Hacia la distribución cuántica de claves en espacio libre a alta velocidad

M. J. García-Martínez *, D. Soto, N. Denisenko y V. Fernández

Instituto de Física Aplicada, Consejo Superior de Investigaciones Científicas, Serrano 144, 28006 Madrid

Resumen

En el presente trabajo se describe el diseño e implementación práctica de un sistema de distribución cuántica de claves (del inglés, Quantum Key Distribution, QKD), en espacio libre, a alta velocidad y en entorno urbano.

1. Introducción

La distribución cuántica de claves [1] utiliza propiedades físicas de partículas individuales, como la polarización o la fase de fotones, para intercambiar una clave criptográfica de manera totalmente segura entre dos partes, comúnmente denominadas Alice y Bob. Emisor y receptor utilizan un canal cuántico (fibra óptica o espacio libre) por el que transmiten los fotones, y un canal clásico no necesariamente seguro (línea de teléfono, conexión Ethernet, etc.) para destilar la clave criptográfica final. La información está codificada en propiedades cuánticas que al ser observadas son inevitablemente modificadas debido al Principio de Incertidumbre de Heisenberg y obligan al intruso a dejar una huella que delatará su presencia.

2. Descripción del sistema experimental

El sistema que estamos construyendo implementará el protocolo B92 [2], que utiliza dos estados de polarización no ortogonales para codificar los estados lógicos binarios uno y cero. En la figura 1 podemos ver un diagrama del emisor. Dos diodos láser tipo VCSEL (Vertical Cavity Surface Emitting Laser), que emiten a una longitud de onda de 850 nm a través de dos polarizadores de alta extinción, serán los encargados de generar los estados necesarios para implementar el protocolo B92. Dos drivers a alta velocidad conectados a un generador de pulsos a frecuencias reloj de GHz modularán los dos VCSELs. Los estados uno y cero serán después combinados utilizando un cubo beamsplitter y dirigidos hacia dos lentes que expandirán el haz para ser transmitido a larga distancia. Dos espejos de alta reflectividad guiarán el haz sobre una plataforma cuadrada que a su vez se montará sobre un sistema gimbal de alta precisión que proporcionará los movimientos de ascensión recta y declinación necesarios para alinear la estación del emisor con el receptor.

El receptor estará situado a 3 km del emisor y recibirá el haz mediante un telescopio Cassegrain de 2.5 m de distancia focal y capacidad de apuntamiento fino. La óptica de Bob ha sido diseñada con monturas ligeras acopladas directamente a la parte posterior del telescopio, tal y como se muestra en la figura 2. Mediante un analizador de intervalos de tiempo se miden los tiempos de llegada de los fotones que alcanzan el receptor y éstos serán utilizados para el post-procesamiento de la señal recibida y para calcular el error cuántico de la clave.

El problema de la sincronización entre los dos relojes remotos de emisor y receptor será resuelto mediante el envío de una señal de sincronizado a intervalos regulares durante todo el protocolo de QKD. Dicha señal consiste en un pulso periódico, no atenuado y a una longitud de onda diferente a la utilizada para enviar los estados cuánticos que cifran la clave.

* *e-mail:* mariajose.garcia@iec.csic.es

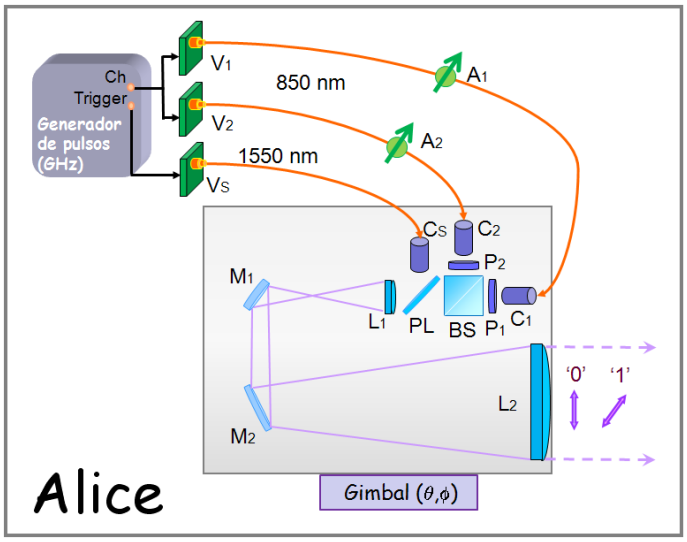

Figura 1: V_1 y V_2 son dos diodos láser tipo VCSEL emitiendo a 850nm; A_1 y A_2 son dos atenuadores acoplados en fibra óptica; C_1, C_2 y C_S son tres colimadores; P_1 y P_2 son dos polarizadores de alta extinción; BS es un cubo divisor de haz; L_1 y L_2 son dos lentes para expandir el haz; y M_1 y M_2 son espejos de alta reflectividad. V_S es un tercer VCSEL a 1550nm que se utiliza como longitud de onda para el sincronizado temporal entre emisor y receptor, y se combinará con 850nm a través de una lámina tipo pellicle (PL) de amplio espectro.

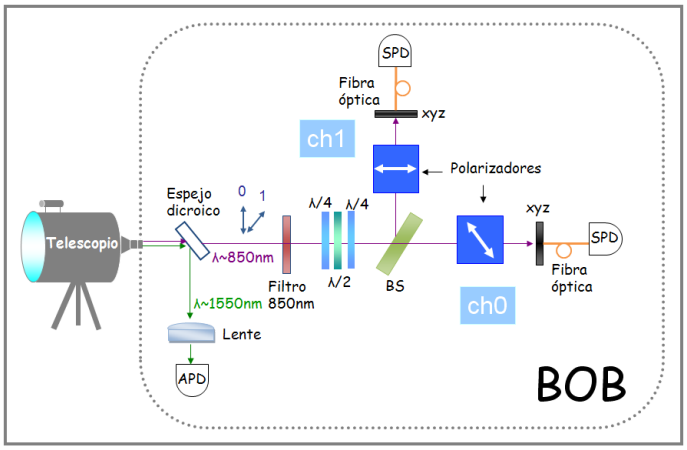

Figura 2: Se utilizan dos longitudes de onda diferentes: $\lambda \sim 850$ nm para transmitir la clave y $\lambda \sim 1550$ nm para sincronizar emisor y receptor. BS es un divisor de haz 50-50; SPD son detectores de fotones individuales; y APD es un fotodiodo de avalancha.

Agradecimientos: Este trabajo ha sido financiado parcialmente por el Ministerio de Educación y Ciencia, proyectos MTM2008-02194 y 200950I073, y el CDTI, Ministerio de Industria, Turismo y Comercio, en colaboración con Telefónica I+D, proyecto SEGUR@ con referencia CENIT-2007 2004.

Bibliografía

[1] C. H. Bennett, G. Brassard, "Quantum cryptography: public key distribution and coin tossing", *Proc. IEEE Int. Conf. Comput., Syst. Signal Process.*, vol. 175, Bangalore, India, (1985).

[2] C. H. Bennet, "Quantum cryptography using any two nonorthogonal states", Physical Review Letters, **68**, p. 3121 (1992).