Diseño de una fuente de estados señuelo para protocolos de distribución cuántica

Daniel R. Sabogal*
(Fecha: 27 de abril de 2021)

A la hora de enviar un mensaje secreto, la seguridad en la transmisión de información es un factor necesario para poder obtener confidencialidad entre dos usuarios. Una forma de obtener esta confidencialidad es utilizando la mecánica cuántica, en donde la idea general es utilizar las propiedades no deterministas de un fotón para obtener una clave aleatoria entre dos usuarios. Esta clave aleatoria permite cifrar un mensaje de tal manera que un usuario externo no pueda obtener información alguna. El primer protocolo para lograr la transmisión segura de llaves cuánticas es el BB84, en donde se codifica una cadena de bits relacionados con la clave en el estado de polarización de una secuencia de fotones individuales. La implementación experimental de este protocolo es realizada normalmente con pulsos con un número promedio de fotones menor a uno, lo que abre la posibilidad de enviar pulsos con un número de fotones mayor a uno ocasionalmente. Por lo tanto, esta implementación experimental tiene fallos que ponen en riesgo la seguridad de la llave debido a que los pulsos con un número de fotones mayor a uno pueden ser divididos utilizando un ataque comúnmente llamado *photon number splitting attack*. No obstante, el uso de una fuente de estados señuelo permite sobrepasar esta dificultad debido a que su uso en un protocolo de distribución cuántica permite detectar la presencia de un espía que divida fotones. En este artículo, se diseña una fuente de estados señuelo de alta simplicidad con pulsos de ancho temporal de $254\mu s$ y distribución del número de fotones con promedio de 0.44 y 0.75 fotones.

I. INTRODUCCIÓN

La criptografía tradicional basa su seguridad en la dificultad computacional de factorizar el producto de dos números primos. Sin embargo, la implementación de tecnologías cuánticas prometen alcanzar un poder computacional tal que se comprometa la seguridad en la criptografía tradicional. Por lo tanto, es necesario establecer métodos alternativos de criptografía que permitan obtener confidencialidad incondicionalmente. A diferencia de los métodos convencionales utilizados en la criptografía tradicional, la distribución cuántica de llaves permite una comunicación segura entre dos usuarios utilizando las leyes de la física cuántica [1].

El primer método cuántico propuesto para distribuir está llave es el protocolo BB84, en donde se plantea utilizar una serie de fotones individuales para distribuir una llave que cifra la información entre dos usuarios convencionalmente llamados Alice y Bob. En este protocolo, Alice elige aleatoriamente una base y un bit para preparar el estado de polarización de un fotón. Posteriormente, utiliza un canal cuántico para enviar el fotón preparado a Bob. 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 la base 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].

El protocolo BB84 fue implementado experimentalmente por primera vez en 1992 [3]. En esta implementación, pulsos de luz atenuada y polarizada fueron utilizados para distribuir la clave. Esto es debido a que la producción experimental de fotones individuales no se puede conseguir experimentalmente con facilidad [4]. Alternativamente, se puede utilizar pulsos coherentes con un número de promedio de fotones menor a uno, denominados normalmente como *weak coherent pulses*.

No obstante, esta implementación experimental abre la posibilidad a un ataque que divida fotones (PNS) y comprometa la confidencialidad de la llave [5]. Este ataque aprovecha el hecho de usar pulsos coherentes debiles, ya que como consecuencia de este hecho algunos pulsos tendrán más de un fotón. Por lo tanto, un espía puede dividir los pulsos que contengan mas de un de fotón y así obtener información de la clave.

Una solución al ataque PNS es utilizar el método de estados señuelo, en donde se mezclan algunos pulsos adicionales con un número promedio de fotones mayor al utilizado normalmente en el protocolo BB84 experimental. De esta manera, se puede establecer una condición de seguridad para obtener un ambiente seguro contra el ataque PNS [6].

El objetivo de este proyecto es diseñar e implementar una fuente de estados señuelo de alta simplicidad. Para este propósito, dos pulsos coherentes débiles con un número de fotones distintos serán diseñados e implementados. Explícitamente, cada pulso coherente tiene que tener una caracterización por medio de una distribución del número de fotones y ancho temporal. Posteriormente a la caracterización de cada uno de los pulsos, se mezclaran dichos pulsos utilizando elementos optomecánicos para crear una fuente de estados señuelo. Los

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

elementos a utilizar para la creación, caracterización y mezcla de los pulsos de luz están disponibles en el laboratorio de óptica cuántica de la universidad de los Andes.

II. MATERIALES Y MÉTODOS

La creación de un pulso coherente débil requiere de un ancho temporal y una distribución de probabilidad del número de fotones para lograr una caracterización definida. El ancho temporal del pulso necesita ser lo suficientemente corto temporalmente para no ser confundido con cuentas oscuras en los detectores. Los detectores usados son contadores de fotones individuales SPCM con un número máximo de cuentas oscuras de 250 conteos/s. Por otro lado, una distribución del número de fotones correctamente caracterizada por una estadística de Poisson es requerida para ejecutar el método de estados señuelo.

El ancho temporal del pulso de luz se diseña generando un pulso de corriente que alimente un diodo láser a 808 nm. De esta manera, el pulso de corriente utilizado mide $0.5\mu s$ temporalmente y tiene que tiene un magnitud de $2.5V$. Este pulso de voltaje es útil debido a que está en el rango de funcionamiento del diodo láser y está alejado temporalmente del rango en el cual las cuentas oscuras son significativas. Posteriormente, el ancho temporal del pulso de luz es monitoreado utilizando la intensidad en función del tiempo dada por un fotodiodo con resolución temporal de ns. Adicionalmente, la duración temporal del pulso es acotada con una señal electrónica con el propósito de obtener una distribución de probabilidad del número de fotones posteriormente. El montaje experimental para generar el pulso de luz y medir su ancho temporal se muestra en la figura 1.

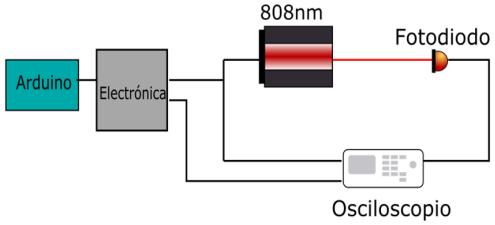

FIG. 1. Montaje experimental para medir el ancho temporal de un pulso láser alimentado por un pulso de corriente. En este montaje, el Arduino se encarga de generar un pulso de voltaje recibido por un sistema electrónico. El pulso de voltaje genera dos pulsos de corriente con distinto ancho temporal: uno para encender el diodo y otro para acotar el ancho temporal del pulso de luz. El pulso de luz será recibido por el fotodiodo con el fin de visualizar todas las señales utilizando un osciloscopio.

Una vez obtenido el ancho temporal del pulso coherente de luz, es necesario determinar el número de fotones que contiene el pulso. Con este propósito, se abre una ventana temporal de detección con la señal que se encarga acotar electrónicamente la duración del pulso. Esta señal se utiliza para discriminar las detecciones de las cuentas oscuras y así contar el número de fotones que llegan al detector en el intervalo de tiempo en el que el pulso tiene intensidad. Utilizando el SPCM y un convertidor tiempo digital se puede obtener una estampa de tiempo que permita determinar la hora de llegada de cada fotón al detector. Esto se logra utilizando el montaje experimental propuesto en la figura 2, en donde se puede contar el número de fotones que tiene un pulso repetidas veces y obtener la distribución de probabilidad del número de fotones, denominada normalmente como P_n.

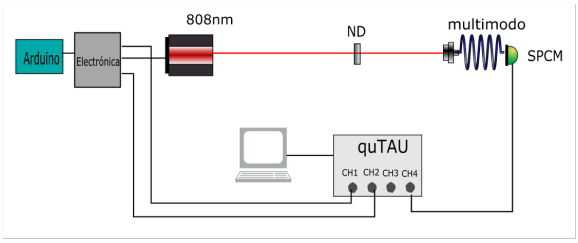

FIG. 2. Medición de P_n. En este montaje, el pulso de luz es atenuado mediante distintos filtros de densidad neutra (ND). Posteriormente, estos pulsos llegan a una fibra óptica que conecta con el detector de fotones individuales (SPCM). Este detector convierte la llegada de un fotón en un pulso TTL con un tiempo muerto de $50ns$. El pulso TTL va al convertidor tiempo digital (quTAU) que se encarga de registrar el tiempo de llegada de cada de cada pulso TTL. Para analizar específicamente los fotones que llegan en el intervalo te tiempo especifico, se registra el flanco de subida y bajada de la señal electrónica que acota temporalmente el pulso de luz.

1. *Consideraciones éticas*

El proyecto tiene un carácter experimental, por lo cual, se citarán todas las fuentes consultadas para el estudio de los temas involucrados. Adicionalmente, el desarrollo del proyecto no supone ningún conflicto de intereses y no está relacionado con actividades ni poblaciones humanas. Por lo tanto, no se considera que el proyecto pase al comité de ética de la Facultad de Ciencias.

III. RESULTADOS Y DISCUSIÓN

Utilizando el montaje experimental para determinar el ancho temporal del pulso de luz se puede obtener señales visualizadas por el osciloscopio. En este caso, las gráfica a y b de la figura 3 muestran las escalas temporales de μs y 100 μs respectivamente. En la escala de μs, una señal de 2.5 V y ancho temporal de 0.5 μs es mostrada en rojo en la gráfica a. Por otro lado, la señal obtenida por el fotodiodo se muestra en azul en la misma gráfica. Es posible ver como el pulso TTL enciende el diodo láser

en 0.5 μs. Sin embargo, la intensidad de luz producida por el diodo láser no decrece inmediatamente cuando el pulso TTl termina. En otras palabras, utilizando un pulso TTL se puede controlar el tiempo de subida en la intensidad de luz pero no su tiempo de bajada.

Para medir el tiempo en el cual el pulso de luz tiene intensidad se necesita hacer uso de la escala de 100 μs. En esta segunda escala, la señal de fotodiodo se muestra en rojo y la señal encargada de acotar la duración del pulso de luz es mostrada en azul. Se puede ver que la intensidad de luz decrece totalmente en 254μs. Este hecho revela el comportamiento de respuesta del diodo bajo la acción de un pulso de 0.5 μs. Este tiempo de respuesta muestra una limitación experimental en donde el mejor régimen temporal para evadir las cuentas oscuras del detector es de 254 μs. Por otro lado, la el propósito de la señal delimitante es determinar la ventana temporal la cual la intensidad de luz del pulso no es cero. Está señal será de ayuda a la hora de medir la distribución de probabilidad del número de fotones P_n.

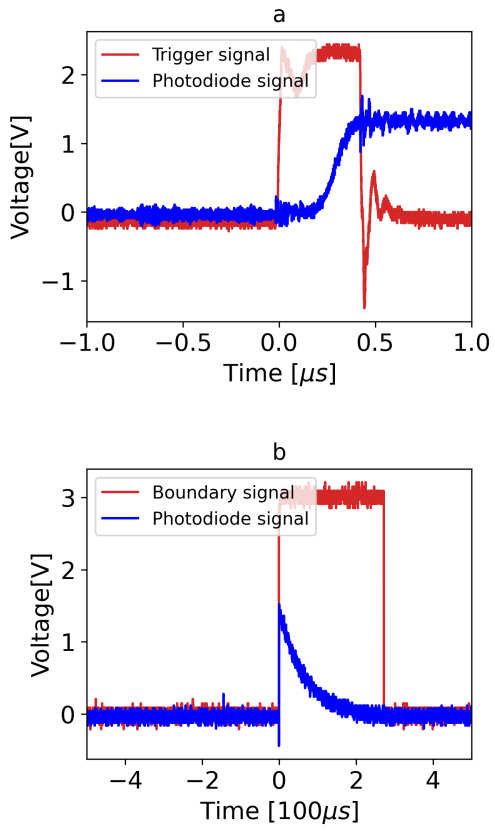

FIG. 3. Tiempo de respuesta del diodo láser en distintas escalas de tiempo.

El primer requerimiento para crear una fuente de estados señuelo se cumple si se asume linealidad en la tasa de cuentas oscuras del detecteor. Bajo esta supocición, existen 0.0635 cuentas oscuras en 254 μs micro segundos. Por lo tanto, es resanobale considerar que no exiten cuentas oscuras en el intervalo temporal en donde el pulso tiene intensidad.

Usando el montaje experimental de la figura 2, se puede enviar repetidamente pulsos de luz para una configuración dada de filtros de densidad neutra. En cada pulso enviado un número distinto de fotones pueden llegar al detector. Contando el número de fotones en todos los pulsos la distribución de probabilidad del número de fotones P_n puede ser construida. Como la distribución de probabilidad P_n es caracterizada por un número medio de fotones μ, una curva que relaciona el número de fotones promedio y la combinación de filtros de densidad neutra se muestra en la figura 4.

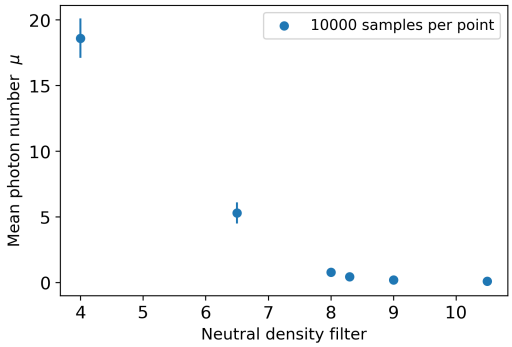

FIG. 4. Caracterización del número promedio de fotones en el pulso según la combinación de filtros de densidad neutra utilizados.

Para obtener pulsos coherente débiles se necesita una combinación de filtros de densidad neutra en la cual el número de fotones promedio es menor a uno. Como la figura 4 muestra, se necesita utilizar filtros con una densidad óptica mayor a ocho. Por otro lado, para obtener pulsos señuelo y pulsos que distribuyen la clave se necesita dos pulsos coherentes débiles con un número promedio de fotones distinto. Por lo tanto, se escogió los una combinación de filtros de densidad óptica de ND = 8.3 y ND = 8. En está combinación de filtros la distribuciones de probabilidad del numero de fotones correspondientes se muestran en la figura 5.

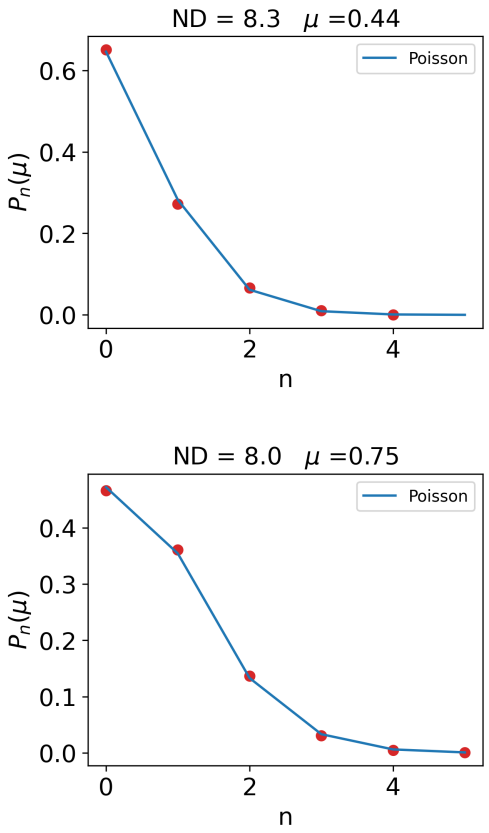

FIG. 5. Distribución de probabilidad del número de fotones para los pulsos señuelo y los pulsos que distribuyen la clave.

Las distribuciones de probabilidad $P_n(\mu)$ obtenidas en la figura 5 son adecuadas para ejecutar el método de estados señuelo por dos razones principalmente. La primera razón que permite utilizar estas distribuciones es que se sigue una estadística de Poisson como lo es requerido en un estado coherente débil. El segundo hecho que justifica esta elección es que el número medio de fotones utilizado en ambos pulsos es lo suficientemente parecido para que un espía no logre diferenciarlo en el ataque PNS.

Específicamente, la distribución de probabilidad con número medio de fotones $\mu = 0.44$ es usada para los pulsos que distribuyen la clave y la distribución de probabilidad con media $\mu = 0.75$ para los pulsos señuelo. Mezclando aleatoriamente los pulsos que distribuyen la clave con los pulsos señuelo se logra construir en su totalidad una fuente de estados señuelo. Una forma de mezclar estos pulsos es usando un motor para cambiar de forma aleatoria entre las dos combinaciones de filtros de densidad neutra disponibles. Por lo tanto, utilizando un código que genere dos posiciones del motor aleatoriamente (RNG), la fuente de estados señuelo se muestra operacional mente en la figura 6.

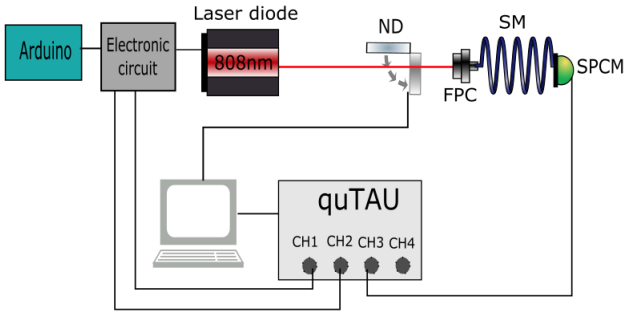

FIG. 6. Fuente de estados señuelo

IV. CONCLUSIONES

Se diseñó un pulso de luz generado por el diodo láser que permite obtener una detección sin ruido ocasionado por las cuentas oscuras. Este pulso tiene un ancho temporal de $254\mu s$, en donde se obtiene menos de una cuenta oscura. Contando el número de fotones que llegan al detector en el intervalo en el cual el pulso tiene intensidad, una distribución de probabilidad en función de los filtros de densidad neutra fue medida. Utilizando esta caracterización, se estableció la media del número del fotones para los pulsos encargados de distribuir la clave y los pulsos señuelo. Mezclando estos pulsos utilizando un motor se construyo una fuente de estados señuelo de alta simplicidad para protocolos de distribución cuántica de llaves. Esta fuente es de gran utilidad para blindar protocolos como el BB84 ya que permite la ejecución del método de estados señuelo.

[1] S. Singh, *The Code Book: The Science of Secrecy from Ancient Egypt to Quantum Cryptography* (Anchor Books, 2000).
[2] C. H. Bennett and G. Brassard, Theoretical Computer Science **560**, 7 (2014), theoretical Aspects of Quantum Cryptography – celebrating 30 years of BB84.
[3] C. H. Bennett, F. Bessette, G. Brassard, L. Salvail, and J. Smolin, Journal of cryptology **5**, 3 (1992).
[4] M. D. Eisaman, J. Fan, A. Migdall, and S. V. Polyakov, Review of Scientific Instruments **82**, 071101 (2011), https://doi.org/10.1063/1.3610677.
[5] N. Lütkenhaus and M. Jahma, New Journal of Physics **4**, 44 (2002).
[6] W.-Y. Hwang, Phys. Rev. Lett. **91**, 057901 (2003).