El País, 16 de agosto de 2001
CiberPaís, Única, pág. 8 - Noticias
INVESTIGACIÓN
JOAN CARLES AMBROJO El matemático Sandu Popescu aporta sus teorías, que la empresa aplica en informática y comunicaciones

Hewlett-Packard utiliza la física cuántica para crear firmas digitales

Desintegrar una persona y replicarla en otro lugar en un instante es algo que hacen rutinariamente en la serie *Star Trek*. En la realidad esto es imposible. Como mucho, los científicos han conseguido teletransportar un fotón, una partícula elemental, refrendando las teorías de la mecánica cuántica.

Investigadores de Hewlett-Packard y otras compañías informáticas están desarrollando sistemas que permitan emplear los fenómenos de la física cuántica en aplicaciones de comunicaciones y sistemas criptográficos comerciales. La mecánica cuántica es la teoría que describe el comportamiento de las partículas elementales (electrones, átomos, fotones, etcétera). Por ejemplo, una partícula microscópica puede estar simultáneamente en dos lugares, y dos partículas muy alejadas, comunicarse instantáneamente.

"Obviamente, compañías como Hewlett-Packard están buscando aplicaciones prácticas de la informática cuántica, gracias a la unificación de las tecnologías de la información y la mecánica cuántica", afirma el científico rumano Sandu Popescu, matemático que trabaja en los laboratorios BRIMS de HP y en las universidades de Bristol y Cambridge. La teleportación es, por ahora, una quimera. La creación de firmas digitales basadas en la física cuántica tiene grandes visos de ver la luz. Según Popescu, la aparición de sistemas de cifrado cuánticos es una cuestión más de mercadotecnia que de tecnología. ¿Una firma digital que funciona a través de fotones? No es ninguna fantasía de ciencia-ficción. Los tradicionales sistemas de cifrado no son completamente seguros.

Descubrirlos es una cuestión de tiempo y potencia de cálculo. Los investigadores piensan que, utilizando fotones (partículas de la luz), es posible crear mensajes que sean imposibles de interceptar. Y si alguien trata de averiguar el contenido de un mensaje, el código desaparece misteriosamente ante el intruso.

Popescu, que fue galardonado en marzo con el Adams Prize por sus aportaciones en informática cuántica, ha desarrollado las teorías del enmarañamiento y no localización de las partículas.

Ordenadores cuánticos

El investigador rumano no trabaja con tubos de ensayo, pero cree que los físicos dedicados a la construcción de un ordenador cuántico lo conseguirán tarde o temprano. "Está probado teóricamente", asegura.

Un ordenador cuántico no funcionará como un ordenador ordinario, pero sí más rápidamente. "La tecnología de silicio actual tan sólo está mejorando la velocidad de cálculo. Sería como escribir unas cifras en la pizarra de igual forma pero más rápidamente". Un ordenador cuántico

lo haría de otra manera. "Aparentemente, puede tener muchas ventajas, porque hay formas en las que podemos resolver problemas que son más eficientes que los de las matemáticas tradicionales; uno de estos problemas importantes es la factorización [proceso que permite descomponer en factores una expresión numérica] de los números. Por ejemplo, 6 = 2 x 3. Pero cuando se tiene un número muy largo es necesario realizar muchos cálculos para descomponerlo, y el tiempo necesario depende de la rapidez con la que se trabaja. Pero los pasos de computador que se necesitan llevar a cabo son fijos y vienen dados por las matemáticas, por cómo se multiplica, divide o suma".

El ordenador cuántico puede reducir el número de pasos requeridos y trabajar con problemas más complejos, factorizar números más y más largos. Otra cosa es la transmisión de la información, como antes se ha indicado; cuando dos partículas se relacionan y se las aleja, continúan estando en comunicación entre ellas. LABORATORIOS HP BRIMS: http://www-uk.hpl.hp.com/brims/