Type: Original Research Paper / Tipo: Artículo Original de Investigación
Special Section: VIII Spanish Meeting on Optoelectronics / Sección Especial: VIII Reunión Española de Optoelectrónica

Amplification of the bit rate for quantum key distribution based on cryptographic hash functions

Amplificación de la tasa de bit para distribución de clave cuántica basada en funciones hash criptográficas

Juan Pradilla, José Mora(*), José Capmany

Grupo de Comunicaciones Ópticas y Cuánticas (GCOC), Instituto de Telecomunicaciones y Aplicaciones Multimedia (iTEAM), Universitat Politècnica de València, C/ Camino de Vera s/n 46022, Valencia, Spain.

(*) Email: jmalmer@upv.es

Received / Recibido: 20/09/2013. Revised / Revisado: 29/10/2013. Accepted / Aceptado: 30/10/2013.
DOI: http://dx.doi.org/10.7149/OPA.46.4.337

ABSTRACT:

The security is a research area in a continuous evolving field and represents one of the most important perspective future lines in telecommunications. This work is focused on new techniques and methods employing the properties of quantum physics with the aim of obtaining unconditional security. Currently, these techniques and methods lack a key rate close to the current transmission rate. In order to improve the quantum key transmission rate, this article proposes the use of cryptographic hash functions used in the privacy amplification layer to expand the bit rate relying on the properties of these functions.

Key words: Quantum Key Distribution, Hash Functions, BB84 Protocol, Privacy Amplification.

RESUMEN:

La seguridad es un campo de trabajo en continuo desarrollo y representa una de las líneas con mayor perspectiva de futuro dentro de las telecomunicaciones. Este trabajo se centra en las nuevas técnicas y procedimientos que emplean las propiedades de la física cuántica con el objetivo de obtener seguridad incondicional. Actualmente, estos sistemas de distribución de clave carecen de una tasa de clave equiparable con las tasas de transmisión actuales. Para lograr mejorar la tasa de transmisión de clave cuántica, se propone en este artículo el uso de las funciones hash criptográficas usadas en la capa de amplificación de privacidad para lograr ampliar la tasa binaria apoyándose en las propiedades de estas funciones.

Palabras clave: Distribución de Clave Cuántica, Funciones Hash, Protocolo BB84, Amplificación de Privacidad.

REFERENCES AND LINKS / REFERENCIAS Y ENLACES

[1]. C. H. Bennett, G. Brassard, "Quantum cryptography: Public key distribution and coin tossing", *Proc. IEEE International Conference on Computers, Systems and Signal Processing*, IEEE Press, pp. 175-179 (1984).

[2]. C. H. Bennett, "Quantum cryptography using any two nonorthogonal states", *Phys. Rev. Lett.* **68**, 3121-3124 (1992). DOI

[3]. V. Scarani, A. Acín, G. Ribordy, N. Gisin, "Quantum cryptography protocols robust against photon number splitting attacks for weak laser pulse implementations", *Phys. Rev. Lett*. **92**, 579011-579014 (2004). DOI

[4]. V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, N. Lütkenhaus, M. Peev, "The security of practical quantum key distribution", *Rev. Mod. Phys.* **81**, 1301-1310 (2009). DOI

[5]. A. Ruiz-Alba, D. Calvo, V. Garcia-Muñoz, A. Martinez, W. Amaya, J. G. Rozo, J. Mora, J. Capmany, "Practical quantum key distribution based on the BB84 protocol", *Waves* **3**, 4-14 (2011).

[6]. X. Tang, L. Ma, A. Mink, A. Nakassis, H. Xu,B. Hershman, J. C. Bienfang, D. Su, R.F.Boisvert, C.W. Clark, C. J. Williams, "Experimental study of high speed polarization-coding quantum key distribution with sifted-key rates over Mbit/s", *Opt. Express* **14**, 2062-2070 (2006). DOI

[7]. Y. Liu, T. Y. Chen, J. Wang, W. Q. Cai, L. K Chen, J. H. Wang, S. B. Liu, H. Liang, L. Yang, C.-Z Peng, Z.-B. Chen, J.-W. Pan, "Decoy-state quantum key distribution with polarized photons over 200 km", *Opt. Express* **18**, 8587-8594 (2010). DOI

[8]. A. R. Dixon, Z. L. Yuan, J. F. Dynes, A. W. Sharpe, A. J. Shields, "Gigahertz decoy quantum key distribution with 1 Mbit/s secure key rate", *Opt. Express* **16**, 18790-18979 (2008). DOI

[9]. G. Brassard, L. Salvail, "Secret-key reconciliation by public discussion", *Lect. Notes Computer Sci.* **765**, 411-423 (1994). DOI

[10]. W. Buttler, J. Torgerson, G. Nickel, C. Donahue, C. Peterson, "Fast, efficient error reconciliation for quantum cryptography", *Phys. Rev. A* **67**, 523031-523038 (2003). DOI

[11]. C. Elliot, A. Colvin, D. Pearson, O. Pikalo, J. Schlafer, H. Yeh, "Current status of the DARPA quantum network", *Proc. SPIE* **5815**, 138-149 (2005). DOI

[12]. D. Pearson, "Building a QKD Network out of theories and devices", *Building the DARPA Quantum Network*, BBN Technologies (2005).

[13]. W. Stallings, *Cryptography and Network Security: Principles and Practice*, 5th Ed., Pearson (2011).

[14]. S. Gueron, S. Johnson, J. Walker, "SHA-512/256", *IACR Cryptology ePrint Archive*, pp. 548-548 (2010).

[15]. D. Elkouss, A. Leverrier, R. Alleaume, J. J. Boutros, "Efficient reconciliation protocol for discrete-variable quantum key distribution", *Proc. IEEE International Symposium on Information Theory*, art. no. 5205475, pp. 1879-1883 (2009).

[16]. M. Bloch, A. Thangaraj, S. W. McLaughlin, J.-M. Merolla, "LDPC-based Gaussian key reconciliation", *2006 IEEE Information Theory Workshop - ITW 2006*, art. no. 1633793 , pp. 116-120 (2006).

1. Introducción

En la actualidad, la seguridad en las comunicaciones se perfila como uno de los temas de mayor desarrollo y relevancia en el mundo. Aplicaciones como las comunicaciones en centrales nucleares, las operaciones interbancarias y las redes de organismos de inteligencia militar requieren que se garantice la máxima seguridad para su operación diaria.

Para dar respuesta a estos requerimientos crecientes de seguridad han comenzado a emerger protocolos para generación y distribución de claves (conocidos como *Quantum Key Distribution*, QKD) que utilizan los principios de la física cuántica con el objetivo de garantizar una seguridad incondicional. Ejemplos de estos protocolos son: el BB84, que fue propuesto por Bennett y Brassard en la *International Conference on Computers, Systems and Signal* celebrada en Los Álamos, California, en el año 1984 [1]; el B92, que es una modificación al protocolo BB84 propuesta en 1992 por Bennett [2], la cual no brinda grandes ventajas sobre su predecesor, por lo que su interés no va más allá del académico; y el SARG04, propuesto en el año 2004 por Scarani, Acín, Ribordy y Gisin [3], como una alternativa al protocolo BB84, para evitar el ataque por división del número de fotones, PNS.

Todos estos protocolos utilizan varios principios de la física cuántica. En primer lugar, el principio de incertidumbre de Heisenberg que asegura que es imposible determinar, con precisión absoluta y de forma simultánea, el valor de dos magnitudes conjugadas de un sistema elemental. Por otro lado, el teorema de la no clonación propuesto por Dieks, Wootters y Zurek, asegura que no se puede clonar de forma exacta un estado cuántico desconocido manteniendo el original sin modificaciones, y finalmente que las correlaciones cuánticas obtenidas de medidas separadas de estados entrelazados violan la desigualdad de Bell y por tanto impiden crear un acuerdo antes de la medida [4]. El hecho de que la seguridad esté basada en los principios de la física sugiere la posibilidad de seguridad incondicional que permite que un sistema sea seguro sin ninguna restricción en las capacidades que tenga un atacante, salvo los límites fijados por la física [1].

Sin embargo, todos estos protocolos presentan una carencia importante: sus tasas binarias (del orden de los pocos Mbps a

distancias de 100 km) mediante el canal cuántico son bajas comparadas con las tasas de binarias mediante canal clásico (del orden de Gbps o Tbps a distancias de 100 km) [5-8]. Esto ha llevado a centrar la atención de varios investigadores con el fin aumentar las tasas binarias de los protocolos de distribución de clave cuántica (QKD) de forma que se equipare la generación y distribución de claves con la generación y distribución de información, logrando así, sistemas de comunicaciones más rápido y seguros.

El presente artículo explora el funcionamiento del protocolo BB84 y propone una técnica, para aumentar la tasa binaria de los sistemas de distribución de clave cuántica. Inicialmente presenta el funcionamiento del protocolo BB84. Posteriormente, muestra una técnica que usa las propiedades de las funciones hash criptográficas para el aumento de la tasa binaria. Finalmente, muestra las conclusiones del trabajo realizado utilizando esta técnica.

2. Funcionamiento del protocolo BB84

El protocolo BB84 para la distribución de clave cuántica se modela como la interacción de tres actores: un emisor (Alice), un receptor (Bob) y un atacante (Eve). Para comunicarse Alice y Bob emplean dos canales de comunicación: uno cuántico, que les permitirá compartir señales cuánticas, y un canal clásico, en el cual pueden enviar mensajes de forma clásica [4].

El canal clásico necesita ser autenticado, lo que implica que Alice y Bob deben identificarse entre ellos directamente o a través de un tercero (entidad certificadora). Eve, por su parte, puede escuchar la conversación clásica, pero no participar en ella. Sin embargo, el canal cuántico está abierto a cualquier manipulación por parte de Eve. De forma que, la tarea de Alice y Bob es garantizar la seguridad, teniendo en cuenta el libre acceso de Eve para manipular el canal cuántico y escuchar la transmisión del canal clásico. La Fig. 1 muestra un esquema general de esta técnica.

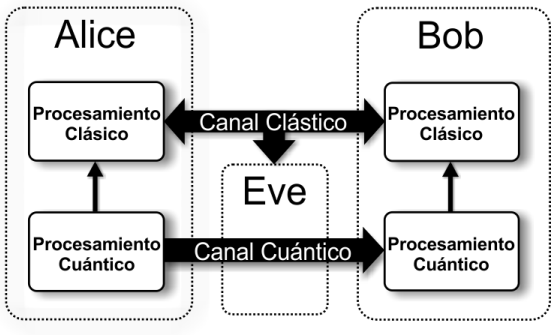

Fig. 1. Modelo de un protocolo de QKD.

Sobre este modelo, el protocolo BB84 se puede dividir en dos partes, según el canal que este empleando: cuántica y clásica. Estas dos partes se presentan en profundidad a continuación.

2. a. Intercambio de la clave a través del canal cuántico

En la primera parte del protocolo BB84 se emplea el canal cuántico, a través del cual, Alice envía a Bob un conjunto aleatorio de qbits (bits cuánticos) codificados según cuatro estados. Estos cuatro estados se agrupan formando dos bases con estados ortogonales: los dos primeros estados de la expresión (1) forman una primera base y los otros dos forman una segunda, logrando que las condiciones correspondientes al producto escalar entre estados sean satisfechas, es decir, $\langle\psi_0 \,|\, \psi_1\rangle = 0$ y $\langle\psi_+ \,|\, \psi_-\rangle = 0$. Al mismo tiempo, los estados de diferentes bases de la expresión (1) no son ortogonales, cumpliendo así la condición $\langle\psi_{0,1} \,|\, \psi_{+,-}\rangle \neq 0$. De esta forma, un estado queda absolutamente determinado al proyectarlo sobre su correspondiente base, mientras que el resultado será totalmente aleatorio si se proyecta en la otra base.

$$Base_1 = \begin{cases} |\psi_0\rangle = |+, x\rangle = |0\rangle \\ |\psi_1\rangle = |-, x\rangle = |1\rangle \end{cases} \quad (1a)$$

$$Base_2 = \begin{cases} |\psi_+\rangle = |+, y\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \\ |\psi_-\rangle = |-, y\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \end{cases} \quad (1b)$$

Por su parte, Bob determina el estado que Alice le ha enviado escogiendo aleatoriamente, para cada uno de los estados recibidos, una de las dos posibles bases, midiendo y almacenando el

resultado. Es de esperar que Bob escoja la misma base que Alice en el 50 % de los casos.

Mientras Alice trasmite a Bob sus estados, Eve puede interactuar con ellos e interferir en la comunicación. Eve no sabe cuál de los cuatro estados de la expresión (1) ha seleccionado Alice. Por tanto, debe escoger aleatoriamente una de las dos bases para realizar sus medidas. En el caso que acierte y escoja la misma base de Alice, Eve podrá trasmitir el estado correcto a Bob. En el caso que seleccione una base distinta, Eve trasmitirá a Bob un estado incorrecto y este podrá detectar la presencia del espía. Es importante remarcar que Eve no sabrá si ha elegido la base correcta hasta que se lleva a cabo la comunicación por el canal público. Por tanto, existe el 50% de probabilidad de que Eve haya usado la base incorrecta en sus medidas. La Fig. 2 esquematiza el proceso de intercambio de clave a través del canal cuántico.

Alice y Bob tienen una forma sencilla de detectar la presencia de Eve, observando si al realizar la fase inicial del proceso de reconciliación de claves encuentran que las bases escogidas en los dos extremos coinciden en un porcentaje cercano o inferior al 25%. Esta estimación es posible porque en un canal cuántico, una fuga de información es cuantificable por medio de la degradación de la comunicación [4].

Desafortunadamente, la transmisión de claves cuánticas sigue siendo una disciplina novel dentro de las telecomunicaciones, lo que conlleva a que los componentes utilizados sean aún imprecisos y por tanto las tasas de transmisión de clave sean bajas. Por ejemplo, los emisores de pulsos atenuados y los detectores de fotones suponen reducir las tasas máximas de detecciones al 10 %.

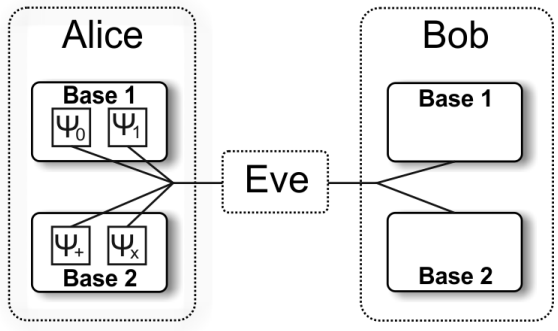

Fig. 2. Esquema del procedimiento para implementar el protocolo BB84.

2.b. Destilación de clave cuántica por canal clásico

Una vez que el envío de la clave finaliza por parte de Alice, comienza el proceso de destilación de clave que se lleva a cabo a través del canal clásico entre los dos extremos. Este proceso está compuesto por cuatro capas sucesivas representadas en la Fig. 3: Reconciliación de bases (*Sifted*), detección de errores (*Error Detection*), corrección de errores (*Error Correction*) y amplificación de la privacidad (*Privacy Amplification*).

En la capa de reconciliación de bases, Alice envía a Bob las bases que ha seleccionado para codificar cada uno de los qbits, pero sin revelar en ningún momento el estado seleccionado. De igual forma Bob comparte qué bases ha empleado para realizar las medidas en cada uno de los qbits que ha recibido, sin indicar el resultado de la medida. Alice y Bob retienen los qbits donde la base elegida por ambos coincide y descartan el resto. Como resultado obtienen una cadena de bits de longitud aproximada la mitad de la original, hecho que inmediatamente reduce en un 50% la tasa de bit y degrada enormemente

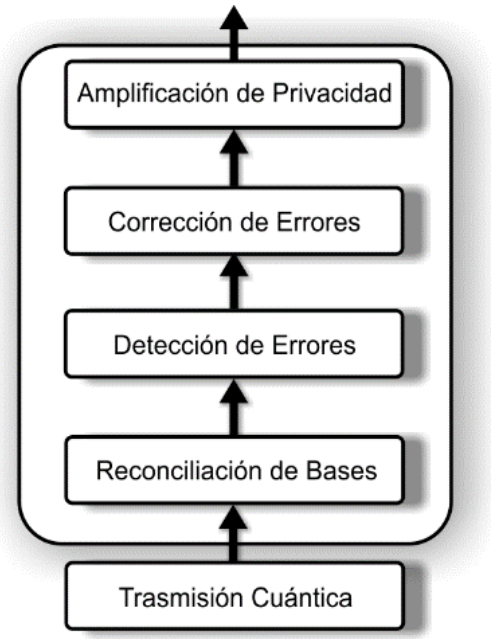

Fig. 3. Capas del proceso de destilación de claves.

la comunicación. En el caso de que un espía intercepte la comunicación, la longitud de la clave será aproximadamente del 25% con lo cual se descartaría la clave completa.

La relación entre los qbits descartados y los enviados es conocida como la tasa de errores cuánticos (QBER, *Quantum Bit Error Rate*), magnitud que resultará clave para decidir si se puede transmitir una clave con seguridad incondicional. Esta cota se debe ajustar a los requerimientos de la aplicación que usara la clave y las características del canal.

Por su parte, la capa de detección de errores comparte una parte de la clave en crudo entre Alice y Bob para tratar de determinar la cantidad de errores que el canal cuántico ha introducido en la comunicación. Los bits compartidos son eliminados de la clave, de forma que la clave resultante junto con la estimación realizada se pasa la capa de corrección de errores para intentar mitigar los errores introducidos por el canal.

En la capa de corrección de errores se pueden emplear diversos algoritmos que corrijan el mayor número de errores y a su vez minimicen la cantidad de información que se revela mediante el canal clásico. Los algoritmos más utilizados incluyen el Cascade [9], el Winnow [10] y el uso de LDPC [11,12].

Para el caso del algoritmo Cascade, que es el más empleado en conjunción con el BB84, la clave se divide en bloques de igual tamaño. Se calcula la paridad a cada uno de los bloques y se intercambia la misma entre Alice y Bob. Si la paridad es la misma se asume que ese bloque no contiene errores, de lo contrario se realiza una búsqueda binaria del error en el bloque. La búsqueda binaria consiste en dividir el bloque en dos y para cada uno de los sub-bloques calcular la paridad y compartirla con el otro extremo de la comunicación. Si las paridades son iguales el bloque no se subdivide. De no ser así, el proceso se repite hasta encontrar el bit erróneo y se corrige.

Siguiendo con el algoritmo Cascade, después de corregir los errores en los bloques iniciales mediante la búsqueda binaria, se reorganizan de forma aleatoria los bits de la clave, y se divide la clave nuevamente para repetir el proceso completo. Se hacen máximo cuatro iteraciones aumentando al doble, en cada ocasión, el tamaño de los bloques iniciales. Se considera que el algoritmo ha corregido todos los errores si llega a las cuatro iteraciones o si el tamaño inicial de bloque supera al tamaño total de la clave.

Contando con una clave idéntica en Alice y Bob se pasa la clave a la capa de amplificación de la privacidad. En esta capa se emplea comúnmente una función hash para codificar los bits de la clave de forma que la información que Eve pueda tener de la clave se reduzca a cero.

Las funciones hash utilizadas en la amplificación de la privacidad son conocidas como hash criptográficas y deben cumplir los siguientes criterios [13]:

- Unidireccionalidad (Resistencia pre-imagen): dado un hash **H**, debe ser computacionalmente inviable encontrar un mensaje **M** tal que **H = hash(M)**
- Resistencia a colisiones: dado **M1** debe ser computacionalmente inviable encontrar **M2** tal que **H = hash(M1) = hash(M2)**
- Uniformidad: dado **H1 = hash(M1)** y **H2 = hash(M2)**; **H1** y **H2** deben diferir en aproximadamente el 50% de sus bits, cuando M2 es igual a M1 con un bit modificado
- Facilidad de cálculo: Debe ser fácil calcular **hash(M)** a partir de un mensaje M
- Resultado constante: para un mensaje **M** la función **hash(M)** debe siempre entregar la misma cantidad de bits (n), sin depender del tamaño de **M**

3. Amplificación la privacidad y la tasa binaria

Como se mencionó anteriormente uno de los grandes problemas de los sistemas de distribución de clave cuántica es la baja tasa de bits que alcanzan. En la actualidad, la aproximación convencional para enfrentar este problema es la de disminuir el número de bits de clave que son descartados en el proceso de corrección de errores. Concretamente, se están haciendo grandes esfuerzos para aprovechar las propiedades de la comprobación de paridad de baja densidad (*Low Density Parity Check*, LDPC) [15,16].

De forma alternativa, para buscar ampliar el tamaño de la clave sin comprometer la seguridad que aporta el protocolo BB84, en este trabajo se propone emplear las funciones hash criptográficas introduciéndoles como entrada una clave de tamaño inferior al de la salida de las mismas, aprovechando así las propiedades de uniformidad y resultado constante.

Para comprobar el funcionamiento de esta propuesta, se ha creado un sistema en el cual Eve tiene entre el 0% y el 99% de la clave que ha obtenido Bob, escenificando así todos los casos posibles incluido el peor caso. Además, se ha definido el QBER inicial entre la clave de Eve y la de Bob como la diferencia entre sus claves (número de bits diferentes) sobre el tamaño total de la clave que se ha obtenido mediante el protocolo BB84 (número de bits de la clave de Bob). Este QBER inicial varia entonces entre 1% y 100% en pasos de 0.1%.

Así, en Bob y en Eve se generan una clave de 2048 bits para cada valor de QBER inicial. Cada una de las claves se procesa mediante la destilación de clave cuántica, utilizando en la capa de amplificación de privacidad una función hash que entrega 512 bits a su salida, obteniendo una clave final de 512 bits en Bob y en Eve. Al comparar los bits que difieren entre la clave final de Bob y Eve y dividirlo por el tamaño total de la clave final se obtiene un QBER medido. En la búsqueda de encontrar un comportamiento medio se realiza 10 veces el proceso para cada uno de los QBER iniciales y se promedian. Los resultados del experimento se muestran en la Fig. 4.

Este resultado, que servirá como línea base de comparación, muestra que para un QBER inicial de entre el 1% y el 100%, es decir en los casos en que Eve dispone entre el 0% y el 99% de la clave, las claves finales de Bob y Eve difieren en un 50 %, hecho atribuible a las propiedades de las funciones hash criptográficas (en este caso SHA-512 [14]).

Para observar el impacto de amplificar el tamaño de la clave final, se plantea un procedimiento análogo al anterior, generando una clave de 2048, procesándola mediante la destilación cuántica pero dividiendo la clave en bloques de 128 antes de emplear funciones hash criptográficas en la capa de amplificación de privacidad. Posteriormente las claves resultado de la función hash se concatenan obteniendo así una clave final de un tamaño promedio de 3072 bits en Bob y en Eve. Calculando el QBER entre las dos claves finales se obtienen los resultados de la Fig. 5.

Este resultado indica que las claves finales difieren en un 50% aproximadamente para QBER iniciales entre el 4% y 99%. También, se observa cómo una degradación de la comunicación cuando el QBER es inferior al 4%. En este caso, el QBER medido es inferior al 50% indicando que el procedimiento impide degradar la clave que obtiene Eve debido a que el número de errores iniciales no es lo suficientemente alto. Desde el punto de vista práctico, los casos en que el QBER sea tan cercano a cero son improbables en la práctica debido a los márgenes de seguridad del protocolo BB84. Por tanto, se puede inferir que la seguridad no se ve comprometida al ampliar el tamaño de la clave. Este resultado es relevante si se tiene en cuenta que con este simple procedimiento, que consume escasos recursos computacionales, se obtiene una mejora evidente en la tasa de bit.

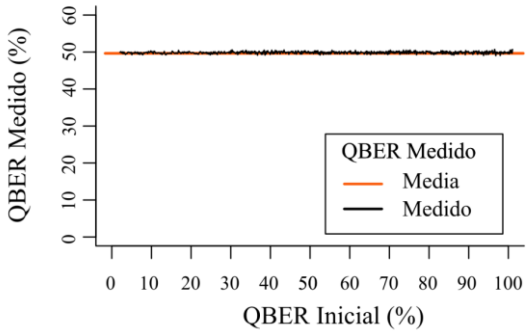

Fig. 4. Clave inicial de 2048, con hash de 512 bits. Clave final de 512 bits.

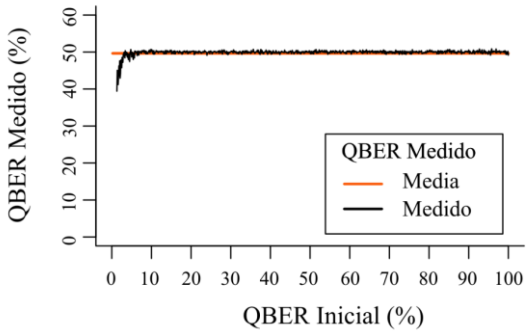

Fig. 5. Clave inicial de 2048, con hash de 512 bits. Clave final promedio de 3072 bits.

Dado que al tener claves iniciales de 128 bits la función hash criptográfica rellena con 384 ceros la clave inicial antes de procesarla, se ve reducido el conjunto de claves posibles de 1 entre 2512 a 1 entre 2128. Por tanto se hace evidente que la seguridad de la clave final con el procedimiento de amplificación mediante funciones hash depende íntegramente de que el protocolo BB84 garantice una seguridad incondicional de forma inequívoca hasta la capa de amplificación de privacidad.

4. Conclusión

La seguridad representa un campo en continuo desarrollo, donde nuevas técnicas y procedimientos que emplean las propiedades de la física cuántica se están abriendo camino al brindar la posibilidad de tener una seguridad incondicional. Sin embargo, estas carecen de una tasa de bit equiparable con las tasas de transmisión actuales.

Para lograr mejorar aumentar la tasa de transmisión de claves cuánticas tradicional-mente se ha propuesto el uso de LDPC. Como línea alternativa, este trabajo presenta el uso de las funciones hash criptográficas usadas en la capa de amplificación de la privacidad para lograr ampliar la tasa binaria apoyándose en las propiedades de estas funciones. Así, experimentalmente se han obtenido mejoras significativas en las tasas de bit para la transmisión de claves cuánticas.

Este trabajo presenta una guía para próximas experimentaciones que usen el proceso de forma iterativa para obtener rendimientos exponenciales de este efecto. Finalmente, en cualquiera de los casos para lograr esta mejora en la tasa de bit sin comprometer la seguridad de la clave se hace necesario que la seguridad incondicional sea asegurada por el protocolo cuántico.

Agradecimientos

Este trabajo ha sido financiado por la ayuda de la Universitat Politècnica de Valencia en la Prueba de Concepto SP20120588 y por Colciencias mediante la beca Francisco José de Caldas. También, este trabajo ha contado con la financiación de la Generalitat Valenciana bajo el programa de investigación de excelencia GVA PROMETEO 2013/012: *Next Generation Microwave Photonic Technologies*.

