TRIBUNA COMPLUTENSE

19 de abril de 2013 **Universidad Complutense de Madrid** Número 135

Una universidad cada vez más internacional

De todos los continentes y prácticamente de todos los países. Este año la presencia de estudiantes extranjeros supera el 11,5 por ciento del total de los que estudian en la Universidad Complutense.

J. DE MIGUEL

FEDERICO MAYOR ZARAGOZA DENUNCIA LA PLUTOCRACIA QUE NOS GOBIERNA Y LA FALTA DE DEMOCRACIA QUE HAY TANTO EN NUESTRO PAÍS COMO EN LA UNIÓN EUROPEA

Ciencia

El futuro de la información pasa por una distribución de claves más segura

▶ LA REVISTA ***SCIENTIFIC REPORTS*** DE PRINCIPIOS DE ABRIL ACABA DE PUBLICAR EL TRABAJO SOBRE CLAVES CUÁNTICAS REALIZADO POR **DAVID ELKOUSS**, POSDOC DE LA **FACULTAD DE MATEMÁTICAS DE LA COMPLUTENSTE**, Y POR LOS INVESTIGADORES DE LA POLITÉCNICA DE MADRID **JESUS MARTINEZ-MATEO** Y **VICENTE MARTÍN**

El trabajo lleva por título "*Key Reconciliation for High Performance Quantum Key Distribution*". Como es algo que puede sonarle extraño a la mayor parte de los lectores, lo primero que le preguntamos a David Elkouss es qué es exactamente eso de la Distribución Cuántica de Claves (QKD).

En el mundo actual la mayor parte de la información se transmite de manera digital. Una de las claves de esa información en red es que exista una confidencialidad entre el emisor y el receptor, para lo que hacen falta claves que sólo ellos dos conozcan y no permitan que terceros accedan a los datos privados. Los métodos de encriptación cada vez son más complejos, pero el más seguro de todos depende de la QKD. Esta permite explotar las propiedades de la mecánica cuántica para distribuir con seguridad claves electrónicas entre dos partes. Lo que diferencia a la QKD de la distribución tradicional de claves es que con la versión cuántica se pueden crear claves seguras, con independencia de los avances tecnológicos que se hagan en los próximos años.

Como asegura Elkouss, se trabaja para que ni siquiera los futuros ordenadores cuánticos sean capaces de descubrir las claves privadas y que la información siga siendo segura. Se supone que con esos ordenadores "toda la criptografía actual sería crackeable. Para contrarrestar ese tipo de ataques que se cree que ocurrirán en algún momento de los próximos 15 o 20 años está la criptografía cuántica".

Explica Elkouss que clásicamente se conoce cómo cifrar algo para que nadie sea capaz de descifrarlo. "Con un texto se crea una clave totalmente aleatoria de una misma longitud. Se usa una sola vez y eso es totalmente imposible de descifrar". El problema

LA VENTAJA DE LA DISTRIBUCIÓN CUÁNTICA DE CLAVES (QKD) ES QUE SERÁ UN MÉTODO SEGURO, CON INDEPENDENCIA DE LOS AVANCES TECNOLÓGICOS

está en conseguir que tanto el emisor como el receptor tengan esa misma clave para descifrar el texto usándola una única vez, y que para cada texto haya una clave distinta. El problema, por tanto, está en "la distribución de claves, y eso es lo que resuelve la criptografía cuántica".

DE TELECO A MATEMÁTICAS

David Elkouss es "teleco" de formación por la Politécnica de Madrid. Después de eso se trasladó a París a hacer un doble diploma, lo que permite obtener el título de dos universidades al mismo tiempo. Allí, un profesor propuso hacer un trabajo sobre corrección de errores clásica, que es lo que más le interesaba a Elkouss ya desde la ingeniería.

En los protocolos de QKD, después de la parte cuántica "hay ciertos errores porque los dispositivos que los implementan no son perfectos y hay que corregirlos". Cuando se corrigen los errores, "se da información adicional, es decir, se da una cierta redundancia que permite a la otra parte corregir

EN LA ACTUALIDAD LA QKD SE UTILIZA ESENCIALMENTE PARA DEMOSTRACIONES AUNQUE YA SE HA USADO DE MANERA PRÁCTICA EN VARIAS OCASIONES

los errores". El problema es que todo eso que se comparte al final reduce la clave secreta entre las dos partes. El objetivo, por lo tanto, es hacer una corrección de errores que "sea lo más eficiente posible, que revele el mínimo de información y que haga que no desaparezca la clave secreta".

EL USO DE LA QKD

Elkouss explica que en la actualidad la Distribución Cuántica de Claves se utiliza "esencialmente para demostraciones", aunque también ha tenido algunos usos prácticos. Se usó durante el Mundial de Fútbol de Sudáfrica, en unas votaciones en un cantón de Ginebra y también se ha utilizado en el Metro de Boston.

En la Universidad Complutense, Elkouss está realizando un posdoc con el profesor David Pérez García. Está inmerso "en un proyecto de composición de canales cuánticos, para saber qué ocurre si se compone en paralelo o secuencialmente, porque todavía no se sabe muy bien cómo de mejor es un canal cuántico con respecto a uno clásico; aún hay muchas cosas por saber".

En el artículo publicado en *Scientific Reports* se habla de la eficiencia de los sistemas QKD, del interés de usar códigos más cortos y menos complicados. Cuenta Elkouss que la nueva generación de dispositivos cuánticos "son muy rápidos, así que quizás lo más importante no es medir la eficiencia, sino la rapidez en equipos reales".

De acuerdo con el investigador, "es muy complicado hallar un código que es básicamente una aplicación que transforma un paquete pequeño de datos en uno más grande que se puede enviar de manera fiable a pesar de que haya un cierto error en el canal de comunicaciones". Los códigos

Texto: Jaime Fernández / Fotografía: J. de Miguel

David Elkouss, posdoc en la Facultad de Matemáticas de la UCM, investiga cómo distribuir claves más seguras

PARA SABER UN POCO MÁS

La UCM y la computación cuántica

La Complutense es la coordinadora del consorcio científico QUITEMAD, que se creó en 2009 y que abarca cinco áreas de investigación cuántica: criptografía, computación, control y tomografía, correlaciones y simulación. Por parte de la UCM, forman parte de QUITEMAD el Grupo de Información y Computación Cuánticas, y el de Matemática e Información Cuántica, al que está adscrito David Elkouss.

El objetivo final de conseguir un ordenador cuántico, capaz de realizar cálculos numéricos complicados y hacer búsquedas en las bases de datos cada vez mayores todavía es algo lejano. Ignacio Cirac, director del Instituto Max Planck de Óptica Cuántica, y licenciado en la Facultad de Físicas de la UCM, asegura que "la computación cuántica progresa de manera continua, pero todavía falta mucho tiempo para que podamos construir un ordenador cuántico lo suficientemente potente. La simulación cuántica progresa mucho más rápidamente, y ya hay experimentos que dicen que pueden hacer simulaciones que son imposibles con ordenadores clásicos".

Sin duda, el avance más relevante que ha dado la investigación en información cuántica es la criptografía cuántica, ya comercializada.

utilizados en su investigación son diseñados mediante "unos algoritmos genéticos que buscan en el espacio de códigos y seleccionan aquellos con mejor comportamiento asintótico". Con cada uno de esos códigos se hacen simulaciones, aplicando el tipo de error que se piensa que tendrá el canal cuántico, y luego se ve si el sistema lo decodifica bien o no. Esto que así expresado parece sencillo, en realidad es bastante intensivo, porque hay que hacer "millones de simulaciones dependiendo de la precisión que se busque o del error que se piensa que vas a tener".

Para estos estudios no es necesario utilizar simuladores cuánticos o dispositivos de QKD (que hoy en día ya comercializan unas pocas empresas), sino que se pueden utilizar ordenadores convencionales. Elkouss reconoce que a veces se han planteado utilizar algún supercomputador que les permita afinar los métodos de corrección, pero el objetivo es que el hardware utilizado sea simple y así conseguir que los dispositivos sean accesibles al público más amplio posible. ■