SANTANDER, 19-23 DE SEPTIEMBRE DE 2011

XXXIII

Reunión Bienal de la Real Sociedad Española de Física

tomo IV

21º Encuentro Ibérico para la Enseñanza de la Física

Astrofísica
Física de Plasmas
Física de la Materia Blanda
Física Médica
Información Cuántica

PUbliCan Ediciones

Reunión bienal de la
Sociedad Española
de Física

21º Encuentro Ibérico para la Enseñanza de la Física

M.ª Teresa Barriuso Pérez (Editora)

XXXIII Reunión Bienal
de la
Real Sociedad Española de Física

21.er Encuentro Ibérico para la Enseñanza de la Física

Santander, 19-23 de septiembre de 2011

Resúmenes de las Comunicaciones

[Tomo IV]
Astrofísica, Física de Plasmas
Física de la Materia Blanda
Física Médica, Información Cuántica

PUbliCan
Ediciones
Universidad de Cantabria

Real Sociedad Española de Física. Reunión Bienal (33ª : 2011 : Santander)
XXXIII Reunión Bienal de la Real Sociedad Española de Física ; 21er Encuentro Ibérico para la Enseñanza de la Física. -- Santander : PUbliCan, Ediciones de la Universidad de Cantabria, 2011.

Reuniones celebradas en el Palacio de la Magdalena de Santander del 19 al 23 de septiembre de 2011.

ISBN 978-84-86116-40-8 (O.C.)
ISBN 978-84-86116-41-5 (T.1)
ISBN 978-84-86116-42-2 (T.2)
ISBN 978-84-86116-43-9 (T.3)
ISBN 978-84-86116-44-6 (T.4)

Física-- Congresos.
Física-- Didáctica-- Congresos.
Encuentro Ibérico para la Enseñanza de la Física (21º : 2011 : Santander)

53(063)
53:37.02(063)

ISBN: 978-84-86116-40-8 (obra completa)
ISBN: 978-84-86116-44-6
DL: S. 1.171-2011

Impreso de España - *Printed in Spain*

Imprenta KADMOS
Salamanca

Distribución cuántica de claves en redes de acceso WDM-PON

A. Ciurana[1], N. Walenta[2], J. Martínez-Mateo[1], D. Elkouss[1], M. Soto[2] y V. Martin[1]

[1] DLSIIS, Grupo de Investigación en Información y Computación Cuánticas, Facultad de Informática, Universidad Politécnica de Madrid, Campus de Montegancedo, 28860 Boadilla del Monte (Madrid); vicente@fi.upm.es.
[2] Group of Applied Physics, University of Geneva, 1211 Geneva, Switzerland; nino.walenta@unige.ch
[3] Security in Networks and Services, Telefónica Investigación y Desarrollo. Distrito C, Ronda de la Comunicación s/n, 228050, Madrid; soto@tid.es

La distribución cuántica de claves (QKD en adelante) es una aplicación de la información cuántica lo suficiente madura como para ofrecerse de forma comercial. Los equipos QKD actuales funcionan mediante enlaces punto a punto, de modo que no resulta posible hacer conexiones arbitrarias entre ellos. Esta es una limitación importante que hace muy difícil su adopción generalizada, para ello es necesaria su integración en una red. Hasta el momento se han realizado prototipos de red que son básicamente una colección de conexiones punto a punto usando una red de fibra óptica separada de las redes de telecomunicaciones comerciales lo que, de nuevo, implica un elevado coste y, con ello, pocos usuarios potenciales. Reducir la dependencia de QKD de estas conexiones *ad hoc* y la capacidad de reconfigurar el canal cuántico para conectar distintos usuarios, es una necesidad para que deje de ser una tecnología nicho. Las redes de telecomunicaciones que se están instalando en la actualidad son ópticas y de tipo pasivo, siendo capaces de establecer un enlace transparente entre dos puntos cualesquiera a través del que podemos crear un canal cuántico. QKD en este tipo de redes ha sido estudiado en el pasado [1], estableciendo las limitaciones de algunas de las tecnologías utilizadas. En un esquema canónico de estas redes (considerando tan sólo las de área metropolitana por las limitaciones en pérdidas/distancia de QKD), podemos diferenciar dos tipos: (i) las redes de acceso, que dan servicio a los usuarios finales y (ii) las centrales, encargadas de conectar las redes de acceso entre ellas y con las de largo alcance.

Hasta ahora se han estudiado redes de acceso en tecnología GPON (*Gigabit Passive Optical Network*) donde una fibra compartida conecta la red central con un divisor de donde parten fibras hasta los usuarios. En este tipo de red el factor limitante es el divisor, ya que introduce pérdidas que se incrementan con el número de usuarios, pudiendo llegar a 21 dB para 128 usuarios. La red central estudiada ha sido en tecnología CWDM (*Coarse Wavelength Division Multiplexing*), donde hasta 16 longitudes de onda comparten una sola fibra. Los factores limitantes aquí eran las absorciones por los dispositivos de encaminamiento y la potencia de los canales clásicos [1, 2]. Si se quiere compartir la red central entre canales cuánticos y clásicos hay que limitar el número de estos, lo que de nuevo implica un coste elevado. Un problema adicional viene dado por que la conexión entre la red de acceso y central requeriría con este diseño un cambio de longitud de onda.

Una manera de evitar estos problemas es cambiar a una tecnología de redes que está empezando ya a implantarse. La base es el direccionamiento mediante longitud de onda, de modo que se pueden conectar dos puntos mediante su selección. En este caso, se reserva una fibra óptica en la red central para la transmisión, en multiplexación por longitud de onda, de una gran cantidad de canales cuánticos, disminuyendo así el

coste por conexión QKD. En la red de acceso utilizamos WDM-PON, que también usa direccionamiento por longitud de onda, lo que permitiría atender tantos usuarios simultáneos como canales en la red central. Además WDM-PON evita el problema del aumento de pérdidas a medida que aumenta el número de usuarios utilizando un AWG (*Arrayed Waveguide Grating*), que introduce unos 5 dB de manera casi independiente del número de usuarios, para separar las distintas longitudes de onda en la fibra compartida y enviarlas hacia las fibras que conectan los usuarios finales en la red de acceso. Con esta estructura se pueden reutilizar dispositivos y fibra instalada en la red de telecomunicaciones normal para crear una red óptica conmutada compartida entre una gran cantidad de canales cuánticos.

Para comenzar a caracterizar esta red, hemos realizado diversas pruebas en el laboratorio con equipos comerciales de WDM-PON. Hemos utilizado un AWG de 32 canales con un mallado de 100GHz (0.8 nm) y equipos QKD (modelo Clavis 3000 de id Quantique modificado para hacerlo sintonizable a varias longitudes de onda). Los resultados se presentan en la Figura 1, donde mostramos la tasa de clave final obtenida y el Quantum Bit Error Rate (QBER) en función de la atenuación. Nuestro sistema QKD funcionando a 5 MHz, nos permite compartir clave a una tasa de hasta 100 bits/sec a 30 Km de distancia, más que suficiente en redes de acceso. A mayor distancia, el QBER aumenta por encima de los valores que permiten destilar clave segura del intercambio cuántico. En contraste, en una red GPON con 32 canales, estos equipos no serían capaces de intercambiar clave.

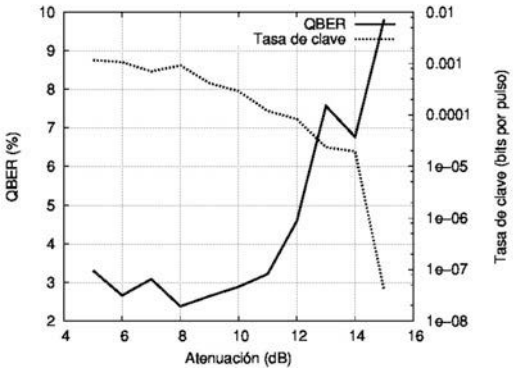

Figura 1. Tasa de clave y tasa de error de la clave compartida (QBER) en función de la atenuación del canal.

En esta comunicación se plantea el estudio de redes para QKD donde sólo coexisten canales cuánticos compartiendo la misma fibra. Se han estudiado las redes de acceso basadas en la tecnología WDM-PON y DWDM (*Dense WDM*) en red central, lo que permitiría el direccionamiento mediante longitud de onda y abaratar la tecnología al compartir un solo sustrato físico, idéntico al usado en redes de telecomunicación, entre multitud de canales cuánticos. Además, hemos comprobado su funcionamiento de forma experimental en el laboratorio con equipos comerciales. En un futuro habrá que estudiar el comportamiento de los distintos componentes de la red y la compatibilidad de los distintos dispositivos QKD para integrarse dentro de un canal compartido en la misma red cuántica.

Referencias

1. D. Lancho, J. Martínez, D. Elkouss, M. Soto, and V. Martín (2009). QKD in Standard Optical Telecommunications Networks. International Conference on Quantum Communication and Quantum Networking, Naples (Italy), Vol. 36, pp. 142-149. arXiv:1006.1858v2.
2. P. Eraerds, N. Walenta, M. Legre, N. Gisin and H. Zbinden (2010). Quantum key distribution and 1 Gbps data encryption over a single fibre. New Journal of Physics, 2010, Vol. 12, pp. 063-027