Simulación de una distribución cuántica de llaves en presencia de ruido

Daniel Ricardo Sabogal Perez*
(Fecha: December 14, 2020)

La distribución cuántica de llaves consiste en transmitir una llave de bits utilizando un canal cuántico. La transmisión de la llave puede ser afectada por el ruido causado en la interacción qubit-ambiente (decoherencia), por lo tanto se induce un error en la clave (QBER). Al utilizar un canal exoticamente desfasante, se puede estudiar el ruido que causa este canal mediante un proceso computacional que simule la distribución cuántica de llaves. Utilizando esta simulación de 2×10^6 qubits se encontró que utilizando dos canales desfasantes se obtiene un protocolo BB84 más seguro cuando se corrige el ruido en función de un parámetro experimental d_c .

I. INTRODUCCIÓN

La seguridad en la transmisión de información es tema que no carece de importancia hoy en día, por lo tanto existen distintos tipos de criptografía que permiten obtener confidencialidad entre dos usuarios. A diferencia de los métodos convencionales utilizados en la criptografía tradicional, la distribución cuántica de llaves (QKD) permite una comunicación segura entre dos usuarios utilizando las leyes de la física cuántica, en donde no se puede duplicar, medir sin perturbar o medir simultáneamente ciertas propiedades del sistema [1].

Una llave es distribuida por una cadena de bits cuánticos (qubits) que pueden ser codificados en distintas entidades físicas. Teóricamente, en 1984 Brasard y Bennet proponen el protocolo BB84, en donde se plantea utilizar qubits para distribuir una llave entre un emisor y receptor llamados convencionalmente Alice y Bob [2]. Para implementar el protocolo BB84 es necesario utilizar un canal cuantico que permita explotar las propiedades del sistema. Sin embargo, los qubits en una distribución de llaves real interactúan con el ambiente y pierden sus propiedades cuánticas, este proceso es llamado decoherencia [1].

El operador densidad permite obtener información de la decoherencia sufrida por el estado en un canal. En otras palabras, información acerca del proceso que induce perdidas en la pureza del estado. Para estudiar este fenomeno se utiliza Quantum Process Tomography (QPT), esto con el fin de obtener una caracterización asociada al proceso que cambia la matriz densidad del estado [3].

La decoherencia sufrida por los qubits generá un ruido en la clave obtenida. Por lo tanto, se puede definir una cantidad que cuantifique que tan bien fue distribuida la clave, esta cantidad es llamada Quantum Bit Error Rate (QBER) y denota el cociente entre el numero de bits erróneos y el numero de bits generados en una muestra de la clave.

Especificamente, el QBER se puede estudiar si se considera un canal cuántico exóticamente desfasante implementando en [4], este canal permite obtener una decoherencia definida utilizando un parametro experimental d_c. Debido a esto, se puede corregir la decoherencia utilizando un canal inversamente desfasante que permita corregir el ruido inducido con el fin de tener un protocolo más seguro.

II. MARCO TEÓRICO

En el protocolo BB84, Alice utiliza un canal cuántico para elegir aleatoriamente un bit y una base en la cual codifica el estado que envía. Posteriormente, cuando Bob recibe el estado cuántico, realiza una medición en una base escogida aleatoriamente y registra el valor obtenido. Utilizando un canal publico, Alice y Bob comparten las bases usadas y descartan todos los valores obtenidos cuando las bases del estado preparado no coincide con la base del estado en la medición. Los bits que aún permanecen en la lista son considerados la clave[2].

Utilizando el estado de polarización de la luz, el estado enviado se puede escribir como $|\phi\rangle = \alpha\,|H\rangle + \beta\,|V\rangle$, en donde α y β son las amplitudes de probabilidad, $|H\rangle$ y $|V\rangle$ hacen referencia al estado horizontal y vertical de polarización.

El canal cuántico desfasante estudiado en este proyecto acopla el estado de polarización de la luz $|\phi\rangle$ y su momento transversal $|\xi\rangle$ como se muestra en la figura 1. Este canal cuántico induce decoherencia en función de un parámetro experimental d_c. Por lo tanto, al conocer el parámetro d_c es posible corregir la decoherencia inducida mediante un canal inversamente desfasante y así recuperar la pureza del estado .

El operador matriz densidad $\hat{\rho} = |\Psi\rangle\langle\Psi|$ da información de la pureza del estado si este no es completamente puro. Para describir con certeza la

* Universidad de los Andes ; dr.sabogal@uniandes.edu.co

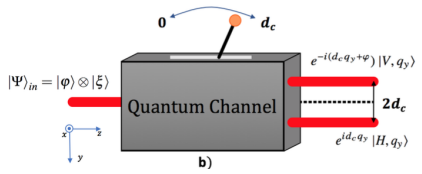

FIG. 1: Canal desfasante. Imagen tomada de [4]

transformación que le ocurre a $\hat{\rho}$ al entrar a un canal desfasante es necesario utilizar QPT.

QPT consiste en una caracterización completa de un proceso, para esto es necesario en encontrar el mapeo lineal ε que actúa sobre $\hat{\rho}$. En otras palabras, $\hat{\rho}_{out} = \varepsilon(\hat{\rho}_{in})$. Normalmente ε se puede escribir como

$$\varepsilon(\hat{\rho}_{in}) = \sum_{n,m} \chi_{mn} \hat{\sigma}_m \hat{\rho}_{in} \hat{\sigma_n}^{\dagger}, \tag{1}$$

en donde $\hat{\sigma}_m$ y $\hat{\sigma}_n$ hacen referencia a los operadores de Pauli más la matriz identidad $\hat{\sigma}_0$, $\hat{\rho}_{in}$ la matriz densidad que entra al proceso y χ_{mn} los elementos matriciales que caracterizan el proceso [3]. Por lo tanto, es necesario obtener la matriz χ asociada al el proceso, para esto se puede se puede escribir el mapeo como $\varepsilon(\hat{\rho}_k) = \sum_j \lambda_{jk} \hat{\rho}_j$, en donde $\hat{\rho}_j$ forma una base en el espacio de Hilbert 2x2 y λ_{jk} son datos obtenidos experimentalmente. Por otro lado, también se puede definir los coeficientes β_{jk}^{mn} tal que $\hat{\sigma}_m \hat{\rho}_j \hat{\sigma}_n^{\dagger} = \sum_k \beta_{jk}^{mn} \hat{\rho}_k$. De esta forma, se puede mostrar que

$$\sum_{m,n} \beta_{jk}^{mn} \chi_{mn} = \lambda_{jk}. \tag{2}$$

Utilizando la ecuación (2) se puede obtener con facilidad la matriz χ y caracterizar cualquier proceso si se tiene datos acerca de la transformación de la matriz $\hat{\rho}$.

III. ESTRUCTURA SIMULACIÓN

Para realizar la simulación de QKD fue necesario utilizar las librerías de Numpy, Matplotlib, Scipy y Qutip del lenguaje de programación Python.

La simulación se realizó utilizando el protocolo BB84, en donde se toma ventaja de la capacidad computacional para generar números aletorios. De esta manera, se logra escoger una serie de bits y bases con el fin de transmitir la llave. Adicionalmente, cada qubit entra a una combinación de canales que se muestran en las figuras 2 y 3.

FIG. 2: Combinación de canales cuánticos que permite controlar el ruido. Esta combinación esta conformada por un un canal desfasante en función del parámetro d_c, un canal despolarizante que simula una distribución de llaves a largas distancias y un canal desfasante inverso para controlar el ruido inducido.

FIG. 3: Combinación de canales cuánticos que induce ruido no controlado en función del parámetro d_c. El canal despolarizante también se tiene en cuenta en esta combinación de canales.

Se transmitieron 5000 claves utilizando 100 veces 50 valores distintos del parámetro d_c para cada combinación de canales. Cada clave fue distribuida enviando 2×10^6 qubits, de está manera se puede obtener una clave con un número de bits $\approx 1 \times 10^6$. Todo esto, con el fin de ver cómo cambia el QBER en función del parámetro d_c.

IV. RESULTADOS

Utilizando los resultados teóricos mostrados en [4], se generó un arreglo de matrices densidad para caracterizar los canales desfasantes. Para esto, se usó el cambio en la matriz densidad de los estados $|H\rangle$, $|V\rangle$, $\frac{1}{\sqrt{2}}(|H\rangle + |V\rangle)$ y $\frac{1}{\sqrt{2}}(|H\rangle + i\,|V\rangle)$. Por otro lado, el canal despolarizante se caracterizó con los mismos estados y la definición teórica mostrada en [1]. Como un ejemplo, se puede mostrar la caracterización de los canales desfasantes en las figuras 4 y 5, mientras que el canal despolarizante se evidencia en la figura 6.

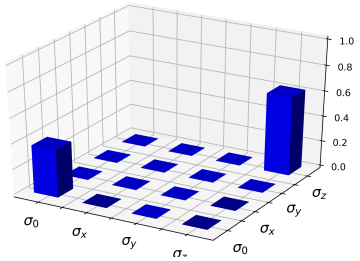

FIG. 4: $Re(\chi)$ Canal desfasante($d_c = 0.5$)

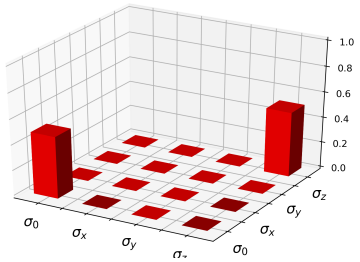

FIG. 5: $Re(\chi)$ Canal inversamente desfasante($d_c = -0.5$).

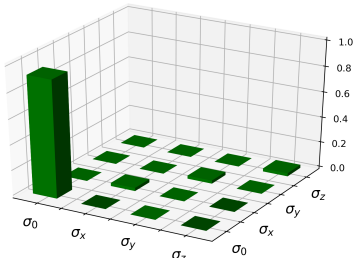

FIG. 6: $Re(\chi)$ Canal despolarizante, probabilidad despolarizante $p = 0.1$

Puede verse en las figuras anteriores que el canal despolarizante generá un coeficiente asociado a la matriz identidad en el proceso mostrado en la ecuación (1). Por otro lado, los canales desfasantes tienen coeficientes en la matriz identidad y adicionalmente rotaciones con el operador σ_z.

Utilizando 50 valores del parámetro d_c en la combinación de canales de la figura 3 se puede obtener un QBER. La figura 7 muestra el comportamiento del QBER en función del parametro(d_c). En este caso, los puntos hacen referencia a los resultados obtenidos en la simulación y la linea continua a una función de error obtenida en [5]. Por otro lado, se puede notar que este comportamiento es oscilatorio y a medida que aumenta d_c el error en la clave se estabiliza en 0.5.

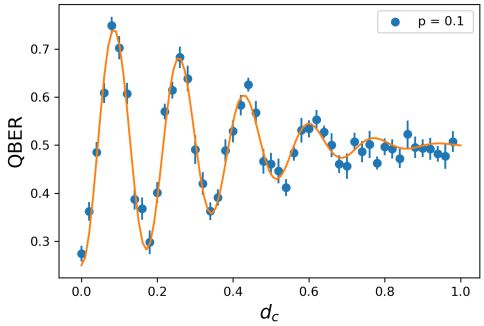

FIG. 7: Quantum bit error rate utilizando d_c en el canal desfasante y una probabilidad despolarizante de $p = 0.1$

Por otro lado, la figura 8 muestra el comportamiento del QBER cuando se intenta corregir el ruido generado por el primer canal desfasante. Se puede notar que aunque se corrige el ruido, el QBER no está en cero completamente. Se puede atribuir este comportamiento al canal despolarizante ya que se cambia la polarización del estado con una probabilidad $p = 0.1$.

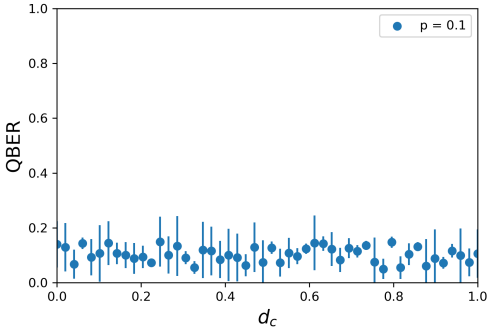

FIG. 8: Quantum bit error rate utilizando $|d_c|$ para el canal desfasante y desfasante inverso.

Las figuras 7 y 8 muestran cómo se puede corregir el error en la clave si el canal desfasante y inversamente desfasante utilizan el mismo $|d_c|$. Por lo tanto, si Alice y Bob tienen control de este parámetro es posible obtener un protocolo más seguro. Esto es, porque además de realizar el protocolo BB84 estándar, se necesita intercambiar el parámetro externo d_c para poder recuperar la clave sin un error significativo. Adicionalmente, se puede utilizar los valores óptimos del parámetro d_c con el fin de obtener una seguridad adicional en presencia de un espía. En otras palabras, si un espia intercepta la clave, obtendrá un resultado sin información relevante si $d_c > 0.5$.

V. CONCLUSIONES

Se caracterizó el proceso de perdida de pureza sufrido en un canal cuántico utilizando QPT. De esta manera, se logra especificar con exactitud que tanta decoherencia sufre un estado en el canal. Posteriormente, utilizando la caracterización exacta del canal se puede obtener un canal inversamente desfasante que asista el ruido y permita recuperar la información transportada por el estado. Por ultimo, se estudio el QBER en función del parámetro d_c para obtener un protocolo más seguro si Alice y Bob intercambian este parámetro.

VI. ANALISIS PERSPECTIVAS

Los objetivos propuestos inicialmente de estudiar el QBER y mostrar cómo se puede utilizar ventajosamente para obtener mayor seguridad fueron alcanzados. Sin embargo, no se logró comparar la fidelidad del proceso caracterizado respecto a la fidelidad esperada teóricamente.

[1] M. Nielsen and I. Chuang, *Quantum Computation and Quantum Information: 10th Anniversary Edition* (Cambridge University Press, 2010).

[2] C. H. Bennett and G. Brassard, Theoretical Computer Science **560**, 7 (2014), theoretical Aspects of Quantum Cryptography – celebrating 30 years of BB84.

[3] I. Bongioanni, L. Sansoni, F. Sciarrino, G. Vallone, and P. Mataloni, Phys. Rev. A **82**, 042307 (2010).

[4] D. F. Urrego, J.-R. Álvarez, O. Calderón-Losada, J. Svozilík, M. N. nez, and A. Valencia, Opt. Express **26**, 11940 (2018).

[5] A. F. Herrera Fernández and A. C. Valencia González, *Noise assisted quantum key distribution.* (Uniandes, 2019).