Formato de Presentación de Informes para emisión de paz y salvos de Asistencias Intersemestrales (junio-julio 2022)
Fecha de entrega: 19 de Julio 2022 (fecha de envío al profesor asesor**)**

1. **Nombre del estudiante y código**

Daniel Ricardo Sabogal Pérez
201512414

2. **Programa de posgrado al que pertenece**

Maestría en Ciencias - Física

3. **Nombre del profesor asesor**

Alejandra Catalina Valencia González

4. **Título de la propuesta**

Estudio de la decoherencia en el protocolo de distribución cuántica de llaves BB84.

La distribución cuántica de llaves permite obtener confidencialidad entre dos usuarios convencionalmente llamados Alice y Bob mediante una llave que es capaz de cifrar y descifrar información. El primer protocolo de distribución cuántica de llaves fue desarrollado por primera vez por Gilles Brassard y Chales Bennet en el año 1984, este método consiste en distribuir una llave utilizando el estado de polarización de la luz y las leyes de la mecánica cuántica [1].

Para implementar experimentalmente el protocolo BB84 es necesario tener en cuenta detalles técnicos como el uso de una fuente de fotones individuales [2] para distribuir la llave con confidencialidad. Sin embargo, este requerimiento es difícil de alcanzar aun cuando se tiene tecnología sofisticada. Una alternativa para lograr este requerimiento es una fuente de fotones individuales anunciados. Esta fuente consiste en fotones que son generados espontáneamente, pero existe un mecanismo que anuncia la producción del fotón exitosamente.

La seguridad de la distribución cuántica de llaves tiene como soporte las leyes de la mecánica cuántica. Una espía, convencionalmente llamada Eva, puede utilizar ataques sofisticados para obtener información acerca de la llave. Un ataque especifico es el *Single photon two-qubit quantum logic gate attack* (SPTQQLG) [3]. En este ataque Eva puede obtener información de la clave pagando el precio de inducir errores en la distribución de llaves entre Alice y Bob.

La distribución de la llave en el protocolo BB84 también puede ser afectada por ruido. Un tipo de ruido que aparece en información cuántica es la decoherencia. La decoherencia esta asociada a la perdida de información codificada en un sistema cuántico y ha sido estudiada en sistemas ópticos de tal manera que la polarización de la luz es acoplada con variables espaciales induciendo decoherencia controlada [4].

En esta propuesta, se estudiarán los efectos de decoherencia en el protocolo BB84 cuando Eva utiliza el ataque SPTQQLG. Para esto, un arreglo de doble decoherencia controlada se usará. En este arreglo la decoherencia inducida por Alice será revertida por Bob. La presente propuesta tiene componente teórica y experimental. En la parte teórica, se explicarán y cuantificarán las ventajas de utilizar el arreglo de doble decoherencia controlada ante el ataque SPTQQLG. En la parte experimental, se implementará el protocolo BB84 distribuyendo la clave con una fuente de fotones individuales anunciados.

[1] Charles H Bennett and Gilles Brassard. Quantum cryptography: Public key distribution and coin tossing. Theoretical Computer Science, 560:7–11, 2014.

[2] M. D. Eisaman, J. Fan, A. Migdall, and S. V. Polyakov. Invited review article: Single-photon sources and detectors. Review of Scientific Instruments , 82(7):071101, 2011.

[3] Jeffrey H Shapiro and Franco NC Wong. Attacking quantum key distribution with single-photon two-qubit quantum logic. Physical Review A, 73(1):012315, 2006.

[4] Daniel F Urrego, Juan-Rafael Álvarez, Omar Calderón-Losada, Jiri Svozilık, Mayerlin Nuñez, and Alejandra Valencia. Implementation and characterization of a controllable dephasing channel based on coupling polarization and spatial degrees of freedom of light. Optics Express, 26(9):11940–11949, 2018.

5. **Objetivos propuestos**:

Objetivo general:

Estudiar los efectos de decoherencia en el protocolo BB84 bajo el ataque SPTQQLG.

Objetivo específico:

1. Desarrollar un modelo teórico que permita explicar las ventajas del arreglo de doble decoherencia controlada bajo el ataque SPTQQLG.
2. Implementar el protocolo BB84 con una fuente de fotones individuales anunciados.

6.**Metodologia**:

Para realizar el objetivo específico número 1 se realizará un cálculo de información cuántica basado en los siguientes pasos: primero se explicará cómo se puede entrelazar un estado que Alice le envía a Bob con un sistema adicional utilizando una compuerta C-NOT. Posteriormente se tendrá en cuenta el efecto del arreglo de doble decoherencia controlada en el sistema entrelazado. Por último, se calculará el grado de información que un espía puede obtener del sistema entrelazado.

Para realizar el objetivo específico número 2 se realizarán los siguientes pasos: Primero se utilizará un cristal no lineal BBO tipo II con el fin de generar pares de fotones. Una vez los pares de fotones son creados, un fotón del par se encargará de distribuir la clave entre Alice y Bob mientras que su pareja se encargará de anunciar la presencia de su pareja. Para ejecutar el protocolo BB84 se utilizarán dos láminas de onda que permiten controlar la polarización de la luz, un divisor de haz polarizado que permite discriminar entre luz polarizada verticalmente y horizontalmente, dos contadores de fotones individuales para detectar la presencia de fotones y un sistema electrónico para sincronizar todo el protocolo BB84.

7.**Cronograma**:

I. Actividad 1.1 Calculo de entrelazamiento utilizando la compuerta lógica C-NOT
Actividad 1.2 Calculo del efecto del arreglo de doble decoherencia controlada en la compuerta C-NOT.
Actividad 1.3 Calculo del grado de información que puede obtener el espía.

II. Actividad 2.1 Alineación de elementos ópticos para implementar el protocolo BB84.
Actividad 2.2: Sincronización del protocolo BB84 utilizando un sistema electrónico.
Actividad 2.3: Toma de datos (Obtención clave entre Alice y Bob).
Actividad 2.4: Análisis computacional de datos.

III. Actividad 3.1: Escritura y reporte de resultados.
Actividad 3.2: Presentación avances en el seminario de óptica cuántica.

Plan de Trabajo / Semanas	1	2	3	4	5	6	7	8
Objetivo específico 1: Desarrollo modelo teórico.								
Actividad 1.1: Explicación de entrelazamiento mediante la compuerta CNOT.			X					
Actividad 1.2: Efecto del arreglo de doble decoherencia en la compuerta C-NOT				X				
Actividad 1.3: Calculo de información mutua.					X			
Objetivo *específico* 2: Implementación experimental del protocolo BB84.								
Actividad 2.1: Alineación elementos ópticos	X	X						
Actividad 2.2: Sincronización protocolo BB84		X	X	X				
Actividad 2.3: Toma de datos				X	X			
Actividad 3.2: Análisis de datos						X	X	X
Socialización resultados								
Actividad 3.1: Escritura de reporte parciales y final.			X			X		X
Actividad 3.2: Socialización seminario óptica cuántica							X	

8. **Resultados**

8.1 Objetivo específico 1: Modelo teórico:

Se desarrolló un modelo teórico en el cual se utiliza el ataque SPTQQLG. Esta transformación está dada explícitamente por:

$$|H\rangle|T_{in}\rangle \rightarrow |H\rangle|T_o\rangle + |V\rangle|T_e\rangle$$

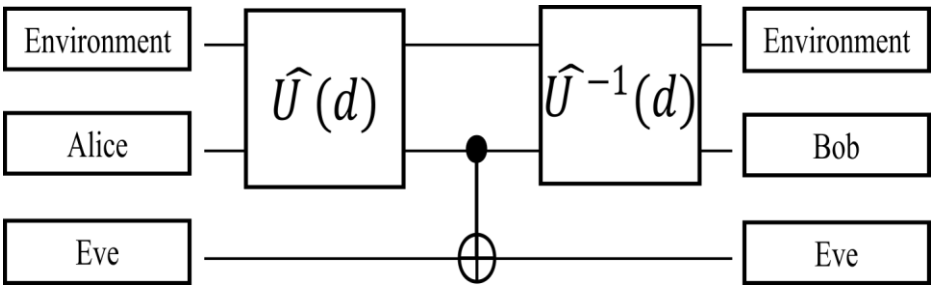
$$|V\rangle|T_{in}\rangle \rightarrow |V\rangle|T_1\rangle + |H\rangle|T_e\rangle$$

$$|D\rangle|T_{in}\rangle \rightarrow |D\rangle|T_o\rangle - |A\rangle|T_e\rangle$$

$$|A\rangle|T_{in}\rangle \rightarrow |A\rangle|T_1\rangle - |D\rangle|T_e\rangle$$

Figura1: Transformación dada por [3].

Utilizando el efecto de dos canales exoticamente desfasantes, se considero el siguiente esquema:



Con este esquema se llego a una nueva transformación bajo el ataque SPTQQLG, explícitamente la nueva transformación está dada por:

$$|\mathrm{D}\rangle|T_{in}\rangle \rightarrow |D\rangle|T_{0_{new}}\rangle + |A\rangle\,|T_{eD_{new}}\rangle$$

$$|A\rangle|T_{in}\rangle \rightarrow |A\rangle|T_{1_{new}}\rangle + |D\rangle|T_{eA_{new}}\rangle$$

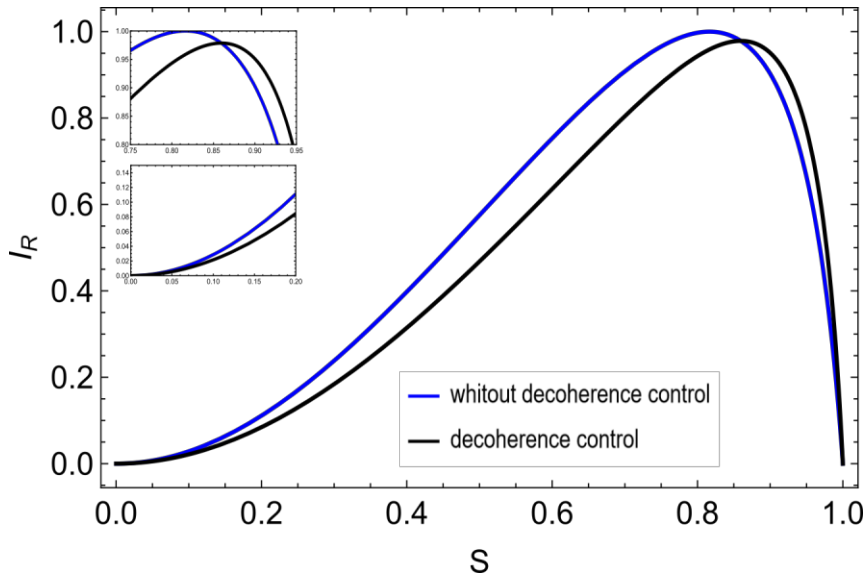
$$|H\rangle|T_{in}\rangle \rightarrow |H\rangle|T_{2new}\rangle + |V\rangle|T_{eHnew}\rangle$$

$$|V\rangle|T_{in}\rangle \rightarrow |V\rangle|T_{4new}\rangle + |H\rangle|T_{eVnew}\rangle$$

Transformación obtenida

Bajo esta transformación se evidencio que un espia tiene que distinguir entre dos estados adicionales para obtener información de la llave. Utilizando la nueva transformación se calculó la información mutua que un espía puede obtener utilizando el ataque SPTQQLG. A

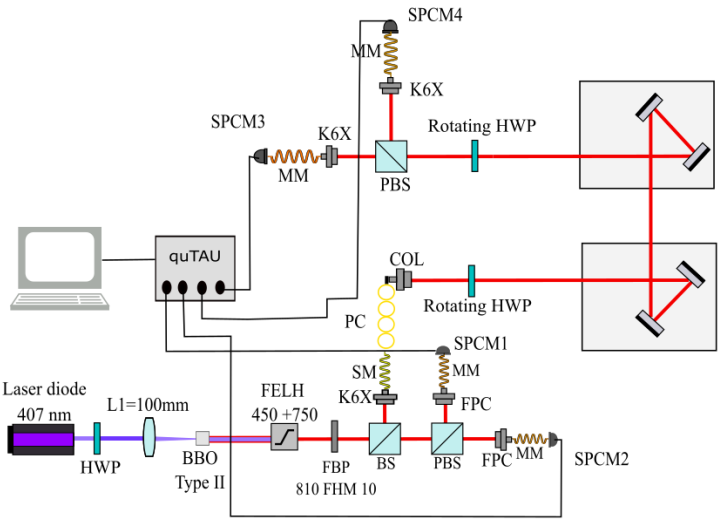
continuación, se presenta una comparación entre la gráfica de información mutua de Renyi en funcion de un parametro S al controlar y no controlar la decoherencia.



Se puede evidenciar que al controlar la decoherencia, se reduce la cantidad de información mutua que un espía puede obtener al utilizar el ataque SPTQQLG.

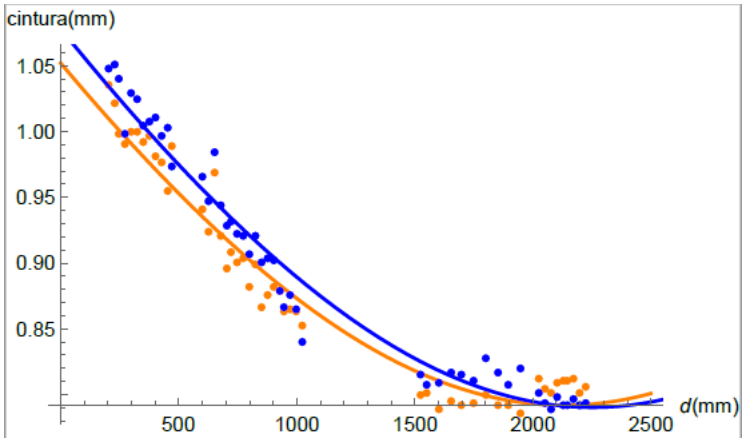
8.2 Objetivo específico 2: Implementación experimental del protocolo BB84.

Para implementar el protocolo BB84 se utilizo el siguiente montaje experimental:



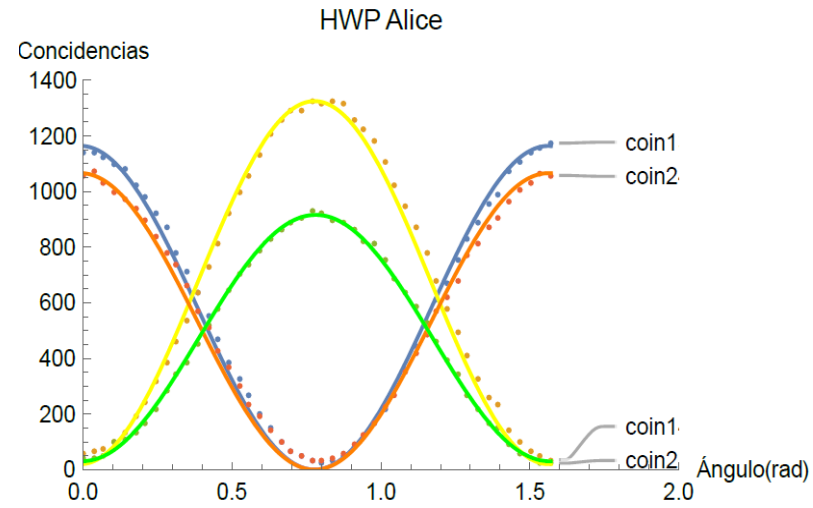
En este montaje experimental se utilizó un diodo láser a 407nm para bombear un cristal no lineal BBO tipo 2. En el cristal BBO se producen pares de fotones a 814nm. Posteriormente se utilizaron filtros espectrales FELH y filtros pasa banda 810+-10 nm para poder detectar los pares sin que el bombeo afecte en la medición. Un beam splitter (BS) se encarga de definir el camino por el cual los pares de fotones son enviados. Adicionalmente, se utiliza un polarizing beam splitter (PBS) para saber la polarización del fotón que se envía al protocolo BB84. En el protocolo BB84 un controlador de polarización (PM) se encarga de definir la polarización que sale del colimador (COL). Posteriormente se prepara un estado de polarización utilizando un una lamina de onda rotante (rotating HWP). Para medir el estado de polarización se emplea otra lamina de onda rotante y un PBS. Posteriormente la luz se detecta con detectores de fotones individuales SPCMs. Todas las señales obtenidas son almacenadas por un convertidor tiempo digital quTAU.

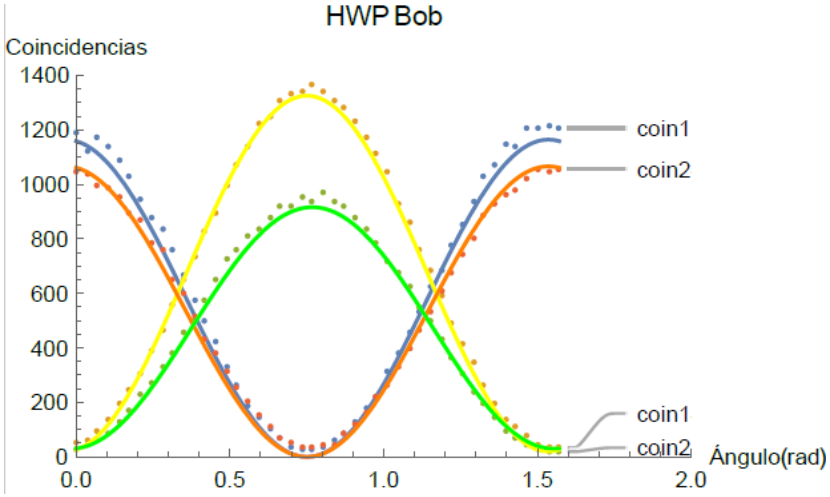
Antes de montar todos los elementos ópticos, fue necesario medir la cintura del haz para asegurar que el experimento se encuentre en una región en donde se pueda considerar la luz como una onda plana. La medida del ancho del haz fue la siguiente:



De la gráfica anterior se encontró que el rango en donde la onda se puede aproximar a una onda plana (rango de Raleigh) es de 2.4m. Por lo tanto, se puede considerar que el haz esta colimado durante todo el experimento

Al montar las laminas de onda, se caracterizaron moviendo un ángulo de a un grado y viendo cómo cambia la cantidad de coincidencias en todos los detectores respecto al ángulo. Con este procedimiento se encontró un respectivo cero. El resultado fue el siguiente:





De los ajustes utilizados, se encontró que las laminas de onda entre Alice y Bob se debían ajustar 2 y -2 grados respectivamente.

Por último, utilizando un programa de LabVIEW y analizando los datos computacionalmente se logro obtener el siguiente resultado:

N bits	Ventana de coincidencia	Error entre claves
500	0.5 nm	3.02%

8.3 Objetivo especifico 3:

El día 18 de junio del 2022 se presentó en el Journal Club de óptica cuántica el trabajo obtenido.

Daniel Sabogal
Nombre y firma del estudiante

Vo.Bo. del profesor asesor