

Avance y Perspectiva

Revista de divulgación del CINVESTAV

Llaves cuánticas

Karina Galache · Tuesday, April 2nd, 2019

Categorías: [Ciencias Exactas](#), [Zona Abierta](#)

La información almacenada y aquella que se transmite por la red de telecomunicaciones están en riesgo. La amenaza, así como una posible solución, surge de la aparición de una tecnología disruptiva, resultado de la combinación del concepto de información y de mecánica cuántica lo cual ha dado lugar al campo del conocimiento que se conoce como información cuántica. En este documento se describe un sistema de distribución de llaves cuánticas.

INTRODUCCIÓN

De acuerdo con el Diccionario de la Lengua Española [1], el concepto de información se refiere a “comunicación o adquisición de conocimientos que permiten ampliar o precisar los que se poseen sobre una materia determinada”. Así pues, la información es un tema que se puede abordar desde diferentes perspectivas: del contenido, de su procesamiento, de su transmisión y su seguridad, entre otras. En este texto se aborda el tema en cuanto a la seguridad, la forma en que se cifra –es decir la manera en que se registra siguiendo un código dado- y más específicamente de los medios que se usan para implementar el cifrado.

Las condiciones en que vivimos cambian constantemente. En cuanto a información se refiere, a los jóvenes les parece imposible que hace apenas algunas décadas toda la información se distribuía en físico. Ahora el mundo está interconectado, la comunicación es instantánea, no existen barreras geográficas, las distancias se vuelven irrelevantes, y prácticamente en cualquier lugar hay acceso a instrumentos de información.

Este cambio ha dado lugar a una gran y justificada preocupación por la seguridad de la información [2]. Aspectos que causan inquietud son: *a)* la facilidad que hoy en día tiene cualquier persona para acceder a los medios en que se almacena y a los canales que se usan para intercambiarla y *b)* el incremento en la capacidad de cómputo.

El hecho que la información requiere de medios físicos para su almacenamiento, transmisión y procesamiento, permite entender la intensa relación que existe entre las áreas dedicadas a la información y la física. De hecho, la reducción del tamaño y el aumento en la capacidad de almacenamiento de los dispositivos llevan a considerar a los átomos (o iones) como potenciales

depositarios de la información [3], en cuyo caso los efectos cuánticos se vuelven relevantes.

CIFRANDO LA INFORMACIÓN

La utilidad de la información radica en que se puede intercambiar y procesar, para lo cual resulta conveniente cifrarla. El código ASCII (acrónimo de **American Standard Code for Information Interchange**) [4] asocia una secuencia de ceros y unos a cada uno de los símbolos (por ejemplo, a la letra *d* se le asocia 01100011). Si queremos manipular la información es conveniente implementar una realización por medio de propiedades físicas, un pulso -señal diferente de cero en un intervalo de tiempo- se usa frecuentemente para representar el 1 mientras que la ausencia de pulso representa el 0. Cualquier propiedad física puede ser utilizada, lo importante es que se pueda diferenciar el 1 del 0 y claro, que sea práctico. A esas unidades de información, se los conoce como bits.

Además de cifrar, frecuentemente es necesario *encriptar* la información, es decir ocultarla de manera que sólo se pueda acceder a ella mediante una llave. Un tipo de llave consiste en una secuencia de unos y ceros, de la misma longitud del texto bajo consideración. El encriptamiento se realiza implementando una relación entre la llave y la información que se quiere compartir. Este sencillo procedimiento permite transmitir de manera segura la información, ya que para tener acceso a ella se requiere de la llave. También es posible que uno quiera compartir la llave con una o varias personas, en cuyo caso lo ideal es hacerles llegar la llave por algún medio. Evidentemente este es un problema serio, pues empezamos queriendo compartir un mensaje de manera segura, y terminamos buscando formas de enviar de manera segura la llave. ¡El mismo problema! Esto nos conduce al concepto de “**Sistema de Distribución de Llaves**”

Lo que hemos descrito es la forma tradicional de implementar los unos y ceros, en cuyo caso quien tenga acceso a la llave puede copiar, almacenar, analizar y en su caso obtener la información. Existe una forma de evitar esas debilidades del tratamiento convencional, pero antes de exponerla haremos una breve visita al mundo cuántico.

PINCELADAS DEL MUNDO CUÁNTICO

Aun cuando no seamos conscientes de la relevancia de la mecánica cuántica para la conformación del paisaje de nuestro entorno, a un nivel dado, todo es cuántico. Muestra de ello es que fuera de ese marco es imposible entender el funcionamiento de los instrumentos que nos facilitan la vida (computadoras, teléfonos, láser, etc.). Un concepto muy adecuado para describir un objeto cuántico es el de **ente**, que de acuerdo con el diccionario [1] se refiere a “Lo que es, existe o puede existir”. Los **entes** que habitan el mundo cuántico (escala atómica) tienen un comportamiento extraño, los siguientes son algunos ejemplos:

- Al hacer una medición sobre un ente no podemos saber si lo que observamos corresponde al estado en que se encontraba antes de observarlo. Más aún, se demuestra que *es imposible* diseñar un procedimiento para hacer una copia del original.
- Pérdida de identidad, en el sentido que no hay una clara definición de la naturaleza del ente. Objetos materiales, por ejemplo, un electrón, tienen la capacidad de interferir, como las ondas. Esto se observa al hacer incidir electrones sobre estructuras periódicas, como es el caso de cristales, o de algunos materiales biológicos. Por el contrario, la luz, a la que convencionalmente

asociamos ondas, en condiciones especiales (muy bajas intensidades) se comporta como si fuera una canica.

- La luz existe en dos estados de polarización a los cuales podemos llamar: V1 y V2. En el mundo macroscópico la intensidad de la luz corresponde a la suma de la luz que tiene la polarización V1 y la que tiene V2. Los lentes para sol usan esa propiedad, lo que hacen es bloquear la luz con una de esas polarizaciones, reduciendo de esta manera la intensidad. En el mundo cuántico, la situación es ligeramente diferente, un solo ente, en este caso fotón, puede existir en un estado que incluye a la vez, V1 y V2. En ese caso, al poner en el camino del fotón unos lentes para luz, no tenemos certeza de lo que sucederá. Si repetimos el experimento de hacer incidir uno de esos fotones sobre los lentes, en algunos casos pasará mientras que en otros será reflejado. En términos generales, si en la naturaleza se observan dos o más “estados” de un mismo ente cuántico, entonces en un solo ente pueden coexistir todos los estados, con peso relativo arbitrario, lo que conduce a una infinita gama de posibilidades para un solo objeto cuántico.

En los últimos años ha surgido una tecnología que ha modificado las pautas que hasta hace poco se usaban al manejar y procesar información. La innovación que aporta esta tecnología proviene de la realización física de los unos y ceros mediante entes cuánticos. Así, lo que se hace es reemplazar el bit convencional por el **qubit**, el equivalente cuántico del bit. Mientras que el bit clásico sólo puede tomar dos valores, de forma excluyente, el uno o el cero, el qubit incluye infinitas posibilidades. Aunque no abundaremos sobre este tema, un ejemplo donde esto se aplica es la computación cuántica, la cual se ha implementado usando núcleos [5].

LLAVES CUÁNTICAS

En el caso de la distribución de llaves para encriptamiento (QKD por sus siglas en inglés: Quantum Key Distribution) se usan fotones [2,6,7], es decir el mínimo paquete de luz de un color dado. La información que transporta cada fotón sólo se puede determinar al realizar una medición, sin embargo, la naturaleza cuántica del fotón tiene dos consecuencias relevantes: *i*) el resultado de la medición no necesariamente corresponde a la información que contenía el fotón antes de hacer la medición y *ii*) permite detectar cuando alguien no autorizado trata de leer la información toda vez que la medición modifica el estado del ente.

El sistema de QKD involucra dos partes interesadas (**A** y **B**) que quieren intercambiar información de forma segura, para lo cual disponen de un canal clásico (teléfono, internet, etc.) y uno cuántico, por donde viajarán los fotones (fibra óptica, aire).

A y **B** usan todos los medios y procedimientos a su alcance para asegurar que identifican, uno a uno, los fotones, el estado cuántico en que se encuentran. También, tienen la capacidad de detectar la posible intrusión de un espía (**E**), en caso de que haya sucedido. De esta manera se logra establecer una forma segura de distribuir llaves de criptografía, cuya seguridad se fundamenta en la naturaleza cuántica de los portadores de la información y complementada con procesos de criptografía convencional [8].



Fig (1). Módulo de Alice. Esquema de los componentes ópticos y de control: (Laser) Laser CW @ 1550 nm, (Pol) Polarizador en fibra, (IM) Modulador de intensidad para pulsar el láser, (PM1) Modulador de Fase para introducir la codificación en fase, (VOA) Atenuador óptico variable, (FPGA1) Controlador basado en una FPGA.

Un sistema de QKD incluye los siguientes módulos: emisor (**Alice**), receptor (**Bob**), de sincronización, de adquisición y post-procesamiento y finalmente el canal de propagación cuántica. En los siguientes párrafos se describe muy brevemente cada uno de ellos, para lo cual usamos como referencia el sistema que está siendo desarrollado en la Universidad de Guanajuato. La Fig. (1) muestra un esquema del módulo Alice, mientras que en la Fig.(2) se representa el módulo receptor (Bob). No se incluyen separadamente el módulo de sincronización, el de adquisición y post-procesamiento porque están incluidos parcialmente en Alice y Bob. En realidad, no tiene sentido separarlos físicamente ya que es un software incluido en las FPGA's y en equipo de cómputo periférico.



Fig (2). Módulo de Bob. Esquema de los componentes ópticos y de control: (BS1) Divisor de haz de separación, (PM2) Modulador de Fase para introducir la selección de la base de detección, (BS2) Divisor de haz de interferencia, (APD1 y APD2) Detectores de un solo fotón, (FPGA2) Controlador basado en una FPGA, (TDC) Convertidor digital de tiempo.

Módulo emisor (Fig. 1): En este módulo se preparan los estados cuánticos a partir de los cuales se generan las llaves secretas. Para realizar las tareas asignadas, este módulo requiere: *i) la fuente de luz (laser)* con las características adecuadas, que incluyen la longitud de onda, la polarización, la potencia, la estabilidad de la potencia emitida, entre otras. *ii) polarizador* que nos asegura que el sistema funciona con un solo estado de polarización, *iii) modulador de amplitud*, que permite generar pulsos cuyas características relevantes son: ancho de pulso, la frecuencia de repetición, y posteriormente, la sincronización como se discutirá más adelante, *iv) modulador de fase*, con este dispositivo se induce una fase a cada pulso, la selección de fases se hace de manera aleatoria, en eso consiste la generación de los cuatro estados cuánticos que son usados para transmitir la información, *v) Atenuador*, como su nombre lo indica atenúa la intensidad del pulso, la energía contenida en cada uno de los pulsos. En nuestro caso, la atenuación se hace de manera que cada pulso tenga un número promedio de fotones ≈ 1 . *vi)* Se usa una FPGA (Field Programmable Gate array) para generar pulsos de 3.5 V, en nuestro caso a una frecuencia de 40 MHz y con un ancho temporal ns. Este voltaje se aplica al modulador de intensidad con el fin de generar pulsos a la frecuencia elegida. La misma FPGA se usa para aplicar un pulso de voltaje al modulador de fase, el cual se elige de manera aleatoria entre cuatro posibles valores, (V_1, V_2, V_3 y V_4). Los valores de los V 's se encuentran al caracterizar los moduladores de fase, lo cual permite determinar el valor del voltaje que se debe aplicar para incrementar en pasos de $\pi/2$ la fase. El resultado neto es que se están enviando un tren de pulsos. Cada uno con un número medio de fotones menor o igual a uno, y cuyas fases difieren aleatoriamente en un múltiplo de $\pi/2$. Esos cuatro tipos de pulsos son los cuatro estados cuánticos que se usan para encriptar la información; *vii)* La seguridad del sistema requiere que los números aleatorios mencionados en el punto *vi* sean realmente aleatorios. En este momento usamos números pseudo-aleatorios generados por un software de computadora, pero se puede implementar un sistema cuántico que genere una secuencia de números realmente aleatorios [9].

Módulo receptor: Incluye un interferómetro tipo Mach-Zehnder asimétrico (ver Fig.(2)), en uno de cuyos brazos se coloca un modulador de fase, el control de las fases se realiza con una FPGA y

las salidas del interferómetro van a dos detectores. Si el tamaño de los brazos fuera igual, un pulso que entra interfiere en el divisor de haz de salida (BS2), es decir el pulso interfiere consigo mismo. Sin embargo, en nuestro caso el interferómetro está construido de manera que el pulso que viaja por el brazo más largo coincide en el BS2 no consigo mismo sino con el pulso que le sigue (porque viaja por el brazo más corto). Además, la FPGA del módulo receptor induce, de manera aleatoria, una fase que es 0 o $\pi/2$. La combinación de la fase inducida en el módulo emisor y la aplicada en el módulo receptor es lo que determina, de manera probabilística, el resultado de la detección. Nótese que también en este módulo se requiere una secuencia de números aleatorios.

Módulo de sincronización: Dado que el intercambio de información implica la emisión y recepción de fotones, se debe identificar cada fotón sin posibilidad de confusión o error. Esto es, se debe sincronizar el momento en que inicia la emisión y la recepción de manera que hay control absoluto sobre la coincidencia entre el pulso emitido y la detección que se realiza. Es claro que esto requiere de sincronización y que en el caso de grandes distancias, cientos de kilómetros, requiere el uso de tecnología satelital. De hecho, también se requiere una sincronización local que considere los tiempos de vuelo dentro del módulo emisor y del receptor y que primero se generan los pulsos y posteriormente a cada uno de esos pulsos se les induce una fase mediante la aplicación de un voltaje calibrado al modulador de fase. Además del tiempo que pasa el pulso en el módulo emisor, se requiere determinar, sin ambigüedad en cuanto a la identificación, el voltaje que se aplica a cada pulso. Dado que la frecuencia a la que se generan los pulsos es 40 MHz, se requiere que la sincronización pueda distinguir sin ambigüedad los pulsos emitidos a intervalos de 25 ns. La sincronización que implementamos distingue espacios del orden de 2 ns.

Módulo de adquisición: En lo que se refiere a equipo, este módulo incluye dos fotodiodos de avalancha (APD1 y APD2) y un convertidor tiempo-digital (TDC), sincronizado con las FPGAs, de manera que se identifican intervalos de tiempo en los que se espera el arribo de un pulso. El TDC incluye varios canales, así que es posible usar un canal para monitorear el APD1 y, de forma independiente, otro canal para el APD2. El TDC monitorea las señales recibidas por los fotodiodos y asigna un 1 o 0 a cada intervalo de tiempo, dependiendo del detector que se activa. Mientras que en los intervalos de tiempo en los que no hay detección no se asigna bit. En resumen, Alice envía un tren de pulsos (qubits) en los que cifra unos y ceros, se sincroniza todo el equipo de manera que Alice y Bob están de acuerdo en lo que significa pulso 1, pulso 2, y así hasta el total de pulsos enviados. A cada uno de esos pulsos el TDC le asocia un uno o un cero, dependiendo de la actividad del correspondiente detector. Debido a la aleatoriedad en los moduladores de fase, dependiendo de la combinación de voltajes que se aplican, idealmente existen sólo tres posibles resultados en la ventana de tiempo que corresponde a un pulso: *i*) ninguno de los detectores se activa, *ii*) se activa uno de los dos detectores y *iii*) se activan los dos detectores.

Existen diferentes combinaciones que dan lugar a cada uno de esos resultados y se debe calcular la probabilidad de que cada uno de ellos se produzca. El primer elemento a tener en cuenta es la posibilidad de que el pulso no contenga ningún fotón, que contenga un fotón o que contenga más de un fotón. Recordemos que la fuente que se usa es un láser y por lo tanto la distribución de fotones es Poissoniana. Otro elemento a tener en cuenta es lo que sucede en el separador de haz BS1 a la entrada del módulo de Bob, cuando en el pulso no hay fotón este divisor es irrelevante, cuando en el pulso hay un fotón se asigna la misma probabilidad a que el fotón siga cualquiera de los dos caminos disponibles, y cuando el pulso contiene más de un fotón, existe probabilidad de que el pulso completo viaje por los dos caminos, de que un fotón viaje por un camino y el resto por el otro camino. Finalmente, se considera la probabilidad de que en el intervalo considerado uno de los detectores ocurra una cuenta oscura –cuando el detector se activa aunque no reciba fotones- o

bien que, en los dos detectores, simultáneamente, se produzcan cuentas oscuras.

La descripción del último párrafo deja en claro que el proceso de transmisión induce errores – la ausencia de fotón en algunos pulsos y las cuentas oscuras que son inherentes a los detectores. Lo importante es que, una vez caracterizado el equipo que se usa, los errores mencionados son calculables y forma parte del post-procesamiento que a continuación se describe.

Post-procesamiento: Una vez que el emisor hace llegar una secuencia de bits al receptor, intercambian información por un canal clásico, que depende del protocolo usado, sobre las condiciones de emisión y detección de cada uno de los pulsos. Esto les permite establecer cuáles de los bits que tienen cada uno de ellos coinciden. De esta manera **A** y **B** pueden descartar los bits en los que saben que emisión y recepción no son compatibles. A la secuencia de bits que les queda, se aplica el siguiente procedimiento: Primero, mediante simulación que considera las características del equipo usado -detectores y el canal de comunicación cuántica- se determina cuál es la razón de errores (quantum bit error rate – QBER) que se debe esperar en la secuencia. **A** y **B** usan una porción (típicamente 25% de la secuencia) para estimar el QBER con los datos reales, y en caso de que el QBER así medido resulte mayor que el obtenido de la simulación, la diferencia se atribuye a un espía, a alguien que está realizando mediciones y obteniendo información. Si la información obtenida por el espía es mayor que un valor crítico [10], entonces se debe desechar la secuencia porque la seguridad no se puede garantizar y debe reiniciarse el proceso.

Otros procesos que se aplican son, la corrección de errores y la ampliación de la privacidad. En el primero de ellos se usan algoritmos desarrollados en la criptografía clásica, un ejemplo de ellos es **CASCADE** [11,12]. El concepto base es el de paridad, para lo cual se asigna paridad positiva al 0 y negativa al 1. De esta manera a una secuencia de bits se le asigna la paridad que resulta de multiplicar la paridad de cada uno de sus elementos. Lo que se hace con *cascade* es dividir la secuencia en bloques de tamaño $T_1=2^{d_1}$, se compara la paridad de cada uno de esos bloques y se divide en dos, cada vez que resultan diferentes los valores de paridad que se encuentran. Se sigue este procedimiento hasta encontrar el error y corregirlo. Este ciclo se repite cuatro veces, excepto que se duplica la longitud del tamaño de los bloques de inicio, de manera que para el *i*-ésimo ciclo el tamaño de los bloques es $T_i=2^{d_i}$. Este procedimiento asegura dos cosas, primero que se corrigen los errores generados por características inherentes al equipo usado y segundo que es óptimo, en el sentido que se minimiza tanto la información liberada como la probabilidad de que la secuencia obtenida contenga errores.

Es importante hacer notar que la corrección de errores requiere intercambio de información entre **A** y **B** –las paridades- lo cual se hace por medio de un canal clásico. La ampliación de privacidad tiene como objetivo limitar los riesgos que generan esa posible fuga de información en la implementación de *cascade*. Con este fin, **A** y **B** comparten por un canal público una secuencia aleatoria y con esa secuencia generan la transformación de la secuencia libre de errores realizando el mapeo a una nueva secuencia. En nuestro caso el mapeo se hace mediante una matriz de Toeplitz [13,14]. Las funciones hash[15] y las condiciones rigurosas para su seguridad, son temas extensos y de continua discusión, aquí nos limitaremos a mencionar algunas de las características que las hacen una herramienta adecuada para QKD. Por ejemplo, el mapeo es determinista, que en este contexto significa que cada vez que se aplica el mapeo a un mensaje siempre resulta en el mismo hash, otra propiedad es que un cambio pequeño en la secuencia a la que se aplica la función hash cambia totalmente la secuencia que se obtiene, esto es particularmente útil dado que se espera que el espía tenga una limitada cantidad de información sobre la secuencia. El punto central es

establecer las condiciones que garanticen la seguridad y optimicen el uso de recursos.

Canal de propagación cuántica: La calidad del intercambio de información se puede medir en lo que se denomina la capacidad del canal, la cual depende de la naturaleza de la fuente de luz, del medio en que se propaga, pero también del sistema de medición. Así, entre otras cosas, la transmisión de información es sensible a la forma en que se transporta, en particular de la interacción entre el ente en que se codifica la información y el medio por el que se propaga, es decir la fibra óptica. Respecto al canal de transmisión, se requiere caracterizar la fibra óptica, la calidad del tendido de fibra, posibles efectos externos (temperatura, presión, etc.) sobre las características de la fibra y sobre la transmisión de los fotones. La atenuación, es decir la absorción de los fotones en la fibra, es una de las limitaciones más importantes para el desarrollo a grandes distancias del tipo de sistemas aquí descrito.

Hasta aquí hemos hecho una breve descripción de los módulos que se deben desarrollar para implementar un sistema de criptografía cuántica. La velocidad con la que este campo del conocimiento avanza, y que se ve reflejada en desarrollo de tecnología es vertiginoso y altamente retador. Un avance significativo ha sido la implementación de memorias cuánticas [16], es decir un dispositivo que almacena la información cuántica. Características importantes de estas memorias son: que funcionan a temperatura ambiente, que logran almacenar la información durante microsegundos, con potencial de incrementarlo a milisegundos, que se puede extraer la información de manera controlada y con alto grado de fidelidad.

El mecanismo consiste en transferir la información que ha sido cifrada en un fotón a un átomo o a una nube de átomos y extraerla en forma análoga, es decir lograr que los átomos emitan un fotón con características cuánticas idénticas a las del fotón inicial. Los desarrollos más prácticos, usan nubes de átomos de rubidio y su desarrollo es tal que en los próximos años se volverá rutinaria esta tecnología. Nótese que en este caso no se hace una copia del estado, el ente cuántico se destruye, la información pasa a un sistema atómico y posteriormente se crea otro fotón [16].

Es importante mencionar, antes de concluir este texto, que uno de los avances más recientes se da en el contexto de la distribución de llaves cuánticas a través del aire, no por medio de fibra óptica [6]. La relevancia de este esquema es que incrementa el alcance en que se pueden distribuir las llaves, de hecho, se puede prever que este es el primer paso hacia un esquema global de comunicación cuántica. Entre los retos importantes que se deben superar se encuentran [17]: la existencia de una red de satélites con capacidad cuántica, la necesidad de perfeccionar las memorias cuánticas, que localmente se sigue dependiendo de las redes de fibras ópticas de telecomunicaciones, y reducir los costos de la implementación de de redes QKD.

Finalmente mencionamos que una colaboración entre el CIDESI, la unidad Querétaro del CINVESTAV y la Universidad de Guanajuato se está implementando un sistema de QKD con financiamiento proporcionado por CONACyT y la Universidad de Guanajuato.

CONCLUSIÓN

Los entes cuánticos poseen atributos que son un recurso, en el sentido que esas propiedades nos permiten realizar tareas que sería imposible de lograr de otra forma. La tecnología cuántica (el manejo y la aplicación de objetos cuánticos y de sus propiedades) ya es una realidad y ha tenido un desarrollo vertiginoso, el cual se acelerará en los próximos años. El impacto que esto tendrá en los

temas de información es múltiple, incluyendo la capacidad de cómputo y la seguridad de la información. Éste es un tema fascinante por la investigación básica que requiere y altamente relevante por sus aplicaciones.

REFERENCIAS

- [1] Real Academia Española (2014). Diccionario de la lengua española (22^a ed.). Consultado en <http://www.rae.es/rae.html>
- [2] Nicolas Gisin, Grégoire Ribordy, Wolfgang Tittel, and Hugo Zbinden, “Quantum cryptography”; *Rev. Mod. Phys.* **74**, 145 – 195, (2002)
- [3] Th Sriarunothai, S Wölk, G S Giri, N Friis, V Dunjko, H J Briegel and Ch Wunderlich “*Speeding-up the decision making of a learning agent using an ion trap quantum processor*”; *Quantum Science and Technology* **4**, 015014 (2019)
- [4] Charles E. Mackenzie, “*Coded Character Sets, History and Development. The Systems Programming Series*” (1^a edición), Addison-Wesley Publishing Co. Inc. (1980).
- [5] Bjoern Lekitsch, Sebastian Weidt, Austin G. Fowler, Klaus Mølmer, Simon J. Devitt, Christof Wunderlich and Winfried K. Hensinger; “Blueprint for a microwave trapped ion quantum computer” *Sci. Adv.* **3**, e1601540 (2017).
- [6] Liao, S. K, *et al*, “Satellite-to-ground quantum key distribution” *Nature* **549**, 43-47, (2017)
- [7] Hoi-Kwong Lo, Marcos Curty, and Kiyoshi Tamaki, “Secure quantum key distribution”; *Nature Photonics* **8**, pp. 595 – 604, (2014)
- [8] Jennifer Chu, “The beginning of the end for encryption schemes?” *MIT News Office* March 3, 2016; Consultado en <http://news.mit.edu/2016/quantum-computer-end-encryption-schemes-0303>
- [9] Miguel Herrero-Collantes and Juan Carlos Garcia-Escartin, “Quantum random number generators”; *Rev. Mod. Phys.* **89**, 015004, (2017)
- [10] Norbert Lütkenhaus, “Security against individual attacks for realistic quantum key distribution”, *Phys. Rev. A* **61**, 052304 (2000)
- [11] Mateo Martínez, Jesús Pacher, Christoph Peev, Momtchil Ciurana, Alex Martin, Vicente, “Demystifying the Information Reconciliation Protocol Cascade” *Quantum Information and Computation*, **15**, 453 (2015),
- [12] Calver, T.I.1, **Grimaila, M.R.**, and Humphries, J, “An Empirical Analysis of the Cascade Error Reconciliation Protocol for Quantum Key Distribution,” Proceedings of the Cyber Security and Information Intelligence Research Workshop (CSIIRW 2011), Oak Ridge National Laboratory, Oak Ridge, TN, October 12-14, 2011.
- [13] Nikolay Gegov; Quantum Key Distribution Data Post-Processing with Limited Resources: Towards Satellite-Based Quantum Communication. Waterloo, Ontario, Canada, 2013.; *UWSpace* <http://hdl.handle.net/10012/7244>
- [14] Oleg Nikiforov, Alexander Sauer, Johannes Schickel, Alexandra Weber, Gernot Alber, Heiko Mantel, Thomas Walther; “Side-Channel Analysis of Privacy Amplification in Postprocessing Software for a Quantum Key Distribution System” Technical Report TUD-CS-2018-0024 (2018)
- [15] Alfred J. Menezes, Paul C. van Oorschot and Scott A. Vanstone, “Handbook of Applied Cryptography”, CRC Press 2011
- [16] M. Namazi, C. Kupchak, B. Jordaan, R. Shahrokhshahi and E. Figueroa, Ultralow-Noise Room-Temperature Quantum Memory for Polarization Qubits, *Physical Review Applied* **8** (3), 034023 (2017)
- [17] Eleni Diamanti, Hoi-Kwong Lo, Bing Qi, and Zhiliang Yuan, “Practical challenges in quantum key distribution”; *npj Quantum Information* **2**, 16025 (2016)

José Luis Lucio Martínez, Carlos R. Valdivia y Carlos Wiechers.
Departamento de física; D.C.I. Campus León. Universidad de Guanajuato.

This entry was posted on Tuesday, April 2nd, 2019 at 9:20 am and is filed under [Ciencias Exactas, Zona Abierta](#)

You can follow any responses to this entry through the [Comments \(RSS\)](#) feed. Both comments and pings are currently closed.