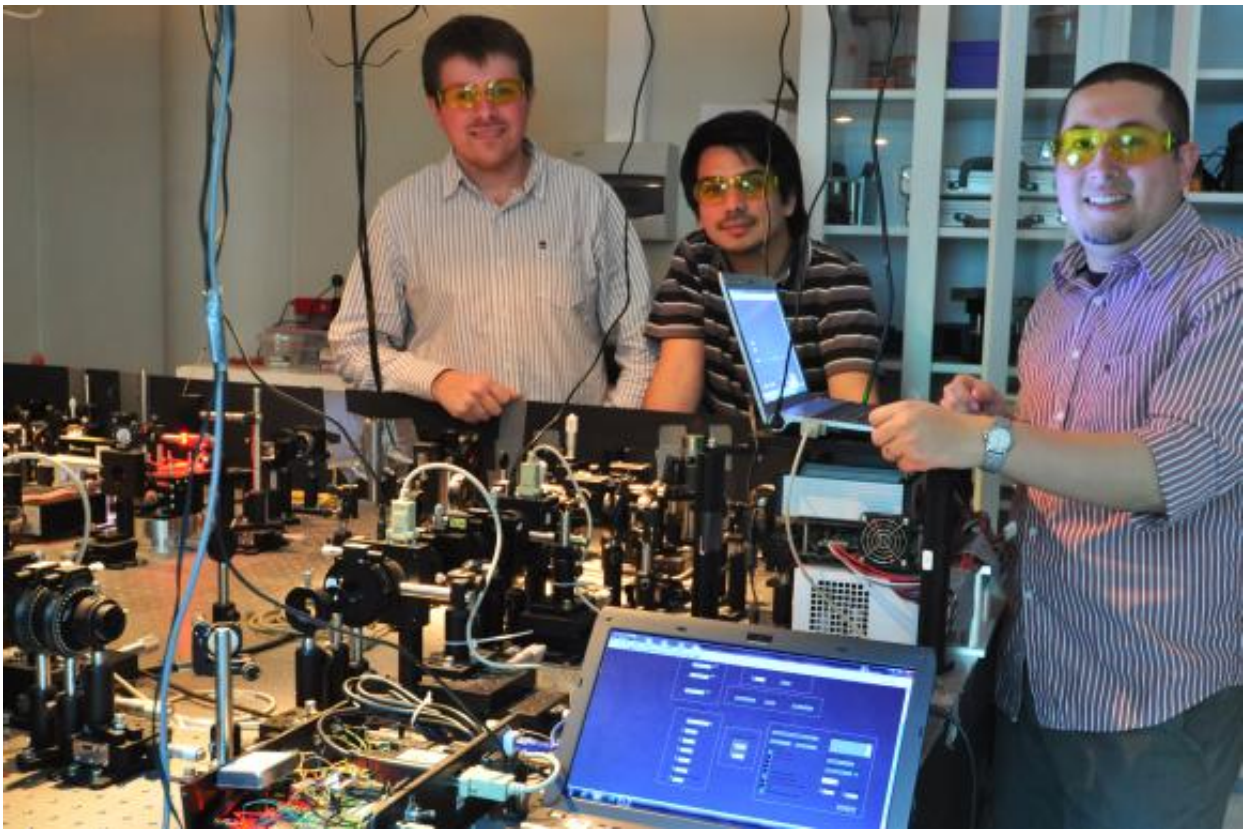
Infocyt
agencia informativa
Información sobre ciencia - tecnología - innovación - divulgación

Ciencia

Científicos chilenos innovan en criptografía de última generación

Publicado: **2013-09-03**

Investigadores del CEFOP están desarrollando nuevos esquemas de "criptografía cuántica experimental en altas dimensiones". Aunque suene complicado, su desarrollo apunta a convertirse en una innovación mundial en nuevos sistemas de transmisión de información, más seguros y de mayor capacidad. Nota realizada por periodistas del CEFOP.



Piense en cuántas claves de seguridad usa a diario. Cada vez que utiliza un cajero automático, al abrir su correo electrónico y en muchas otras ocasiones, está protegiendo, por algún medio, cierta información privada que no desea que sea conocida por terceros. ¿Qué pasaría si esos datos cayeran en manos mal intencionadas?

De acuerdo al "Informe de Amenazas de Seguridad 2012", realizado por la empresa Sophos Security, las pérdidas provocadas por filtraciones de datos alcanzaron en 2010 una media de 7,2 millones de dólares por incidente, lo

que incluye tanto costos directos como indirectos, entre ellos la pérdida de confianza entre los usuarios. En un mundo donde el envío de información confidencial es un problema cotidiano, con el que deben lidiar entidades bancarias, gobiernos y ciudadanos, la búsqueda de una técnica segura de envío de información es el santo grial de investigadores en todo el mundo.

En esa tarea se encuentra desde hace varios años un grupo de investigadores del Centro de Óptica y Fotónica (CEFOP), de las Facultades de Ingeniería y Ciencias Físicas y Matemáticas de la Universidad de Concepción, quienes han creado un sistema de criptografía cuántica hasta ahora único. Los logros de su investigación fueron publicados este martes 30 de julio en *ScientificReports* (medio perteneciente a la prestigiosa revista *Nature*), con lo que se abre una ruta para alcanzar tecnologías que volverían inviolables los mensajes. Este avance es consecuencia de una de las líneas de investigación del Centro, cuyos primeros resultados experimentales en el ámbito de computación cuántica datan de 2009, en la cual han participado más de diez investigadores de CEFOP y de colaboradores internacionales. Estas actividades experimentaleshan contado con el apoyo del Fondo de Fomento al Desarrollo Científico y Tecnológico, Fondef, el Programa de Financiamiento Basal y de la Iniciativa Científica Milenio, estos últimos pertenecientes a CONICYT y al Ministerio de Economía, respectivamente.

¿Qué es la criptografía cuántica?

Tradicionalmente, la criptografía se dedica a buscar diferentes formas para proteger los mensajes de lectores no autorizados. La tecnología actual, basada en algoritmos matemáticos, es capaz de proteger la información, pues la "esconde" utilizando factorizaciones de números primos, un ejercicio que aún los computadores con mejores procesadores del mundo tardarían años en descifrar. Sin embargo, el avance hacia equipos cada vez más potentes ha facilitado esta operación, dejando obsoletos sistemas hasta hace poco considerados confiables. Además, una vez descubierta la clave, la detección del intruso es casi imposible, por lo que el sistema se vuelve vulnerable.

En este campo, la física cuántica ofrece una alternativa que aprovecha las leyes fundamentales de la naturaleza: el estado de un fotón, la partícula elemental de la luz, no puede ser medido sin alterar sus características. Por lo tanto, cualquier intruso que intente interceptar su camino, inevitablemente destruirá el mensaje enviado o provocará errores que harán evidente su presencia. La idea de utilizar estos principios para *encriptar* mensajes surgió en los '70, pero solo en 1984 se logró el primer protocolo. A partir de entonces, la criptografía cuántica ha pasado de la teoría a la práctica, logrando que ya existan sistemas de seguridad beneficiados por esta tecnología.

El avance "made in Chile"

Los actuales protocolos de distribución de claves cuánticas (o QKD) permiten que usuarios distantes puedan compartir una clave secreta, usando canales cuánticos de comunicación. Estos sistemas han sido implementados por un banco Suizo, por ejemplo, con el fin de garantizar la transmisión segura de datos entre sus distintas sucursales. Otro ejemplo de aplicación la realizó en octubre de 2007 el Gobierno de Ginebra, cuando por primera vez utilizaron un cifrado híbrido mezclando QKD con el sistema AES tradicional de criptografía, para enviar información entre los lugares de votación y la estación central de conteo de votos, protegiendo así la autenticidad e integridad de los datos recogidos en el referéndum, con un tipo de seguridad nunca antes visto, que detecta la presencia de espías.

Sin embargo, aún hay restricciones: una es la distancia entre los usuarios, que no puede superar un cierto rango, definido por las condiciones de transmisión de los sistemas cuánticos. La segunda limitación es la cantidad de información transmitida, que depende del número de dimensiones que posea el sistema y de la velocidad de los componentes. "Un problema que esta tecnología tiene es que la tasa de transmisión es todavía baja comparada con

los sistemas tradicionales de telecomunicaciones. Las demostraciones en laboratorio de QKD más avanzadas en dos dimensiones llegan a 1 o 2 megabits de clave segura generada por segundo. Mientras los sistemas de telecomunicaciones modernos pueden llegar a varios gigabits por segundo", señaló el Dr. Guilherme Xavier, investigador de la Facultad de Ingeniería de la Universidad de Concepción y miembro de CEFOP. "Por este motivo este prototipo es un avance importante, porque hemos probado que se puede aumentar la tasa 4 veces y con un cambio de la tecnología esto se puede incrementar aún más, pues ahora hemos realizado un experimento que es una prueba de principio de funcionamiento", destacó.

Cuando se habla de dimensiones de un sistema físico, se debe pensar en la cantidad de estados "perfectamente distinguibles" que pueden ser medidos. Por ejemplo, un interruptor tiene dos dimensiones, por lo tanto, la información que se puede obtener es si está encendido o apagado. Hasta ahora, los sistemas de comunicación cuánticos en general utilizan estados cuánticos de dos dimensiones, determinadas por la polarización o la fase de un fotón. "Con esto se puede codificar la información, porque los bits tienen también dos dimensiones, 0 y 1. Nosotros, en lugar de ocupar estas propiedades, usamos otra, en este caso propiedades espaciales de un fotón" indicó el Dr. Gustavo Lima, profesor de la Facultad de Ciencias Físicas y Matemáticas de la Universidad de Concepción. Explorando las propiedades transversales de un fotón, se logra crear un sistema físico no a dos, sino a 16 dimensiones; como si en vez de elegir entre dos caminos, pudiéramos seguir 16 rutas distintas. "Con esto, codificamos la información, ya no en bits, sino en altas dimensiones, de 0 a 15. Así, en lugar de enviar 1 bit por fotón, envía 4 bits, con lo que crece la cantidad de información que estamos transmitiendo de una sola vez en el sistema de comunicación".

Incrementar las dimensiones en sistemas de comunicación cuánticas, tuvo un desarrollo teórico durante la década pasada, y ahora recién está empezando la etapa experimental" enfatizó el Dr. Lima. "Además de enviar más bits por fotón compartido, al aumentar las dimensiones, aumenta también la seguridad del sistema, de modo que nuestro sistema es más robusto frente al ataque de un espía.

Innovación y desarrollo

Los estudios teóricos realizados en el CEFOP permiten ahora ir un paso adelante, ya que hasta el momento otros centros trabajan en general con menos dimensiones, o en forma manual en altas dimensiones. La publicación de estos investigadores demuestra que es posible usar más dimensiones en el mundo real, a través de un sistema totalmente automatizado y con tasas de error que garantizan la inviolabilidad de la clave. "En dos dimensiones ya hay muchos experimentos, pero en mayores dimensiones es la primera vez que se tiene éxito. Además, nosotros tenemos un sistema automatizado. Los estados cuánticos se envían y detectan en forma aleatoria, por lo tanto el sistema tiene que responder de forma dinámica y en tiempo real a las características de la información enviada".

Nuestro país sigue siendo un consumidor, pero no un productor de tecnologías de información, lo que se observa en rankings latinoamericanos sobre adopción de nuevas herramientas de comunicación, liderados por Chile, pero sin lograr abrir escenarios para la creación de nuevos instrumentos. Un paradigma que investigaciones como la desarrollada en CEFOP contribuyen a romper, al iniciar un desarrollo experimental de protocolos no ensayados en otros países, que puede continuar avanzando.

El Dr. Carlos Saavedra, Director Científico de CEFOP, apuntó: "La próxima etapa de investigación es hacer pruebas de campo, ampliando la distancia y enviando estas claves, por ejemplo, desde una facultad a otra. Por otra parte, las tasas de transmisión se pueden mejorar mucho si se usan dispositivos que nos permitan codificar en forma más rápida, que ya existen, aun cuando no están comercialmente disponibles. Actualmente, nos encontramos en etapa de preparación de los próximos experimentos para aumentar las distancias y tasas de transmisión en

espacio libre y en fibras ópticas y esperamos contar con nuevos recursos, provenientes de fondos concursables, que nos permitan financiar estas nuevas etapas".

Entre los desafíos próximos de CEFOP está el generar nueva instrumentación, basada en los resultados científicos de sus investigadores; el reciente resultado es un paso importante en esa dirección, que complementa otras líneas desarrolladas en el Centro, vinculadas al desarrollo de herramientas aplicadas en campos como la prevención y control de contaminación ambiental y otras utilizadas por diferentes empresas del sector productivo.

Fuente:

Comunicaciones del CEFOP: Centro de Óptica y Fotónica: http://www.cefop.cl/noticias/destacados/

S. Etcheverry, G. Cañas, E. S. Gómez, W. A. T. Nogueira, C. Saavedra, G. B. Xavier & G. Lima, "Quantum key distribution session with 16-dimensional photonic states", *Scientific Reports* **3**, Article number: 2316 doi:10.1038/srep02316 En: http://www.nature.com/srep/2013/130730/srep02316/full/srep02316.html

Más información en:

"Informe de amenazas de seguridad", Sophos. En: http://www.sophos.com/es-es/medialibrary/PDFs/other/SophosSecurityThreatReport2012.pdf

Otros Artículos de Ciencia

- ¿Cómo estimular la generación de nuevas neuronas?
- Articulo 2
- Nota de prensa de prueba: estudio sobre comportamiento.
- ESO: un peso pesado intergaláctico
- 5º concurso nacional de centros en investigación FONDAP 2013
- Llega la nieve al desierto de Atacama
- ALMA reescribe la historia del "Baby Boom" estelar del universo
- Científicos de la Usach lideran investigaciones sobre efectos del cambio climático en la Antártica
- La extraña pareja: Dos nubes de gas muy diferentes en la galaxia de al lado
- Variaciones del Pacífico repercuten en la nieve de Los Andes del centro-norte chileno
- ALMA capta en detalle el dramático nacimiento de una estrella
- Nueva teoría para modelar oleaje aplicada a la erosión de sedimentos
- Expedición científica logra llegar a la cima del Monte Sarmiento en Tierra del Fuego
- Astrónomos descubren que agujero negro de la Vía Láctea expulsa gas, en vez de atraerlo
- Científicos chilenos innovan en criptografía de última generación

Copyright © 2012 Infocyt