Juan Ignacio Cirac

Max Planck Institutuko Optika Kuantikoaren Zentroko fisikaria

ARGAZKIAK: JON URBE/ARGAZKI PRESS

Guillermo Roa Zubia
Elhuyar Zientziaren Komunikazioa

“Ordenagailu kuantiko bat egiten den unetik, modu bakarra egongo da informazio sekretua bidaltzeko”

Juan Ignacio Cirac oso argi mintzatu da: fisikari kuantikoen etorkizunerako proiekzioa ordenagailu kuantikoz beteta dago. Oso makina ahaltsuak izango direla esaten du, kodetutako edozein informazio deskodetzeko ahalmena izango dutelako. "Ez bada kodetze-sistema bera ere fisika kuantikoa erabiliz egiten", esan du. Enkriptazio kuantikoa existitzen da, eta, ustez, hori erabiliz baino ezin izango zaio aurre egin ordenagailu kuantikoen ahalmenari. Oso kontu zirraragarria da fisikari batentzat; horregatik, Juan Ignacio Ciracek bietan egiten du lan, ordenagailu eta enkriptazio kuantikoak garatzen.

Ez da ohikoa fisika kuantikoan ikertzen ari den pertsona bat aplikazioen mundura begira egotea. Ciracek horixe bilatu zuen, eta argi dago ondo aritzen dela, nazioarteko ospea duelako. Sari asko eta asko ditu, tartean Príncipe de Asturias, eta Thomson Reuters aholkularitza-enpresak Fisikako Nobel saria irabazteko hautagaitzat hartu du. Auskalo.

Sari asko jasotzeak esan nahi du ikerketa-esparrua bera garrantzitsua dela saria ematen duenarentzat. Zure kasuan hala da?

Bai, bai. Ni esparru honetan aspaldi hasi nintzen. Eta garai hartan ez zuten saririk ematen; oso jende gutxik egiten zuen lan horretan, eta oso esparru exotikoa zirudien. Denborarekin, jendea konturatu da etorkizun handiko esparrua dela, eta, ikerketa horretan, fisikariak ez ezik, kimikariak, matematikariak, informatikariak eta beste arlo batzuetako zientzialariak ere elkartu dira. Zientziaren barruko esparru handia bilakatu da. Eta nolabait aitzindariak izan ginenoi egokitu zaigu sariak jasotzea.

Max Planck Institutuko Optika Kuantikoaren Zentroko sail baten burua zara. Lanpostuak fisika egiteko denbora asko uzten dizu?

Ba, zorionez, horretarako aukera ematen dit. Hain zuzen ere, institutu horrek eskaintzen duen gauzetako bat da, eta hori izan zen hona etortzeko arrazoietako bat. Oso administrazio ona dugu, oso eraginkorra; ia lan administratibo guztia kentzen digute.

Juan Ignacio Cirac

Manresan jaio zen, 1965ean. Madrilera joan zen Fisika ikastera. Karreraren bigarren mailan zegoela, Ingeniaritza Industrialean ere matrikulatu zen, eta bi ikasketak egin zituen aldi berean. Baina fisikaren aldeko apustuak irabazi zuen, Ciracek fisika kuantikoa aurkitu zuenean. Esparru horretako ikerketa izan da bere bizimodua eta pasioa, eta izen handienetako bat bilakatu da. Gaur egun, Max Planck Institutuko Optika Kuantikoaren Zentroan egiten du lan, Garching hirian, Alemanian; han, Fisika Teorikoaren Sailaren zuzendaria da.

Konputazio kuantikoan eta enkriptazio kuantikoan aritzen zara. Bietan.

Nire esparrua informazio kuantikoa da, eta horren barruan biak daude sartuta. Konputazioari lotutako ezaugarri batzuk ditu, kriptografiari lotutako beste ezaugarri batzuk ere bai, baita komunikazioarekin edo simulazioarekin lotutakoak ere; eta dena sartzen da fisika kuantikoan. Horregatik egiten dut lan kriptografian, ordenagailuetan, simulazioan eta beste hainbat gauzatan.

Baduzu arlo bat bestea baino gustukoago?

Egunaren arabera. Aldi bereko proiektu asko ditugunez, batzuetan batzuk dira interesgarriagoak, zirraragarriagoak, edo aurkikuntza bat egiten dugu… Azkenaldian egindakoen arabera ditut lehentasunak.

Ustez, ordenagailu kuantikoek informatikaren iraultza ekarriko dute, baina ez dira errazak egiteko. Erronka handiagoa da fisikarentzat informatikarentzat baino?
Erronka bat baino gehiago dago. Erronka nagusia da nahi dugun potentziako ordenagailu kuantiko bat egitea. Oraingoz, ezin dugu prototipo txikiak besterik egin, eta horrek esan nahi du lege fisikoak ondo ezagutzen ditugula, badakigula nola egin behar den, eta pentsatzen ditugun gauzak zuzenak direla. Baina garapen teknologiko baten faltan gaude ordenagailu kuantiko handi bat egiteko. Agian, luze joko digu hori lortzeak; hamar, hamabost, hogei, berrogei, berrogeita hamar urte izan daitezke. Dena dela, beste aplikazio batzuetarako ez da hain ordenagailu kuantiko handia egin behar. Aplikazio horietan ere egiten dugu lan, epe laburrago batean.

Albisteen arabera, ordenagailu kuantikoren bat eginda dago.
Prototipo txikiak dira, eta ez dituzte fisika kuantikoak posible egiten dituen adinako kalkuluak egiten. Guk qubitekin egiten dugu lan, ohiko informatikaren biten baliokideak. Ordenagailu kuantiko bat potentzia handikoa izateko, milioi bat qubit izan beharko lituzke, gutxi gorabehera. Oraingoz, 14 qubiteko ordenagailu bat egitea lortu da; beraz, badugu bide luze bat aurretik, baina 14 qubit horiekin badakigu nola egin kalkulu kuantiko batzuk, eta frogatu dugu gauzek funtzionatzen dutela.

"Ordenagailu kuantiko batek milioi bat qubit izan behar ditu, gutxi gorabehera. Oraingoz, 14 qubitekoa egitea lortu da."

Bihar milaka qubit elkartzeko modua izango bagenu, eta etzi funtzionatzen jarri ahal izango bagenu, prest egongo ginateke orain ordenagailu horiek erabiltzeko?
Bai, bai... Noski, informatika kuantikoaren arloa garatu behar da oraindik. Algoritmo asko eta softwarea oraindik garatzeko daude. Baina orain ordenagailu kuantiko bat izango bagenu, etekin handia aterako genioke. Batez ere simulazio kuantikoak egin ahal izango genituzke, eta horrek materialen diseinuan lan egiteko aukera emango liguke. Baita erreakzio kimikoen eta farmakoen diseinuan ere; badakigu nola egin mota horretako lanak, eta ohiko ordenagailuak baino askoz ahalmen handiagoa emango liguke ordenagailu kuantikoak.

Enkriptazio kuantikoa ere martxan dago?
Arazoa da oraindik oso garestiak direla, ohiko enkriptazio-sistemak baino askoz garestiagoak, eta oraingoz ez dago arrazoirik ohiko sistema horiek baztertzeko. Arrazoi bat agertzen denean, enkriptazio kuantikoaren sistemak estandarrak izango dira, edo behintzat garrantzitsuagoak, batez ere teknologikoki garatzen direnean, prestazioak hobetzen dituztenean, prezioak murrizten dituztenean eta abar.

Baina zertarako behar dugu kriptografia kuantikoko sistema bat? Bada, hori lotuta dago ordenagailu kuantikoen ikerketarekin. Ordenagailu kuantiko bat egingo bagenu, oraingo sistema kriptografikoak (Interneten kreditu-txartelarekin erosteko erabiltzen ditugunak, gobernuek mezu sekretuak bidaltzeko erabiltzen dituztenak edo dena delakoak) ez lirateke seguruak izango. Ordenagailu kuantikoek deskodetu ahal izango dute edozein mezu. Ordenagailu horien aurka babestuta egoteko aukera bakarra enkriptazio kuantikoko sistema hauek erabiltzea da, hain zuzen ere. Ordenagailu kuantiko bat egiten den unetik, modu bakarra izango baita informazio sekretua bidaltzeko.

"Hacker batzuek etekina atera diete kriptografia kuantikoaren inplementazio zuzena ez zuten sistemei. Oraindik ez dago inplementazio erabat zuzen bat."

Enkriptazioa korapilatze kuantikoaren kontzeptuan dago oinarrituta. Badirudi gaur egungo ikerketaren mugetako bat dela zenbateko distantziara bana daitezkeen korapilatutako bi fotoi. Zer fasetan gaude?
Kriptografia kuantikoa egiteko, telegarraio kuantikoa izeneko fenomenoa erabiltzen da; informazioa toki batetik desagertzen da, eta beste batean agertu, tarteko bidea egin gabe. Eta horregatik da segurua; inork ezin du geldiarazi, ez baita tartetik pasatzen. Horretarako, argiaren egoera korapilatuak erabiltzen dira. Fotoi-bikoteak dira; fotoi bakoitza leku batera bidaltzen da, eta fotoi horiei esker pasatzen da informazioa leku batetik bestera. Problema nagusia da gaur egun egiten dituzten esperimentuetan egoera korapilatu horiek dituzten fotoiak 20-30 kilometro aldendu daitezkeela. Errekorra 150 kilometro dira, baina salbuespen bat da. Normalean 20 edo 30 kilometro izaten dira. Eta horrek esan nahi du distantzia horietara bakarrik komunika gaitezkeela.

30 kilometro ez dago gaizki.
Beno, ez dago gaizki; hiri handi samar baten behar kriptografikoak asetzen ditu, baina ez ditu bi hiri komunikatzen; adibidez, batetik bestera 80 kilometro daudenean.

***Hacker* kuantikoei buruzko albisteak ere izan dira. Ustez, kriptografia kuantikoz bidalitako mezuren bat edo beste geldiarazi dute. Oker ez banago, Swiss Telecom-eko mezuak ziren.**
Egia da *hacker* batzuek etekina atera dietela kriptografia kuantikoaren inplementazio zuzena ez zuten sistemei. Izan ere, oraindik ez da inplementazio erabat zuzena existitzen. Produktu horiek saltzen dituzten enpresek ere badakite ez dutela inplementatzen fisika kuantikoak eskatuko lukeen bezala, eta, horren ondorioz, ez dira erabat seguruak. Norvegian eta Singapurreko esperimentu batzuetan erosi egin dituzte sistema horietako batzuk, eta frogatu dute ez daudela erabat ondo eginda, ate batzuk irekita uzten dituztela, eta, beraz, informazioa irakurgai dagoela.●