Pribatutasuna ziurtatzeko, kriptografia kuantikoa

Lasa Oiarbide, Aitzol
Elhuyar Zientziaren Komunikazioa

ARTXIBOKOA

Ordenagailua eta Internet geroz eta jende gehiagok erabiltzen ditu. Hori horrela izanagatik ere, inork gutxik erabiltzen du enkriptatzeko software egokia.

Kriptografiaren historia norgehiagoka baten historia da. Kriptoanalistek kodeak apurtzea lortzen duten heinean, kriptografoek kode indartsuagoak sortzen dituzte. Edozein gizarte-antolamendutarako ezinbestekoak dira kodeak, eta badirudi gaur egungo sistemek segurtasun erabatekoa eskaintzen digutela. Baina balizko ordenagailu kuantiko batek zalantzan jarriko lituzke gaur egungo kriptografia-sistema guztiak.

EROSKETA BAT ORDAINTZEKO AURREZKI-KUTXAKO TXARTELA ERABILTZEN DEN BAKOITZEAN, transakzioa segurua izan dadin, txartelaren kodea eta bankuko informazio guztia enkriptaturik dago. Bere kontura sartzeko ordenagailua erabiltzen duenak ere kodea erabiltzen du. Enpresetako teknikariek beren artean mezuak igortzen dituzte, eta ez dute nahi lehiakideek jakin dezaten zertan dabiltzan. Zientzialariek, berriz, beren ikerketak giltzapean gordetzen dituzte, harik eta publikatzeko prest dauden arte, baina, aldi berean, beren kolaboratzaileei informazioa gordetzen duten ordenagailurako sarbidea ematen diete, hura kontsulta dezaten. Hori guztia egiteko programa informatikoak erabiltzen dira, informazioa enkriptatzen dutenak.

Kriptografia, beraz, denon inguruan dago. Baina, hori horrela izanagatik ere, ez dugu modu naturalean erabiltzen. Egia da ordenagailura sartzeko erabiltzaile-kodea dugula, baina Internet bidez enkriptatu gabe bidaltzen ditugu mezuak. Dena den, gaur egungo teknologiarekin ezinezkoa da Interneten dabilen informazio-trafiko guztiari erreparatzea.

Algoritmo informatikoak

Mezuak enkriptatzeko algoritmo seguruak badaude gaur egun. Bueno, algoritmo horiek teorian ez dira seguruak,

Kriptografia-softwareak dira ordenagailuen giltzarrapoak (ezkerrean), baina ordenagailu kuantikoak haustura ekarriko du teknologian (goian).

ARTXIBOKOAK

baina praktikan bai. Hots, teorikoki badago bide bat kodetutako mezu horiek dezifratzeko, baina horretarako behar den teknologia eta konputazio-indarra ez daude eskuragarri. Izan ere, gaur egungo kriptografia-sistema guztiak printzipio berean daude oinarrituta; hau da, sistema bat segurua da, baldin eta munduan dauden ordenagailu guztiak aldi berean lanean jarrita ere, unibertsoaren adina besteko denbora behar badute mezu bakar bat dezifratzeko.

Ordea, badago egungo ordenagailuen konputazio-indarrarekiko menpekotasunik ez duen beste kriptografia-eredu bat, kriptografia kuantikoa deiturikoa. Kriptografia-eredu hori partikulen fisikan dago oinarrituta eta ordenagailu kuantikoekin batera garatutako kontzeptua da.

Gaur egun erabiltzen diren kriptografia-sistemak ez bezala, kriptografia kuantikoa berez da segurua, hots, ez dago kriptografia kuantikoaren bidez kodetutako mezu bat dezifratzeko modu fisikorik. Eta ez da kontzeptu teoriko hutsa, baizik eta egunez egun garatzen ari den teknologia.

"gaur egun erabiltzen diren kriptografia-sistemak ez bezala, kriptografia kuantikoa berez da segurua"

Baina, gaur egungo kriptografia-sistemek behar besteko segurtasuna eskaintzen badute, zergatik da beharrezkoa kriptografia kuantikoa garatzea? Ez al da denbora eta dirua galtzea? Bada, ez. Noizbait ordenagailu kuantikoa eraikitzen badute, ordenagailu horrek kualitatiboki atzean utziko ditu gaur egungo ordenagailu guztiak, eta, horrekin batera, erabilgaitz utziko ditu gaur egungo kriptografia-sistema guztiak.

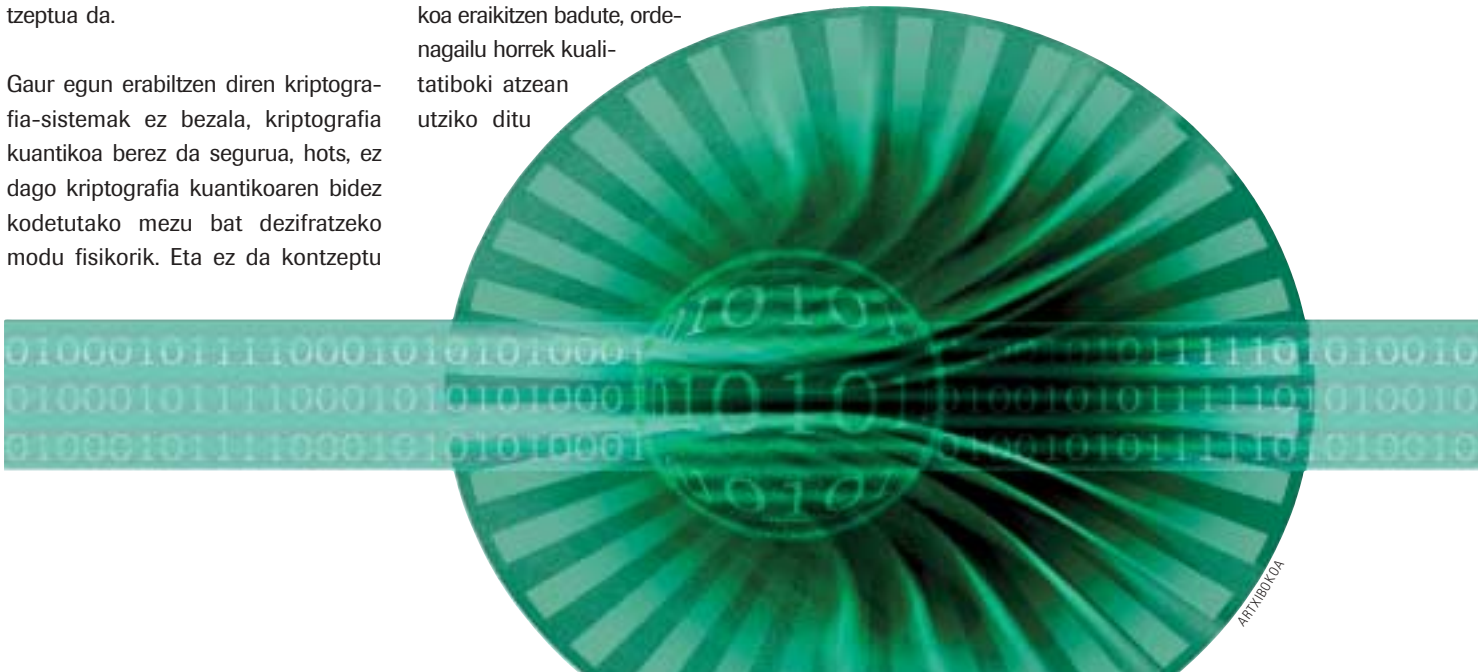
Ordenagailu kuantikoak

Gaur egungo ordenagailuek bitak erabiltzen dituzte oinarrizko kalkuluak egiteko. Bita aritmetika bitarreko digitua da, eta bi balio posible dauzka, 0 eta 1. Biten bidez, ohiko ordenagailu batek kalkuluak egiten ditu sekuentzialki. Kalkulu bat egiten du, eta gero beste bat.

Aldiz, ordenagailu kuantiko batek ez ditu ohiko bitak erabiltzen, baizik eta bit kuantikoak, eta bit kuantikoek oso bestelako jokabidea dute. Partikulen propietateak erabiltzen dira bit kuantikoak definitzeko, eta Heissenbergen ziurgabetasunaren printzipioaren arabera jokatzen dute.

Sinesgaitza dirudien arren, bit kuantiko batek aldi berean hartzen ditu 0 eta 1 balioak, eta, ondorioz, ordenagailu kuantikoak ez ditu kalkuluak sekuentzialki egiten, baizik eta aldi berean. Eta, hori gutxi balitz, ordenagailu kuantiko batek aldi berean egiten ahal dituen kalkuluen kopurua esponentzialki hazten da bit-kopuruarekiko. Hots, bit kuantiko batek bi eragiketa egin ditzake aldi berean, baina 2 bit kuantikok 4 eragiketa egingo dituzte, 5 bit kuantikok 32 eragiketa, eta 20 bit kuantikok milioi batetik gora.

Aldi berean.



ARTXIBOKOA

Fotoien fisika

Konputazio-abiadura itzel horrekin, ordenagailu kuantikoek arrazoizko denboran egingo lituzkete ohiko ordenagailuek eternitatean egingo lituzketen kalkuluak, eta horrek erabilgaitz utziko lituzke gaur egungo kriptografia-sistemak. Beraz, suposatzen badugu ordenagailu iraultzaile hori errealitate bat dela, nola lor daiteke informazioa modu seguruan gorde eta transmititzea? Bada, ordenagailu kuantikoaren indarra teoria kuantikoan oinarritzen bada, logikoa da pentsatzea teoria kuantikoak berak emango duela aukerarik kriptografia-eredu seguru bat sortzeko.

ARTXIBOKOA

Ordenagailuen txipak geroz eta bizkorragoak dira. Hala ere, ordenagailu kuantikoek atzean utziko dituzte txip bizkorrenak ere.

Kriptografia-eredu horri kriptografia kuantikoa esaten zaio, eta orain arte egin diren esperimentuak fotoietan oinarritzen dira. Fotoiek bibrazio-angelua deitzen den propietatea dute, hots, norabide jakin batean bibratzen dute.

Argi zuriak norabide guztietan bibratzen duten fotoiak sortzen ditu, baina, polaroid filtro baten bidez, bibrazio-angelu jakin bat duten fotoiak aukeratu daitezke. Horrela, fotoien sekuentzia bat lor daiteke, non fotoiek aldez aurretik erabakitako bibrazio-angeluak dituzten. Baina begiluze batek sekuentzia hori aurkitu nahiko balu, lehenengo eta behin neurtu egin beharko luke fotoien bibrazio-angelua zein den, eta neurketa horrek derrigorrean dakar fotoiaren beraren bibrazio-angelua aldatzea. Hau da, norberari ez dagokion mezua bidean atzeman nahi duenak okerreko informazioa jasoko luke, eta, gainera, mezuaren hartzailea konturatu egingo litzateke norbaitek informazio hori irakurri duela.

"fotoien bibrazio-angelua neurtzeak derrigorrean dakar fotoiaren beraren bibrazio-angelua aldatzea"

Diru kuantikoa

Kriptografia kuantikoaren sorrera Estatu Batuetan kokatzen da. 1960ko hamarkadan, Stephen Wiesnerrek bere tesi-zuzendariari proposatu zion diru kuantikoaren ideia. Wiesnerrek fotoi polarizatuak gordeko zituzten gelaxka batzuk diseinatu nahi zituen, horiek billeteetan txertatzeko. Horrela, bankuak zerrenda bat izan dezake non agertzen diren billete bakoitzaren zenbakizko kodea eta hari dagozkion fotoien polarizazioak. Diru faltsua egin nahi duenak zenbakizko kodea kopiatu dezake, baina ez du modurik fotoien polarizazioa zein den jakiteko, neurketa batek fotoiaren polarizazioa bera aldatuko lukeelako.

MEC

Teoria kuantikoaren mugen barruan kokatzen dira, beraz, bai informazioa modu seguruan gorde eta transmititzeko arazoa, baina baita arazo horren konponbidea ere. Ordenagailu kuantikoak erabilgaitz uzten du gaur egungo kriptografia, baina, aldi berean, kriptografia kuantikoa eskaintzen du, fisikoki ezin dezifratuzkoa dena.

Aurrera bidean

Kriptografia kuantikoaren inguruan egindako lehenengo esperimentua Charles Bennettek egin zuen duela ia 20 urte. 1988an, elkarrengandik 30 zentimetrora zeuden bi ordenagailu komunikatzea lortu zuen fotoien transmisio baten bidez. Esan bezala,

elkarrekintza txiki batek fotoiaren bibrazio-angelua alda dezake, eta, horregatik, lehenengo transmisioak inguru hermetikoetan egin ziren.

1995ean, 23 kilometro luze zen zuntz optikoa erabili zuten, Genevatik Nyonera, fotoi bidezko komunikazio enkriptatua egiteko. Baina, etorkizunean, ikertzaileen helburua da satelite bidezko komunikazioak egitea fotoi-transmisioen bidez. Bide horretan, Estatu Batuetako Los Álamos ikerketa-zentroan, kilometro bateko fotoien transmisioa egin dute airean barna.

Esperimentu horiek guztiek argi uzten dute kriptografia kuantikoa garatzen ari dela, eta zientzialariek espero dute kriptografia hori erabilgarri egotea ordenagailu kuantikoak sortzen direnerako.

Kodeek eta kriptografia-sistemek bilakaera handia izan dute eta erabiltzen zituztenek konfiantza osoa zuten zifra horietan, baina denborak erakutsi du zifra guztiek dituztela beren makalguneak. Gaur egun ere, kriptografia kuantikoa dezifratzea ezinezkotzat jotzen da, hura dezifratzeak esan nahiko lukeelako, besteak beste, kuantuen teoria akastuna dela. Baina nork daki etorkizunak zer ekarriko digun berri.

> *"etorkizunean, ikertzaileen helburua da satelite bidezko komunikazioak egitea fotoi-transmisioen bidez"*

ARTXIBOKOA

Kuantuen teoriaren arabera, dado bat jaurtitzen dugunean, aldi berean erakusten ditu sei aldeak, baina unibertso paraleloetan.