

La revolución informática

Dentro de veinte años los chips de los ordenadores serán tan pequeños que los efectos de la mecánica cuántica reemplazarán a las leyes físicas que ahora damos por sentadas. Mientras que hoy en día los ordenadores se basan en bits que toman los valores cero o uno, la unidad básica de la informática cuántica es el bit cuántico, el *qubit*, que puede valer cero y uno simultáneamente (con una probabilidad asociada a cada uno de estos valores). En el mundo extraño de la informática cuántica, procedimientos tan complicados como la factorización de números grandes se hacen mucho más rápidamente, porque la ingente cantidad de pasos necesarios se realizan de forma concurrente. La meta última de los matemáticos, físicos, informáticos e ingenieros en este campo es crear un ordenador cuántico que pueda solucionar en segundos ciertos problemas que a los más potentes ordenadores actuales les llevaría millones de millones de años resolver.

Entre las capacidades de un ordenador cuántico estaría la habilidad de hacer los cálculos necesarios para acabar con los métodos de encriptación electrónicos actuales. Esto no es tan alarmante como pudiera parecer, puesto que los criptógrafos ya han diseñado algoritmos que sacan partido de un principio de la mecánica cuántica que enuncia que la mera observación del estado de un sistema lo modifica. Por lo tanto, los usuarios de una red de comunicaciones cuántica podrían detectar cualquier intento de intrusión. Resulta irónico que las mismas leyes que gobiernan la barrera hacia la miniaturización de los ordenadores actuales puedan ser de gran ayuda para el futuro de la informática.

Más Información:

"Rules for a Complex Quantum World". Michael A. Nielsen. *Scientific American*, November 2002.



Imagen cortesía de MITRE Corporation.



El programa **Momentos Matemáticos** promueve la apreciación y el conocimiento del papel que desempeñan las matemáticas en la ciencia, la naturaleza, la tecnología y la cultura.

www.ams.org/mathmoments

Versión en español de

www.matematicalia.net
REAL SOCIEDAD MATEMÁTICA ESPAÑOLA



matematicalia

revista digital de divulgación matemática

