

Garantizado con fotones

Un físico de la UPC descubre cómo reforzar la seguridad de las transacciones por internet

PERFIL

Quebraderos de cabeza cuánticos

“Al principio no me gustaba nada la física cuántica”, reconoce Gabriel Molina Terriza (Ciudad Real, 1975). Sus principios antiintuitivos le desconcertaban. Pero después de licenciarse en Física en la Universitat de Barcelona y hacer el doctorado sobre fotónica clásica en la Universitat Politècnica de Catalunya, “se nos ocurrió que la física cuántica ofrecía muchas posibilidades con los fotones y me empecé a interesar”. En el 2002 consiguió un contrato en el Instituto de Física Experimental de la Universidad de Viena (Austria), donde trabaja un grupo líder en criptografía cuántica y donde hizo gran parte del trabajo publicado ahora. El año pasado se reincorporó al Institut de Ciències Fotòniques (ICFO) de la UPC. ¿Y cómo va su relación con la física cuántica? “Ahora encuentro que incluso se puede explicar”.



Gabriel Molina Terriza, ayer en el laboratorio del Institut de Ciències Fotòniques de la UPC

JOSEP CORBELLA
Barcelona

Se puede jugar a cara o cruz por teléfono? “Si yo lanzo la moneda en mi casa, tú dices cara y yo te digo que ha salido cruz, ¿cómo puedes saber si te he engañado?”, explica Gabriel Molina Terriza, físico del Institut de Ciències Fotòniques (ICFO) de Barcelona. Y sin embargo se puede. No se juega por teléfono, sino por ordenador y no con monedas sino con fotones, pero se puede jugar de modo que los dos jugadores sepan si el otro le engaña, según ha demostrado Molina Terriza.

La investigación, que resuelve un problema que se resistía a los investigadores desde 1981, puede ser útil en situaciones en que dos personas hagan intercambios a distancia y desconfíen una de otra. La más inmediata son los casinos virtuales: ¿cómo jugar al póquer por internet y saber que otro jugador no nos engaña cuando dice que le ha salido un póquer de ases? Pero hay otras: la firma de un contrato a distancia, donde uno debe asegurarse de que no le van a cambiar las condiciones del contrato una vez ha firmado; o los correos electrónicos en los que hay que tener garantías de que los ha enviado quien los firma; o las compras por internet.

Los resultados de la investigación se publicaron la semana pasada en *Physical Review Letters*, la revista de física más importante del mundo, en un artículo titulado *Lanzamiento de monedas cuántico experimental*. Las revistas científicas *Nature* y *Science* han destacado esta semana el trabajo de Molina Terriza como un gran avance en el campo de la criptografía cuántica.

Para comprender cómo se hace un lanzamiento de monedas cuántico, primero hay que hacer

Nature y Science destacan la investigación de Molina Terriza como un gran avance en criptografía cuántica

un acto de fe. Hay que aceptar que dos fotones, alejados uno de otro, están de algún modo entrelazados: si cambian las propiedades de un fotón, cambian al instante las propiedades del otro. Es como si los fotones fueran novios: incluso cuando no están juntos, el comportamiento de uno está relacionado con el comportamiento del otro. Esta propiedad de la física cuántica, que desafía el sentido común porque nadie sabe de qué modo un fotón puede afectar a otro a dis-

tancia, ha sido comprobada en miles de experimentos. En la investigación de Molina Terriza, la persona A (conocida como Alice en el mundillo de la criptografía cuántica) lanza al aire un par de fotones. Uno de los dos se envía a la persona B (conocida como Bob). El otro se lo queda Alice. Alice ya sabe en ese momento en qué estado se encuentran los fotones, que pueden estar –metafóricamente– en cara o en cruz.

Debido al noviazgo entre los fotones, Bob no tiene modo de saber en qué estado se encuentra su fotón sin conocer el estado del de Alice, que aún no le ha llegado. En ese momento, Bob hace su apuesta. Pongamos que dice cara. Alice, que ya sabe en ese momento si Bob ha acertado o no, le dice entonces en qué estado está su fotón para que Bob pueda comprobar si ha acertado.

La investigación demuestra por primera vez que es posible reforzar la seguridad de las transacciones mediante la criptografía cuántica. Pero aún “la técnica aún no está a punto para aplicarla a gran escala”, advierte Molina Terriza. “Hay problemas que aún no están resueltos”. Falta, sobre todo, poder conservar los fotones sin que se modifiquen durante todo el proceso y poder enviar fotones sin que se modifiquen a grandes distancias para garantizar las transacciones entre personas que se encuentran en ciudades o países distintos.●

CIENCIA

La inversión del superordenador Mare Nostrum asciende a 113 millones

MADRID. (Redacción.) – El proyecto del superordenador Mare Nostrum, instalado en Barcelona, supondrá una inversión total de 113,3 millones de euros. El Consejo de Ministros aprobó ayer la constitución del consorcio de gestión de una de las supercomputadoras más potentes del mundo, en el que participarán el Ministerio de Educación y Ciencia, la Generalitat de Catalunya y la Universitat Politècnica de Catalunya. A los 70 millones que el Gobierno pagó a IBM por la adquisición de Mare Nostrum se unen ahora los 43,3 millones de euros necesarios para la explotación de la máquina, en la que podrán trabajar simultáneamente equipos investigadores de distintas disciplinas.

De esos 43,3 millones de inversión, Educación y Ciencia aportará casi 27,3 millones de euros, mientras que la Generalitat se hará cargo de los restantes 16 millones. El consorcio estará encargado de “gestionar la creación construcción, equipamiento y explotación del Barcelona Supercomputing Center-Centro Nacional de Supercomputación (BSC-CNS)” que albergará el Mare Nostrum. La inauguración oficial del superordenador está prevista para el próximo 23 de febrero, aunque, según el Gobierno, llegará a su plena operatividad “la próxima primavera”.

Con una capacidad de realizar 40 billones de operaciones en un solo segundo, Mare Nostrum será usado en estudios relacionados con el genoma humano, la realización de simulaciones y predicciones climáticas, aplicaciones de la industria aeroespacial, automovilística y farmacéutica. Funciona con el sistema Linux y cuenta con 4.564 procesadores. Podrá alcanzar una capacidad de procesamiento de datos muy elevada, con un pico de 40 teraflops, el equivalente a las operaciones que una persona con calculadora tardaría en resolver más de un millón de años.●

Europa estudia lanzar vuelos tripulados desde la base espacial de Guayana

Viene de la página anterior

lanzamientos. Según la Agencia Espacial Europea, es “la base mejor situada del mundo”. Al encontrarse a una latitud de sólo 5 grados al norte del ecuador, los cohetes que despegan de Kurú pueden situar satélites en órbitas ecuatoriales con un consumo de combustible mínimo. Por el contrario, los que despegan de Cabo Cañaveral en Estados Unidos, a una latitud de 28°N, o de Baikonur en Kazajistán, a 46°N, necesitan más combustible para corregir su trayectoria y situarse sobre el ecuador. O lo que es lo mismo: desde Kurú se pueden lanzar satélites más grandes que desde Cabo Cañaveral o desde Baikonur para un cohete de potencia igual.

Además, al encontrarse en la costa este de Sudamérica, la base de

La industria espacial europea se juega hoy parte de su futuro en el lanzamiento del nuevo Ariane 5

Kurú permite lanzar cohetes en dirección al mar –puesto que por norma se lanzan hacia el este aprovechando la rotación de la Tierra– y, por lo tanto, sin riesgo de que causen daños en zonas habitadas si falla algo en el lanzamiento.

En Kurú toda la atención se concentra esta semana en el llamado *Ariane 5 pesado* que, salvo contratiempos de última hora, despegará esta tarde con dos satélites a bordo

y del que depende el futuro a corto plazo de la industria espacial europea. El cohete incorpora dos grandes novedades para hacerlo más potente que su predecesor, el *Ariane 5 genérico*. Si el cohete utilizado hasta ahora puede situar satélites de hasta 6 toneladas en órbita geoestacionaria –la órbita en la que deben situarse los grandes satélites de telecomunicaciones, situada a 36.000 kilómetros de altitud sobre el ecuador–, el nuevo Ariane 5 puede lanzar cargas de hasta diez toneladas.

La principal novedad es un nuevo motor situado en la base del gran cilindro central del cohete y que propulsa el aparato en los minutos iniciales de vuelo. Este nuevo motor, el Vulcain 2, falló en su primer lanzamiento el 11 de diciembre del 2002 debido a que la tobera –el tubo de escape del cohete– se deformó al no resistir las altas temperaturas de los gases que salían del motor. Al ver que el cohete había entrado en una trayectoria errática, el director de operaciones del centro de control de Kurú pulsó el botón que le daba la orden de autodestruirse.

La otra gran novedad es un segundo motor situado a media altura en el cilindro central del cohete que de-

EL DATO

Un satélite español a bordo

■ El Ariane 5 que está previsto lanzar esta noche desde Guayana lleva a bordo el satélite militar español Xtar-Eur, que inaugura el nuevo programa español de comunicaciones gubernamentales por satélite. El Xtar-Eur, de 3.616 kilos, debería permanecer operativo hasta el 2019. El programa se completará con un segundo satélite, el Spainsat, que se lanzará dentro de alrededor de un año. Entre ambos triplicarán la capacidad actual de comunicaciones por satélite del ejército español.

be encenderse cuando el primer motor se apague. Este segundo motor funcionó con éxito en más de 130 lanzamientos del Ariane 4, un cohete ya jubilado, y nunca se ha probado hasta ahora en un Ariane 5.

De cara al futuro, informa Fer-

nando Doblas, la ESA estudia la posibilidad de cambiar este segundo motor por uno más avanzado para ganar en potencia y, sobre todo, en versatilidad. “Podríamos subir de 10 a 12 toneladas, pero lo que más nos interesa es la posibilidad de encender y apagar el motor varias veces durante el vuelo” para poder insertar los satélites en órbita de manera más eficiente.

También está en estudio la posibilidad de empezar a lanzar vuelos tripulados desde Kurú, no con los Ariane 5 –puesto que no se han desarrollado para misiones tripuladas– sino con los Soyuz. Desde el accidente del transbordador Columbia de la NASA, los Soyuz se han convertido en el vehículo habitual de los astronautas que despegan rumbo a la estación espacial desde Baikonur. Aunque por ahora no hay ningún acuerdo entre la agencia espacial europea y la rusa para que los Soyuz de Kurú despeguen con astronautas a bordo, “vamos a construir la zona de lanzamiento de modo que, si algún día se deciden lanzar vuelos tripulados, se pueda hacer sin cambiar casi nada”, declara Doblas. ¿Cuándo podría ser eso? “No antes del 2010”.●