Factorització amb ordinadors quàntics

El treball de Peter Shor

La informació següent es va difondre com una nota de premsa, datada el 18 d'agost de 1998, durant el Congrés Internacional de Matemàtics a Berlín.

Ara fa exactament quatre anys que el matemàtic Peter Shor va fer públic el seu algoritme per factoritzar nombres grans mitjançant ordinadors quàntics. Els seus descobriments varen tenir ressò arreu del món. Gràcies a la seva feina d'investigació en els Laboratoris AT&T, Shor va poder demostrar que els ordinadors d'aquesta nova generació desxifrarien amb molta facilitat tots els codis que s'utilitzen actualment. Aquest anunci va inquietar tots aquells que proclamaven la seguretat que ofereixen els mètodes vigents de xifratge, com l'RSA, que va sorgir el 1977 gràcies a Ronald Rivest, Adi Shamir i Leonard Adleman, i que utilitzen des de les entitats financeres fins als usuaris de la Internet.

Els resultats de Shor varen provocar una reacció immediata dels físics i els informàtics. Grups d'investigació de tot el món varen plantejar-se seriosament la tasca de construir ordinadors quàntics, que l'any 1994 tan sols existien en els estudis teòrics. Només als Estats Units, els instituts de recerca estan gestionant projectes sobre aquest tema amb un pressupost total de més de 1.500 milions de pessetes. Ha nascut una nova especialitat científica, la *informàtica quàntica*, en la qual col·laboren els físics quàntics i els informàtics teòrics.

En aquests moments, els ordinadors quàntics es troben en fase de prototips. Aquests ordinadors calculen fent servir els estats quàntics dels àtoms, la qual cosa els permet processar molta més informació que els ordinadors tradicionals. L'abril de 1998, investigadors d'IBM, del MIT, de la Universitat de Califòrnia a Berkeley i de la Universitat d'Oxford varen anunciar que havien construït un petit ordinador quàntic que feia servir cloroform. Un altre grup de recerca, a Innsbruck, està fent experiments amb trampes d'ions. Tanmateix, els experts opinen que encara hauran de passar ben bé dues dècades abans que al món hi hagi ordinadors quàntics en condicions de funcionament. Els científics encara han de resoldre un bon nombre de problemes seriosos, com l'estabilització dels errors i el control dels estats quàntics en aquests ordinadors nous. Tanmateix, Peter Shor també ha fet propostes fonamentals en aquestes direccions.

La informàtica quàntica combina mètodes matemàtics amb les lleis de la física quàntica. Amb això pretén oferir solucions ràpides a molts problemes que els ordinadors tradicionals no han pogut resoldre de manera eficient. Els sistemes de xifratge actuals s'aprofiten d'alguns d'aquests problemes. Per exemple, el mètode RSA es basa en el fet que els ordinadors convencionals tarden massa a descompondre en factors primers els nombres molt grans. Shor ha demostrat que és possible programar un ordinador quàntic de manera que factoritzi nombres d'una manera eficient. De fet, ha creat un nou principi algorítmic amb aquest objectiu, que s'anomena *paral·lelisme quàntic*. Per tal de descompondre nombres grans en factors primers, fa servir la transformació de Fourier quàntica i agrupa els passos del procés en transformacions parcials apropiades.

Malgrat que els ordinadors quàntics encara no amenacin realment els sistemes de seguretat, els especialistes en codificació ja estan pensant com crear sistemes nous. Els codis secrets que s'utilitzen actualment tenen un inconvenient: no es pot demostrar de manera precisa el nivell de seguretat que ofereixen. Se'ls fa segurs a base d'anar allargant les claus públiques, per tal de mantenir-les fora de l'abast dels delinqüents. A mesura que augmenta la rapidesa dels ordinadors, també va augmentant la mida dels codis, però això no elimina la seva debilitat principal. En contrast amb aquest fet, la informàtica quàntica promet la seguretat total. El fonament d'aquesta afirmació rau en els mateixos principis de la física quàntica: els impulsos elèctrics que es transmeten per cables de fibra òptica no es poden interceptar sense alterar la informació que transporten les partícules i fer detectable la intromissió.

Traducció: Carles Casacuberta
Universitat Autònoma de Barcelona