El problema de Simon*

José María García Rubira

9 de julio de 2007

Todo el mundo ha oído hablar alguna vez del criptosistema de clave pública RSA. Su fuerza reside en la dificultad de factorizar números grandes con los ordenadores de hoy día. Sin embargo la próxima llegada de los ordenadores cuánticos ha puesto en peligro la seguridad del RSA.

De hecho, se puede considerar que todos los ordenadores actuales son, en realidad, cuánticos; el funcionamiento de los chips se basa en las propiedades cuánticas de la materia. Sin embargo, su diseño sigue los conceptos "clásicos" formulados por Turing y Von Neumann. El término "ordenador cuántico" hace referencia a aquel ordenador que utiliza como unidad de computación los estados cuánticos, el más común de los cuales es el "quantum bit" o "qubit". Los clásicos bits de información pueden tomar el valor 0 o 1; un qubit almacena la información en el estado de un átomo. Las propiedades del átomo posibilitan que este no tenga porque ser 0 o 1, sino que puede ser una mezcla de los dos a la vez (este hecho está relacionado con la interpretación de Copenhague del principio de incertidumbre de Heisenberg y la paradoja del gato de Schrödinger). De este modo se puede tratar la información de una sola vez.

La clave de los ordenadores cuánticos se basa en el hecho de que la utilización de los estados cuánticos permitiría, además de simular cualquier ordenador clásico, la utilización de nuevos algoritmos de gran potencia; es decir, la capacidad de resolver problemas que necesitan un elevado número de cálculos en un tiempo muy pequeño.

*Comentario sobre la charla de ALAIN VERSCHOREN "Códigos públicos y ordenadores cuánticos" impartida en el Seminario de Álgebra de la Universidad de Almeria, el 18 de junio de 2007. Publicado en el blog de UALMAT el 9 de julio de 2007, http://ualmat.wordpress.com.

Uno de los primeros algoritmos cuánticos en desarrollarse fue el algoritmo de Shor, que es capaz de descomponer un número N en tiempo $O((\log N)^3)$. El algoritmo que se explicó en la conferencia está relacionado con el llamado problema de Simon. El algorítmo de Simon es un algoritmo cúantico probabilístico que resuelve el problema de la determinación del período de una función periódica $f : \{0,1\}^n \to \{0,1\}^m$ (el problema de la factorización se puede reducir a este último) mediante la evaluación de f un número de veces de orden n (clásicamente, es necesario evaluar la función un número de veces exponencial en n).

La implicación de estas técnicas teóricas es la vulnerabilidad de la información protegida en la actualidad por métodos tipo RSA desde el día en que se encienda el primer ordenador cuántico. Afortunadamente, el uso de ordenadores cuánticos permitirá también el uso de sistemas de protección prácticamente infalibles: la criptografía cuántica. Pero esa es otra historia.

Más información:

1. **Quantum Computation and Quantum Information**, Michael A. Nielsen y Isaac L. Chuang, *Cambridge University Press, 2004*

2. **Los códigos secretos: el arte y la ciencia de la criptografía, desde el antiguo Egipto a la era Internet**, Simon Singh, *Editorial Debate, 2000*

3. http://www.qubit.org/

4. http://www.rsa.com/rsalabs/node.asp?id=2353

5. http://www.wikipedia.org