recuperando m .

OTP fué usado por varias agencias de inteligencia durante el siglo XX para encriptar sus comunicaciones secretas. Inclusive, el “teléfono rojo” que comunicaba directamente la casa blanca con el Kremlin durante la guerra fría, estaba encriptado utilizando a OTP [10].

Dos comentarios finales sobre OTP: cada llave solo puede ser usada una vez, es decir, se debe generar una llave por cada mensaje; si se usa una misma llave para varios mensajes, OTP puede ser atacado. Además, si la llave es más corta que el mensaje, OTP también puede ser atacado.

4.3. Distribución de llaves

OTP puede ser utilizado para que dos partes honestas lleven a cabo una comunicación secreta aún en presencia de un adversario, suponiendo que han compartido previamente una llave secreta. Pero, hay un problema, ¿Cómo se supone que las partes honestas compartan la llave secreta en primer lugar? Si la envían por el canal por donde quieren enviar sus mensajes, el espía podría simplemente robar la llave, ya que estamos asumiendo que el espía tiene acceso al canal.

Una posible solución sería que las partes honestas se encuentren en persona, compartan la llave, y tiempo después la utilicen para encriptar un mensaje. El método anterior sin duda funciona, ya que se han intercambiado llaves de esta manera, y en ausencia de algo mejor, no nos podemos poner exigentes, pero es poco práctico y costoso. Por supuesto, si las partes honestas son gobiernos o corporaciones multinacionales, estas tendrían los recursos para compartir cuantas llaves quieran, pero nos gustaría que existiera una forma práctica y eficiente de distribuir las llaves que se nos antojen, sin necesidad de enviar mensajeros en vuelos internacionales con veinte guardaespaldas y maletines esposados a sus muñecas.

Otra solución a este problema, como se hace desde los 70's, es utilizar criptografía de llave pública, como los criptosistemas RSA, ElGamal y ECC; que facilitan la distribución de las llaves, pero a cambio, renuncian a la privacidad perfecta, siendo solamente, computacionalmente seguros [11]. Por esta razón, los tres criptosistemas antes mencionados tienen sus días contados, ya que una computadora cuántica capaz de ejecutar el algoritmo de Shor, los podrá atacar efectivamente [12].

Debido a lo anterior, ahora se trabaja en crear criptosistemas de llave pública “quantum-resistant”, que sean seguros ante un adversario cuántico.

Capítulo 5

Criptografía Cuántica

Las computadoras cuánticas amenazan con hacer obsoletos los criptosistemas de llave pública más ampliamente usados en la actualidad, los cuales son muy prácticos, a cambio de no ser perfectamente seguros. Sin embargo, al mismo tiempo, la computación cuántica ofrece una forma conveniente de distribuir las llaves de los criptosistemas perfectamente privados, en particular OTP debido a que la información cuántica no se puede copiar de la misma forma que la información clásica [13]. Inclusive, existen también cryptosistemas cuánticos de llave pública, que dan una solución al inconveniente de tener que mantener en absoluto secreto la llave privada de los criptosistemas simétricos [14].

5.1. Protocolo BB84

Un de los protocolos utilizados para distribuir llaves privadas más conocido es BB84. Desarrollado por Bennett y Brassard en 1984 [15, 16].

Primero veamos el protocolo para un solo bit. Alice envía un qubit en una de dos bases elegida aleatoriamente, $z : \{|0\rangle, |1\rangle\}$ o $x : \{|+x\rangle, |-x\rangle\}$, siendo $|\pm x\rangle = \frac{1}{\sqrt{2}}(|0\rangle \pm |1\rangle)$. Los estados $|0\rangle$ y $|+x\rangle$ corresponden al bit 0, y los estados $|1\rangle$ y $|-x\rangle$ corresponden al bit 1. Después de que Bob recibe el qubit, lo mide en una de las mismas bases elegida aleatoriamente. Si Bob elige la misma base que Alice, entonces obtendrá exactamente el bit que ella envió, pero si elige la base incorrecta, obtendrá un resultado incorrecto con probabilidad 0.5. Por ejemplo, si Alice envía $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ y Bob mide en $x : \{|0\rangle, |1\rangle\}$, obtendrá $|0\rangle$ con probabilidad 0.5, o $|1\rangle$ con probabilidad 0.5.

Después de que Bob mide el qubit, le comunica a Alice la base que usó para medir; si es distinta a la que ella usó, desechan el valor de la medición; pero si es la misma, entonces conservan el resultado, habiendo transmitido un bit. Los casos que pueden ocurrir en la transmisión son:

$$\text{Bit de A} = \begin{cases} 0 & \left\{ \begin{array}{l} \text{A envía } |0\rangle \left\{ \begin{array}{l} \text{B mide en } z \Rightarrow \text{B obtiene 0} \\ \text{B mide en } x \left\{ \begin{array}{l} \text{B obtiene 0 con } P = 0.5 \\ \text{B obtiene 1 con } P = 0.5 \end{array} \right. \\ \text{A envía } |+\rangle \left\{ \begin{array}{l} \text{B mide en } z \left\{ \begin{array}{l} \text{B obtiene 0 con } P = 0.5 \\ \text{B obtiene 1 con } P = 0.5 \end{array} \right. \\ \text{B mide en } x \Rightarrow \text{B obtiene 0} \end{array} \right. \end{array} \right. \\ 1 & \left\{ \begin{array}{l} \text{A envía } |1\rangle \left\{ \begin{array}{l} \text{B mide en } z \Rightarrow \text{B obtiene 1} \\ \text{B mide en } x \left\{ \begin{array}{l} \text{B obtiene 0 con } P = 0.5 \\ \text{B obtiene 1 con } P = 0.5 \end{array} \right. \\ \text{A envía } |-x\rangle \left\{ \begin{array}{l} \text{B mide en } z \left\{ \begin{array}{l} \text{B obtiene 0 con } P = 0.5 \\ \text{B obtiene 1 con } P = 0.5 \end{array} \right. \\ \text{B mide en } x \Rightarrow \text{B obtiene 1} \end{array} \right. \end{array} \right. \end{array} \right.$$

Ahora, la estrategia que puede seguir el adversario Eve para robar la llave, es interceptar los qubits que Alice envía, medirlos para obtener el bit, preparar un nuevo qubit y reenviarlo a Bob, pero como Alice no revela la base que usó hasta que Bob mide los qubits, Eve tiene que adivinar, por lo tanto, cada que Eve intercepte y reenvie un qubit introducirá errores en la comunicación que Alice y Bob pueden detectar. Por ejemplo, supongamos que Alice envía $|0\rangle$, y que Eve usa la base x para medirlo y obtiene 1, entonces ella prepara un qubit nuevo $|-x\rangle$ para reenviarlo. También supongamos que cuando Bob recibe el qubit, elige la misma base que Alice y obtiene 1. Entonces, como Alice y Bob usaron la misma base para ese qubit, pero Alice envió 0 mientras que Bob recibió 1, ellos pueden detectar a Eve al comparar su bit.

Por lo tanto, al enviar cadenas de bits, una forma de detectar a Eve, es comparar cierto número de bits para ver si hay diferencias. Si las hay, se desechan los bits y se comienza de nuevo el protocolo. Si no las hay, es poco probable que Eve haya interceptado la comunicación, y se pueden usar los bits transmitidos para crear una llave privada para usarla en OTP.

Para transmitir una cadena de bits, Alice y Bob deben realizar el proceso las veces que sean necesarias. El protocolo para una cadena de qubits es:

- Alice genera aleatoriamente una cadena de n bits, a . Este binario determina la base en la que se envían los qubits; 0 significa la base z , y 1 significa la base x .
- Alice genera aleatoriamente una cadena de n bits, b . Esta es la llave que quiere transmitir a Bob.
- Alice envía los qubits de acuerdo con a y b .
- Bob genera aleatoriamente una cadena de n bits, b' . Este binario determina la base en la que se miden los qubits; 0 significa la base z , y 1 significa la base x .

- Bob crea una cadena de bits a' , utilizando los resultados de las mediciones de los qubits.
- Alice y Bob se comunican b y b' entre ellos, y conservan los bits de a y a' donde los bits de b y b' , coinciden. Obteniendo c y c' de tamaño m , con $m < n$.
- Alice y Bob, de acuerdo a un parámetro $\delta \in [0, 1]$, eligen $m \times \delta$ bits de c y c' , y los comparan entre sí. Si todos son iguales, crean la llave k y k' a partir de los $1 - m \times \delta$ bits de c y c' que no fueron comparados. Si existen diferencias entre los bits comparados, se desechan los bits y se repite el protocolo.

5.2. Protocolo BB84 con ruido

Cuando Eve interviene la comunicación de Alice y Bob, puede introducir errores, pero también el canal de comunicación o el almacenamiento de los qubits, podrían producirlos, ya que en realidad no es posible aislar un sistema cuántico completamente. Es decir, los qubits que Alice le envía a Bob son sistemas cuánticos abiertos que están sujetos a interacciones con el ambiente. En el caso ideal, Alice y Bob deshecharían la llave si es que encuentran diferencias en los bits comparados. Sin embargo, si es imposible evitar por completo que existan diferencias debido a un canal cuántico imperfecto, ellos tendrían que aceptar la presencia de discrepancias entre sus llaves.

Sabemos que la evolución de un sistema cuántico cerrado está descrito por una operación unitaria. Entonces, lo que podemos hacer es considerar dos partes, el sistema principal y el ambiente, que juntos, forman un sistema cuántico cerrado, entonces, podemos describir la evolución del sistema total como una operación unitaria.

Por ejemplo, supongamos que tenemos un qubit en el estado ρ^P , el cual atravesará un circuito cuántico y después lo enviamos a través de algún canal de comunicación. Al hacerlo, el estado total del sistema cerrado será $\rho^P \otimes \rho^A$, que es el producto del estado del sistema principal y el estado del ambiente. Mientras atraviesa el circuito y viaja por el canal, su evolución tendrá la forma

$$\varepsilon(\rho^P \otimes \rho^A) = U(\rho^P \otimes \rho^A)U^\dagger. \quad (5.1)$$

Cuando el qubit llega a su destino, ya no interactúa con el ambiente y para conocer su estado final, calculamos la traza parcial sobre el ambiente

$$\varepsilon(\rho^P) = \text{tr}_A[U(\rho^P \otimes \rho^A)U^\dagger]. \quad (5.2)$$

El objetivo de esta sección es conocer la fidelidad de la transmisión de las llaves usando BB84 en presencia de ruido, ya sea por que el protocolo es atacado o por las pérdidas que pueda sufrir en el camino. En este caso, cuando Alice envía un qubit $\rho = |\psi\rangle\langle\psi|$, Bob recibe $\varepsilon(|\psi\rangle\langle\psi|)$.

5.2.1. Primer modelo: desfasamiento

Este modelo tiene su origen en la teoría de sistemas cuánticos abiertos y se conoce como desfasamiento porque mantiene invariantes los elementos de la diagonal de la matriz de densidad. Depende del tiempo t que el qubit pasa en el canal de comunicación y una constante γ , la cual puede interpretarse como el acoplamiento del sistema central con el entorno que lo rodea. En las unidades adecuadas el parámetro t podría interpretarse como la longitud del canal cuántico en donde entre más largo sea el canal mayores pérdidas tendrá el sistema. El estudio detallado de los sistemas cuánticos abiertos va más allá del propósito de esta tesis, por lo cual simplemente mostraremos el resultado de la evolución temporal de una matriz de densidad arbitraria. Cada qubit que recibe Bob tiene la forma general

$$\varepsilon(\rho) = \rho(t) = \begin{pmatrix} \rho_{00} & \rho_{01}e^{-\gamma t} \\ \rho_{10}e^{-\gamma t} & \rho_{11} \end{pmatrix}. \quad (5.3)$$

Si $\gamma = 0$, se tiene el caso ideal.

Los operadores de densidad correspondientes a cada estado que Alice le envía a Bob son

$$\rho_0 = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \quad \rho_1 = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \quad \text{y} \quad \rho_{\pm} = \frac{1}{2} \begin{pmatrix} 1 & \pm 1 \\ \pm 1 & 1 \end{pmatrix}. \quad (5.4)$$

Al evolucionar a través del canal imperfecto, tenemos

$$\varepsilon(\rho_0) = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \quad \varepsilon(\rho_1) = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \quad \text{y} \quad \varepsilon(\rho_{\pm}) = \frac{1}{2} \begin{pmatrix} 1 & \pm e^{-\gamma t} \\ \pm e^{-\gamma t} & 1 \end{pmatrix}. \quad (5.5)$$

Por lo tanto, la probabilidad P_0 de que Bob reciba $|0\rangle$, cuando Alice envía $|0\rangle$, es

$$\begin{aligned} P_0 &= \langle 0 | \varepsilon(\rho_0) | 0 \rangle \\ &= \begin{pmatrix} 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} \\ &= 1. \end{aligned} \quad (5.6)$$

De manera similar, la probabilidad P_1 de que Bob reciba $|1\rangle$, cuando Alice envía $|1\rangle$, es

$$\begin{aligned} P_1 &= \langle 1 | \varepsilon(\rho_1) | 1 \rangle \\ &= \begin{pmatrix} 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 0 \\ 1 \end{pmatrix} \\ &= 1. \end{aligned} \quad (5.7)$$

Entonces, la transmisión de $|0\rangle$ y $|1\rangle$ no es afectada. Por lo que es igual al caso ideal.

Para los dos estados restantes en la base x , la probabilidad de que Bob reciba $|\pm x\rangle$ cuando Alice envía $|\pm x\rangle$, es

$$\begin{aligned}
P_{\pm} &= \frac{\langle 0 | \pm \langle 1 |}{\sqrt{2}} \varepsilon(\rho_{\pm}) \frac{|0\rangle \pm |1\rangle}{\sqrt{2}} \\
&= \frac{1}{4} \begin{pmatrix} 1 & \pm 1 \end{pmatrix} \begin{pmatrix} 1 & \pm e^{-\gamma t} \\ \pm e^{-\gamma t} & 1 \end{pmatrix} \begin{pmatrix} 1 \\ \pm 1 \end{pmatrix} \\
&= \frac{1}{4} (1 + e^{-\gamma t} \pm e^{-\gamma t} \pm 1) \begin{pmatrix} 1 \\ \pm 1 \end{pmatrix} \\
&= \frac{1 + e^{-\gamma t} + e^{-\gamma t} + 1}{4} \\
&= \frac{1 + e^{-\gamma t}}{2}.
\end{aligned} \tag{5.8}$$

Los qubits en base z no son afectados por el canal, pero los qubits en la base x si. Entonces, a medida que pasa el tiempo, la probabilidad de transmitir un bit exitosamente depende de la base y empeora cuando se utiliza x . Podemos pensar ahora en la probabilidad de que Bob mida exitosamente el mismo bit que manda Alice. Para ello necesitamos sumar cada una de las probabilidades con el peso correspondiente el cual es $1/4$ debido a que hay dos bits posibles codificados en dos bases posibles. La probabilidad de que coincida el bit medido por Bob y enviado por Alice es

$$\begin{aligned}
P &= \frac{1}{4} \times 1 + \frac{1}{4} \times 1 + \left(\frac{1}{4} \times \frac{1 + e^{-\gamma t}}{2}\right) + \left(\frac{1}{4} \times \frac{1 + e^{-\gamma t}}{2}\right) \\
&= \frac{1}{2} + \frac{1 + e^{-\gamma t}}{4}.
\end{aligned} \tag{5.9}$$

Entonces, para $t = 0 \implies P = 1$ y para $t \rightarrow \infty \implies P \rightarrow 3/4$.

Como la llave empleada en OTP debe ser tan larga como el mensaje y solo puede ser usada una vez. Si Alice desea mandar un mensaje que es muy largo o desea tener una conversación con Bob, ellos deben crear y transmitir varias llaves. En presencia de este ruido y sin emplear ninguna técnica de corrección de ruido, la integridad de las llaves y por lo tanto la comunicación encriptada, se verán afectadas a medida que se aumente el tiempo que tarda la transmisión de acuerdo con la ecuación (5.9). Es posible hacer una simulación de este proceso para visualizar lo que podría ocurrir a las llaves. En este caso, si Alice y Bob probaran el canal enviando una llave completa a una distancia muy corta, la llave que se trasmite es afectada por (5.3) en $t_0 = 0$. Después, envían otra llave a una distancia mayor haciendo que ahora la transmisión tome un tiempo $t_1 = t_0 + dt$, y así sucesivamente. La figura 5.1 muestra un ejemplo de la transmisión de 200 llaves de 100 bits cada una, el eje y representa las coincidencias normalizadas

entre las llaves de Alice y Bob, el eje x representa el tiempo. La figura 5.2 muestra el promedio del porcentaje de coincidencias de 200 llaves de 50 bits cada una entre Alice y Bob en 50 transmisiones independientes.

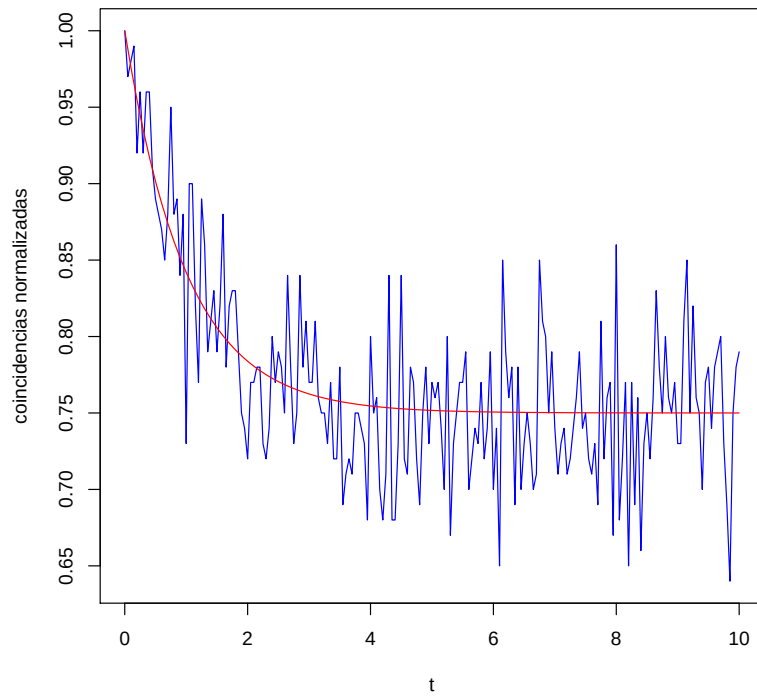


Figura 5.1: La transmisión de 200 llaves de 100 bits cada una, con $\gamma = 1$. Las coincidencias normalizadas entre las llaves de Alice y Bob son representadas por la línea azul mientras que la línea roja es la probabilidad dada por (5.9) de que los bits que mide Bob coincidan con lo que envía Alice. Aún cuando la probabilidad de coincidencia mínima es 0.75, la coincidencia real puede ser menor a este valor.

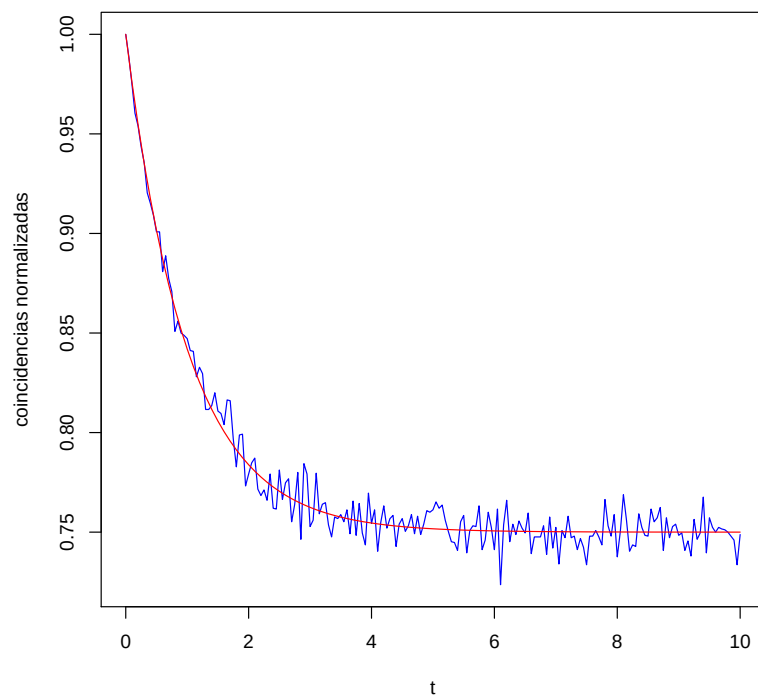


Figura 5.2: El promedio de 50 transmisiones de 200 llaves de 50 bits cada una, con $\gamma = 1$ en azul. La probabilidad de que los bits de Alice coincidan con los de Bob en rojo. En promedio, las coincidencias entre las llaves de Alice y Bob se acercan a la probabilidad dada por (5.9).

Para resumir, hemos encontrado en este modelo de ruido, que en promedio la peor coincidencia entre los bits de Alice y Bob será de 75 %. El comportamiento de este valor decae exponencialmente desde el valor inicial igual 1 al valor menor igual a 0.75. Es así que podemos concluir que este modelo de ruido no es del todo perjudicial, ya que en principio se podría estimar el tiempo de interacción o la distancia del canal que resultara en una coincidencia diferente de 1 hasta cierta tolerancia.

5.2.2. Segundo modelo: Jaynes-Cummings no markoviano

Este modelo viene de considerar un átomo de dos niveles que está en un baño de bosones que induce una degradación en el qubit [17]. Este es un modelo de canal cuántico no markoviano el cual se caracteriza por un entorno con memoria, es decir que su estado se ve afectado por el sistema central. En nuestro caso consideramos este modelo como una degradación del estado del qubit que se manda por el canal cuántico. En este modelo de ruido cada qubit que recibe Bob tiene la forma general

$$\varepsilon(\rho) = \rho(t) = \begin{pmatrix} 1 - |G(t)|^2 \rho_{11} & G(t) \rho_{01} \\ G^*(t) \rho_{01}^* & |G(t)|^2 \rho_{11} \end{pmatrix}, \quad (5.10)$$

con

$$G(t) = e^{-\frac{1}{2}t\lambda} \left[\frac{\lambda}{\Omega} \sinh\left(\frac{\Omega t}{2}\right) + \cosh\left(\frac{\Omega t}{2}\right) \right], \quad (5.11)$$

y

$$\Omega = \sqrt{-2\gamma\lambda + \lambda^2}. \quad (5.12)$$

Que se puede escribir como

$$\Omega = \lambda \sqrt{1 - 2\gamma/\lambda}. \quad (5.13)$$

Definiendo

$$\tilde{\Omega} \equiv \sqrt{1 - 2\gamma/\lambda} = \frac{\Omega}{\lambda} \quad (5.14)$$

$$\tau \equiv \lambda t, \quad (5.15)$$

podemos reescribir $G(t)$ como

$$G(\tau) = e^{-\frac{1}{2}\tau} \left[\frac{1}{\tilde{\Omega}} \sinh \frac{\tilde{\Omega}\tau}{2} + \cosh \frac{\tilde{\Omega}\tau}{2} \right] \quad (5.16)$$

Las matrices de densidad correspondientes a cada estado que puede enviar Alice son

$$\rho_0 = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \quad \rho_1 = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \quad \text{y} \quad \rho_{\pm} = \frac{1}{2} \begin{pmatrix} 1 & \pm 1 \\ \pm 1 & 1 \end{pmatrix}. \quad (5.17)$$

Al evolucionar a través del canal imperfecto, se obtiene

$$\begin{aligned} \varepsilon(\rho_0) &= \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \quad \varepsilon(\rho_1) = \begin{pmatrix} 1 - |G(\tau)|^2 & 0 \\ 0 & |G(\tau)|^2 \end{pmatrix} \\ \text{y} \quad \varepsilon(\rho_{\pm}) &= \begin{pmatrix} 1 - \frac{1}{2}|G(\tau)|^2 & \pm \frac{1}{2}G(\tau) \\ \pm \frac{1}{2}G^*(\tau) & \frac{1}{2}|G(\tau)|^2 \end{pmatrix}. \end{aligned} \quad (5.18)$$

Por lo tanto, la probabilidad P_0 de que Bob reciba un $|0\rangle$ cuando Alice envía $|0\rangle$, es

$$\begin{aligned} P_0 &= \langle 0 | \varepsilon(\rho_0) | 0 \rangle \\ &= (1 \quad 0) \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} \\ &= 1. \end{aligned} \quad (5.19)$$

De forma similar, la probabilidad P_1 de que Bob reciba $|1\rangle$ cuando Alice envía $|1\rangle$, es

$$\begin{aligned} P_1 &= \langle 1 | \varepsilon(\rho_1) | 1 \rangle \\ &= (0 \quad 1) \begin{pmatrix} 1 - |G(\tau)|^2 & 0 \\ 0 & |G(\tau)|^2 \end{pmatrix} \begin{pmatrix} 0 \\ 1 \end{pmatrix} \\ &= |G(\tau)|^2. \end{aligned} \quad (5.20)$$

Finalmente, la probabilidad $P_{\pm}$ de que Bob reciba $|\pm x\rangle$ cuando Alice envía $|\pm x\rangle$, es

$$\begin{aligned} P_{\pm} &= \frac{\langle 0 | \pm \langle 1 |}{\sqrt{2}} \varepsilon(\rho_{\pm}) \frac{|0\rangle \pm |1\rangle}{\sqrt{2}} \\ &= \frac{1}{2} (1 \quad \pm 1) \begin{pmatrix} 1 - \frac{1}{2}|G(\tau)|^2 & \pm \frac{1}{2}G(\tau) \\ \pm \frac{1}{2}G^*(\tau) & \frac{1}{2}|G(\tau)|^2 \end{pmatrix} \begin{pmatrix} 1 \\ \pm 1 \end{pmatrix} \\ &= \frac{1}{2} \left(1 - \frac{1}{2}|G(\tau)|^2 + \frac{1}{2}G^*(\tau) \pm \frac{1}{2}G(\tau) \pm \frac{1}{2}|G(\tau)|^2 \right) \begin{pmatrix} 1 \\ \pm 1 \end{pmatrix} \\ &= \frac{1}{2} \left(1 + \frac{1}{2}G^*(\tau) + \frac{1}{2}G(\tau) \right) \\ &= \frac{1}{2} + \frac{1}{4}G^*(\tau) + \frac{1}{4}G(\tau) \\ &= \frac{1}{2} + \frac{1}{2}G(\tau). \end{aligned} \quad (5.21)$$

En este caso $|0\rangle$ no es afectado, por lo que se reduce al caso ideal. Sin embargo, $|1\rangle$ y $|\pm x\rangle$ si se ven afectados. La probabilidad de que Bob encuentre correctamente estos estados es $|G(\tau)|^2$ y $\frac{1}{2} + \frac{1}{2}G(\tau)$ respectivamente. Entonces, en la medida que el tiempo que el qubit pasa en el canal es mayor, la fidelidad de la llaves entre Alice y Bob empeora. La probabilidad de que Bob mida el mismo bit que Alice envía, es

$$\begin{aligned} P &= \frac{1}{4} \times 1 + \frac{1}{4} \times |G(\tau)|^2 + \frac{1}{2} \times \left(\frac{1}{2} + \frac{1}{2}G(\tau) \right) \\ &= \frac{1}{2} + \frac{|G(\tau)|^2}{4} + \frac{G(\tau)}{4}. \end{aligned} \tag{5.22}$$

Entonces, para $\tau = 0 \implies P = 1$ y cuando $\tau \rightarrow \infty \implies P \rightarrow 1/2$. La figura 5.3 muestra la forma de (5.22)

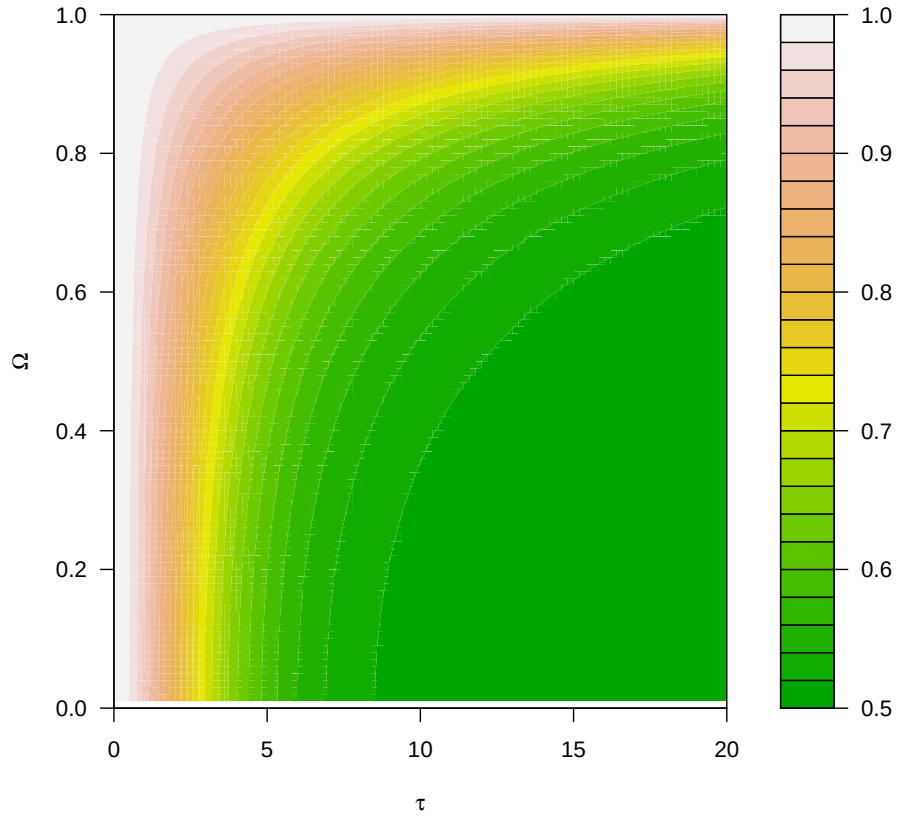


Figura 5.3: P como función de τ y $\tilde{\Omega}$. El valor máximo 1 es representado por rosa y el valor mínimo 0.5 por verde. La probabilidad de las coincidencias de los bits entre Alice y Bob empeora bastante para valores de $\tilde{\Omega} \simeq 0$ mientras que para $\tilde{\Omega} \simeq 1$ es más moderado. Para valores de τ grandes, P tiende a su valor mínimo 0.5 excepto para $\tilde{\Omega} = 1$ que se reduce al caso ideal.

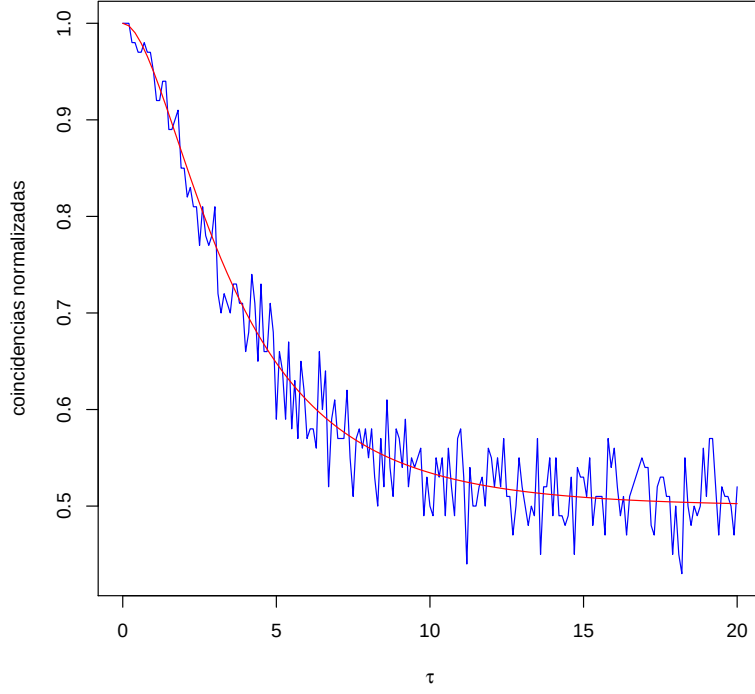


Figura 5.4: La transmisión de 200 llaves de 100 bits cada una con $\tilde{\Omega} = 1/2$ en azul. La probabilidad de que los bits de Alice coincidan con los de Bob en rojo.

Es posible visualizar lo que ocurre con la transmisión con este modelo de ruido haciendo una simulación. Nuevamente Alice y Bob pueden probar el canal cuántico enviando la primera llave a una distancia muy corta lo que toma un tiempo $t = 0$. Después, realizan la transmisión de la siguiente llave a una distancia mayor lo que hace que tome un tiempo $t = t + dt$ y así sucesivamente. La figura 5.4 muestra en azul las coincidencias normalizadas de 200 llaves de 100 bits cada una con $\tilde{\Omega} = 1/2$ y la línea roja la probabilidad (5.22) de que coincidan los bits enviados por Alice con las mediciones de Bob. La figura 5.5 muestra el promedio de 50 transmisiones de 200 llaves de 50 bits cada una con $\tilde{\Omega} = 1/2$ en azul y en rojo la probabilidad de coincidencia (5.22).

Este modelo de ruido es más perjudicial para las llaves transmitidas excepto para el caso $\tilde{\Omega} = 1$ que se reduce al caso ideal, es decir no hay ruido. El comportamiento del decaimiento también es exponencial, dando como límite 0.5 cuando $\tau \rightarrow \infty$.

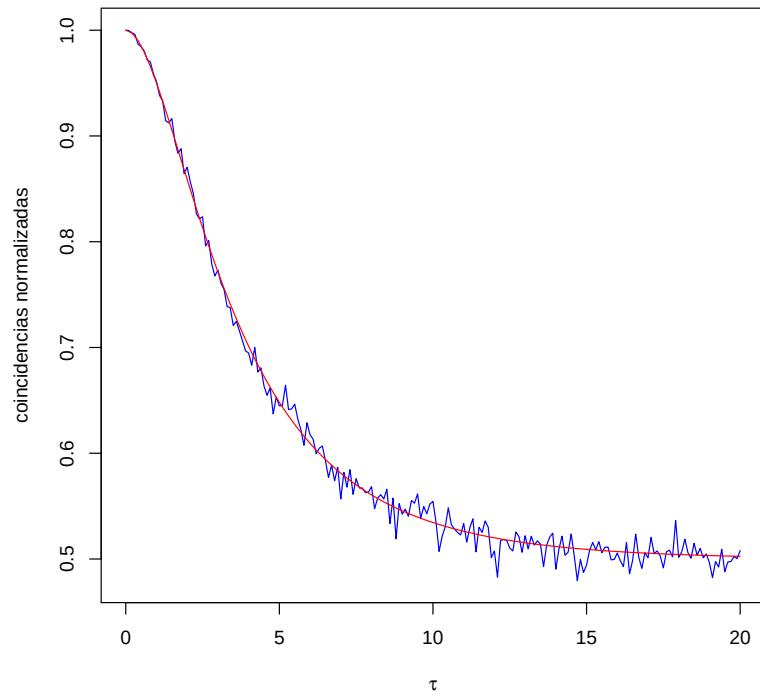


Figura 5.5: La línea azul representa el promedio de 50 transmisiones de 200 llaves de 50 bits cada una con $\tilde{\Omega} = 1/2$.

Capítulo 6

Conclusiones

Aunque son maravillosas las cosas que se pueden lograr con la computación cuántica en un caso ideal, es importante considerar los casos no ideales, ya que los sistemas reales son imperfectos. En este trabajo se ha mostrado lo que ocurre en protocolos de teleportación y criptografía cuántica cuando se introducen imperfecciones debidas al entorno que rodea al sistema.

En el caso de teleportación cuántica, donde el recurso empleado es un estado máximamente entrelazado consideramos en primera instancia un estado que difiere ligeramente de un estado de Bell, es decir, utilizamos un estado mixto cuyos eigenvectores son un estado de Bell y el estado de los dos qubits en el estado base. Se encontró que bajo esta condición inicial la fidelidad del qubit teleportado depende del estado inicial y del resultado de la medición del protocolo de teleportación. En una segunda instancia consideramos estados mixtos del tipo Werner los cuales son diagonales en la base de Bell y dependen únicamente de un parámetro F que mide la similitud con el estado de Bell preferencial. En este caso se encontró que la fidelidad del estado teleportado no depende del estado inicial ni del resultado de la medición del protocolo. Más aún, la fidelidad del estado teleportado es mayor que la fidelidad del estado entrelazado que representa el recurso del protocolo. Esto resulta interesante pues cualquier estado de dos qubits puede ser llevado a un estado de Bell utilizando operaciones sobre qubits individuales. De esta forma, esta familia de estados, para una fidelidad moderada resultan en estados aceptables para llevar a cabo el protocolo de teleportación siempre y cuando se pueda tolerar cierto error medido por la fidelidad del estado teleportado.

En el caso de la transmisión de llaves criptográficas privadas, consideramos que el canal cuántico presenta imperfecciones que afectan a los qubits al ser transmitidos. Estas imperfecciones del canal se traducen en un decaimiento de las coincidencias de las llaves secretas entre Alice y Bob a medida que el tiempo que toma la comunicación aumenta. Esto podría deberse a que se ha aumentado la distancia de comunicación y por lo tanto el tiempo que deben pasar los qubits en el canal ha aumentado proporcionalmente. Encontramos que el primer modelo de ruido no fué tan perjudicial para la comunicación ya que solo uno de los cuatro

estados enviados es afectado. Es decir, en promedio, la peor coincidencia que se produce es del 75 %. El segundo modelo de ruido considerado, demostró ser más perjudicial para la comunicación ya que en este caso, tres de los cuatro estados enviados fueron afectados por el canal. Dando como resultado que en promedio la peor coincidencia entre las llaves de Alice y Bob sea del 50 %. Alice y Bob podrían estimar una distancia que resultara en una coincidencia menor a 1 con cierto nivel de tolerancia. El siguiente paso que podrían tomar Alice y Bob sería la implementación de técnicas de corrección de ruido para mejorar la coincidencia de sus llaves.

Bibliografía

- [1] Thornton S. T. & Rex A. Moder. (2013). Modern Physics for Scientists and Engineers Fourth Edition. United States of America. Ceneage Learning.
- [2] Nielsen, M. A. & Chuang, I. L. (2010). Quantum Computation and Quantum Information (10th Anniversary Edition.). Cambridge, United Kingdom: Cambridge University Press.
- [3] Solovay R. & Strassen V. (1977). A Fast Monte-Carlo Test for Primality. SIAM Journal on Computing, 6(1), 84-85.
- [4] Deutsch D. (1985). Quantum theory, the Church-Turing principle and the universal quantum computer. Proceedings of the Royal Society of London Series A, 400(1818), 97-117.
- [5] <https://www.ibm.com/quantum-computing/learn/what-is-quantum-computing>
- [6] Breuer, H. P. & Petruccione F. (2002). The Theory of Open Quantum Systems. New York: Oxford University Press.
- [7] bit. (s.f). En Wikipedia. Recuperado el 8 de agosto de 2019 de <https://es.wikipedia.org/wiki/Bit>
- [8] Sakurai J. J. & Tuan S. F. (1994). Modern Quantum Mechanics, Rev. ed. (1994). United States of America, Addison-Wesley.
- [9] Charles H. B., Gilles B., Sandu P., Benjamin S., John A. S. & William K. W. (1996). Purification of Noisy Entanglement and Faithful Teleportation via Noisy Channels. Phys. Rev. Lett. 76. 722.
- [10] Katz, J. & Lindell, Y. (2015). Introduction to modern cryptography. Boca Raton, FL: CRC Press.
- [11] Stallings, W. (2017). Cryptography and Network Security: Principles and Practice, 7 th Edition. Malasya: Pearson Education.
- [12] Shor P. W. (1996). Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer. SIAM J. Comput. 26(5). 1484–1509.

- [13] Wootters, W. K. & Zurek, W. H. (1982). A single quantum cannot be cloned. *Nature*, 299, 802–803.
- [14] Seyfarth U., Nikolopoulos G. M. & Alber G. (2012). Symmetries and security of a quantum-public-key encryption based on single-qubit rotations. *American Physical Society*. 77. 032348.
- [15] Bennett C.H. & Brassard G. (1984). Quantum Cryptography: Public Key Distribution and Coin Tossing. In *Proceedings of IEEE International Conference on Computers, Systems, and Signal Processing*, Bangalore, India, December 1984 (IEEE, New York, 1984), p. 175.
- [16] Bergou, J. A. & Hillery, M. (2013). *Introduction to the Theory of Quantum Information Processing*. New York, United States: Springer.
- [17] Carlos Pineda, Thomas Gorin, David Davalos, Diego A. Wisniacki, and Ignacio García-Mata. (2016). Measuring and using non-Markovianity. *American Physical Society*. 93. 022117.