

Kuantum İnternet

Kuantum mekaniği şaşırtıcı olmakla birlikte atomaltı dünyadaki etkileşimleri açıklamakta olağanüstü başarılı bir kuram. Bu mikrodünyanın, bizim dünyamızda alışık olmadığımız özelliklerinden biri de çoklu durumlar; yani, bir şeyin aynı anda hem var, hem de yok olabilmesi. Bu özellik makrodünyamızda hesaplama ve haberleşme için öylesine büyük potansiyel taşıyor ki, araştırmacılar, on yıllardır bundan yararlanacak algoritmalar, programlar ve iletişim ağları tasarlamakla uğraşıyorlar. Çoklu durumların, hızlı ve güvenli haberleşmede kullanılması için yaratıcı teknikler hazırlandı bile. Aşılması gereken zorluk, mikro ve makrodünyalar arasındaki sınırı geçerek, kuantum bilgisayarları gerçekleştirebilmek.

SETH LLOYD'un pek alışılmadık bir uğraşı var. Evrendeki en ilginç, sadece kuantum dünyasında var olan kaynakları kullanarak bir ağ yaratmaya çalışıyor. Bu tuhaf ürüne dolaşıklık (entanglement) deniyor. Dolaşıklık, geçmişte bir zaman etkileşime girmiş parçacıklar arasındaki bir tür hayali, bir bakıma telepatik bir bağ olarak tanımlanabilir. Bu bağlantı, "naklen" gerçekleşiyor ve parçacıklar evrenin iki ayrı köşesinde de olsa çalışıyor. Bu sayede, belki de bilim kurgu romanlarından aşına olduğumuz türden "ışınlama" bir gün gerçek olabilecektir.

Ancak, öncelikle önümüzde duran bazı sorunlar var. Bilim adamları, ilk adım olarak dolaşıklığın yaratılması, saklanması ve dağıtılması gibi sorunların aşılması gerektiğini savunuyorlar. Böylece, çok hızlı kuantum bilgisayarların bir kuantum internetiyle birbirine bağlanması söz konusu olabilir. Kuantum bilgisayarlar, hiç kuşkusuz, araştırmacılara kuantum mekaniğinin evrendeki ilginç rolünü anlamalarına yardımcı olacak. Bunun yanında, bu bilgisayarlar sayesinde, en gizli şifreler kolaylıkla çözülebilecek. Bu nedenledir ki, Lloyd'un Massachusetts Teknoloji Enstitüsü'ndeki

(MIT) çalışmalarına Amerika Birleşik Devletleri ordusu bile destek veriyor.

Dolaşıklık, günümüzde, kuantum şifreleme ve çok küçük ölçekli kuantum bilgi işlem ve ışınlama deneylerinde kullanılıyor. Eğer dolaşık (entangled) parçacıklar, bir kuantum interneti yoluyla dünyanın her bir yanına dağıtılabilseler, bilgi işlem ve haberleşmede bir devrim gerçekleşmiş olacak.

Kuantum bilgisayarlar, çok büyük işlem gücü elde etmek için, birbirine bağlanabilecek. Bu sayede bilgi, bugün ancak kuramsal olarak varolan haberleşme hızından bile çok daha hızlı taşınabilecek. Kuantum işlemleri yapmak isteyen herkes, gereksinim duyacağı yazılımı kuantum internet yoluyla bilgisayarına yükleyebilecek. Fizikçilerse, kuantum maddenin "rafta durmayan" örnekleriyle çalışma fırsatını bulacaklar. Bu tür potansiyel uygulamalar, bir kuantum interneti yaratmak için yeterli nedenler gibi görünüyor.

Ancak, her şey görüldüğü kadar toz pembe değil. Ortadaki en büyük sorunlardan birisi, kuantum parçacıklarının çok "kırılgan" olmaları ve taşıdıkları bilgiyi kolayca yitirebilmeleri. Yalnızca bir bakış bile, taşıdıkları bilgiyi yok edebilir. Öyle görünüyor ki, bir kuantum interneti oluşturmak, bazı ciddi sorunlar çıkarıyor karşımıza.

Ancak, Lloyd ve çalışma arkadaşları, geçenlerde, bir kuantum internetinin nasıl yapılabileceğini ayrıntılarıyla yayımladılar. Üstelik, onlara göre, bugünkü teknolojiyle bunu başarmak mümkün. Lloyd'a göre, tüm gerekli parçalar daha önce yapıldı. Lloyd, üç yıl içinde, bu şebekenin ilk üç ayağını yapabileceğini düşünüyor.

Bir kuantum interneti, aslında, iletişim endüstrisinin altyapısını yeniden inşa etmek anlamına geliyor. Günümüzdeki her telefon çalışması, TV yayınları ve İnternet bağlantıları, kabaca, Claude Shannon'un çalışmalarının bir ürünü. Shannon, 1940'larda, New Jersey'deki Bell Laboratuvarları'nda, klasik haberleşme teknolojisinin temelini atmıştı. Shannon, her iletişim kanalının kapasitesini, yani her kanalın ne kadar bilgi yükünü kaldırabileceğini saptayarak ve bilgi sıkıştırma tekniklerinin ana hatlarını belirleyerek, mühendislere iletileri daha verimli göndermenin yolunu göstermişti.

Shannon, ayrıca, gürültülü kanallarla nasıl baş edeceğini ve bitlerin nerede bozulduğunu gösterdi. Örneğin, güvenilir olması bakımından, gönderici her biti üç kez tekrarlamalıydı. Shannon bunu kanal kodlama olarak adlandırdı. Araştırmacı, verimliliğin kuramsal sınırları üzerine de araştır-

malar yaptı. Yeni nesil cep telefonlarının verimliliği, bu "Shannon sınırı"na oldukça yaklaşmış olacak.

Ne var ki, Shannon'un fikirleri, sadece klasik haberleşmeye uygulanabiliyor. Kuantum internetine giden yoldaki en büyük sorun, onun kuramlarını kuantum dünyası için yeniden oluşturmakta yatıyor.

Kuantum dünyasındaki bilgiişlem, klasik bilgiişleme benzemiyor. Klasik bilgiişlemde bilgi, 0 ve 1'lerden oluşan bir dizi rakamla ifade edilir ve bu bilgi bir kablodaki voltajı değiştirerek taşınır. Bir düzeyin üzerindeki voltaj 1'i; altındakiyse 0'ı temsil eder. Ancak, bir kuantum parçacığına, örneğin bir fotonu bir parça bilgi yüklemek çok daha farklı.

Fotonlar, aynı anda iki ya da daha çok durumda bulunabilirler. Örneğin, bir fotonun elektrik alanı, foton bir düzlemde titreşecek biçimde filtre edilebilir. Buna kutuplaştırma ya da polarizasyon deniyor. Örneğin, kutuplaşma düzlemini dik yaparsak bu 0'a, yatay yaparsak, 1'e karşılık gelir.

Ancak, kuantumda, durumların üst üste gelmesi (süperpozisyon) denen bir olgu var. Bu, bir parçacığın aynı anda birden fazla durumda bulunabileceği anlamına geliyor. Bu nedenle, bir foton aynı anda hem dikeyne hem de yatay kutuplaşabilir. Bu, aynı anda hem 0 hem de 1 demek. Bu fotonun kutuplaşmasına, kubit (kuantum ve bit'in kısaltılmışı) deniyor. Kuantum durumlarının kırılğan doğası olmasaydı, mühendisler, durumların üst üste gelmesi sayesinde bu fotonları kullanarak, iletişim kanallarının hızını hemen iki kat artırabilirlerdi.

Aslında sorun tam olarak ne kadar bilginin depolanabileceği değil, ne kadarının yeniden kullanılabilirliği. Bilgi, bir foton üzerinde yapılacak ölçümle geri kazanılabilir. Ancak, kuantum dünyasında, ölçümler her şeyi değiştirir. Tek bir foton için, kutuplaşma ancak tek bir doğrultu için ölçülebilir. Bu ölçüm yapıldığında da, fotonun taşıdığı bilginin geri kalanı geri kazanılamayacak biçimde yok olur. Bu da bir kubitinden ancak bir bitlik bilgi alınabileceği anlamına geliyor. Yani, kuantum kanalıyla klasik türden bir veri gönderme, klasik kanalın kapasitesini aşmıyor.

Ancak, dolaşıklık için içine girdiğinde her şey değişiyor. İkiliden biri üzerinde yapılan ölçüm, ötekini ölçüm sonucunun da aynı olmasını sağlıyor. Aralarındaki uzaklık ne olursa olsun. Bu, uzay-zamanın iki noktasını sihirli bir biçimde birleştiren olay, iletişimde bir çığır açacak gibi görünüyor.

1992'de, IBM Thomas J. Watson Araştırma Merkezinden Charles Ben-



nett, ve Tel Aviv Üniversitesi'nden Stephen Wiesner, dolaşıklığın, kuantum kanalına göre en azından bir ya da iki kez daha hızlı olabileceğini gösterdiler. Bu, araştırmacıların hayali karakterleri Alice ve Bob için çok iyi bir haberdirdi. Alice, zamanının büyük bölümünü Bob'a kuantum iletileri göndermeye ayırmış. Ne var ki, henüz telefonda olduğundan daha hızlı bir ile-

tişim gerçekleştirememişler. Peki, Alice ve Bob, bir çift dolaşık fotonu paylaşıyor olsalardı ne olurdu?

Her foton, ya yatay (1) ya da dikey (0) kutuplaşmış olabilir. Böylece, ikili, dört durumdan birisinde olabilir: İkisi de dikey; ikisi de yatay, birincisi yatay, ikincisi dikey; birincisi yatay, ikincisi dikey kutuplaşmış olabilir. İkili sisteme göre, bu 00, 11, 01 ya da 10 olacaktır. Onluk sistemdeyse, 0'dan 3'e kadar olan rakamlara karşılık gelir bu. Alice, elindeki fotonlardan birine bakarak, sistemin bu dört durumdan hangisinde olduğunu saptayabilir.

Alice ve Bob, her biri, başlangıçta üst üste gelmiş dört durumdaki dolaşık çiftin birini alır. Sonra, Alice fotonunu basit bir optik sistemin içine koyar. Dolaşıklığın garip doğası sayesinde, Alice'in müdahalesi, Bob'un fotonunu da etkiler. Alice'in hareketi, aynı anda hem kendi hem de Bob'un fotonuna bilgi yükler. Alice, kendi fotonunu, iki foton hakkında da bir bilgiye sahip olmayan Bob'a yollar. Bob, fotonu aldığı anda, ikilinin optik özelliklerine bakarak Alice'in dört işleminden hangisini yaptığını okur. Buradaki en önemli nokta, Alice'in, dolaşıklık yoluyla ve tek foton kullanarak iki bitlik veriyi gönderebilmesidir. Böylece, dolaşıklık, onun kanalının kapasitesini iki katına çıkarmış oluyor. Bu olaya, kuantum süperyoğun kodlama da deniyor.

Aynı yöntemle, bundan da öteye gidilebilir. Fizikçiler, dolaşık üçlüler ve dörtlülerle oynamaya başladılar bile. Doğal olarak bunlar çok daha karmaşık özelliklere sahipler. Ortaya kaçınılmaz olarak çok daha fazla kombinasyon çıkıyor. Eğer bu durumlarla başa çıkılabilirse, kuantum iletilerin inanılmaz hızlarla yapılması olanaklı hale gelecek.

Ancak, ortada bir sorun var. Eğer fizikçiler ortaya çıkan istenmeyen hataları düzeltmenin bir yolunu bulamazlarsa, bu muhteşem buluş, hiçbir işe yaramayabilir. Kuantum durumları o kadar kırılğan ki, dışarıdan gelecek en ufak etki, onların bozulmalarına neden olabiliyor. Bu nedenle, pek çok fizikçi, yakın zamana kadar kuantum bilginin güvenilir bir biçimde gönderilemeyeceğini düşünüyordu. Ancak, geçen yıl, iki fizikçi bu soruna mükemmel bir çözümle geldiler.

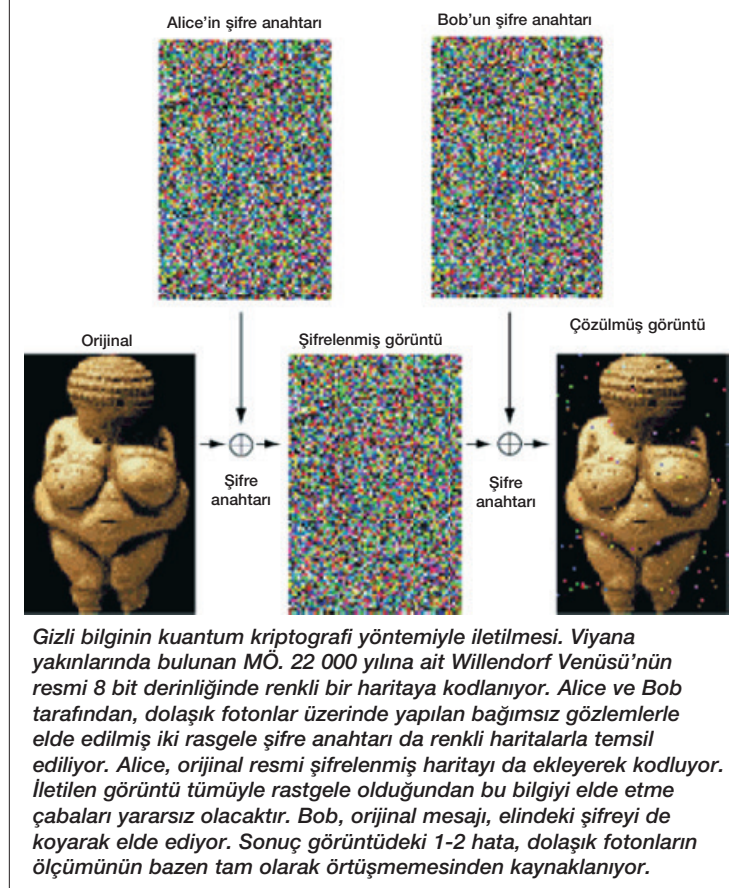
IBM'in California Almaden Araştırma Merkezi'nden Isaac Chuang ve Washington'daki Microsoft Araştırma'dan Daniel Gottesman, kuantum hesaplamaları yapan, kuantum iletilerinin içeriğini koruyan ve bitlerin hatasız kalmalarını sağlayan bir program geliştirme yolunda epeyce ilerlediler. Ve, bunu olanaklı kılan en önemli katkı, dolaşıklık. Chuang ve Gottesman'ın fikri, kuantum ışınlamayı temel alıyor. Araştırmacılar, önce gönderilecek kubit üzerinde bir ölçüm yapıyorlar. Aynı ölçümü, dolaşık çiftin yarısının üzerinde de yapıyorlar. Bu, çiftin öteki yarısına kubit hakkında bilgi gönderiyor.

Kuantum hesaplama, basitçe, bir kuantum durumunun bir başkası üzerindeki etkisinin bir sonucu. Dolaşık çiftin durumunu belirli bir biçimde hazırlarken, ışınlanan, orijinal kubit üzerinde yapılan işlemlerin sonucu.

AT&T Laboratuvarları'ndan Peter Shor ve Oxford Üniversitesi'nden Andrew Steane, 1995 yılında, veriler üzerinde yapılan bir takım basit işlemlerle hataların düzeltilebileceğini öne sürmüşlerdi. Chuang ve Gottesman'a göre, bir kuantum web sitesinden bir set halinde, hata düzelteren dolaşık fotonlar indirerek bu sorunu halledebilirsiniz.

Chuang ve Gottesman'ın makalelerinde, dolaşık parçacıkların ticari bir kaynak olabileceğine değinmişlerdi. Öyle ki, onlara göre, bu parçacıklar kuantum interneti yoluyla alınıp satılabilecekler. Ayrıca, bu parçacıkların yapısı sayesinde, taşıdıkları bilgiyi başkalarının görmesi engellenebilecek. Bir başkası onlara baktığında durum değiştireceklerinden, gizlilik daha güvenilir hale gelecek.

Belki de buraya kadar anlatılanların hepsinden de ilginç olan, kuantum internetin karmaşık moleküllerin dünya'nın herhangi bir yerine ışınlan-



Gizli bilginin kuantum kriptografi yöntemiyle iletilmesi. Viyana yakınlarında bulunan MÖ. 22 000 yılına ait Willendorf Venüsü'nün resmi 8 bit derinliğinde renkli bir haritaya kodlanıyor. Alice ve Bob tarafından, dolaşık fotonlar üzerinde yapılan bağımsız gözlemlerle elde edilmiş iki rasgele şifre anahtarı da renkli haritalarla temsil ediliyor. Alice, orijinal resmi şifrelenmiş haritayı da ekleyerek kodluyor. İletilen görüntü tümüyle rastgele olduğundan bu bilgiyi elde etme çabaları yararsız olacaktır. Bob, orijinal mesajı, elindeki şifreyi de koyarak elde ediyor. Sonuç görüntüdeki 1-2 hata, dolaşık fotonların ölçümünün bazen tam olarak örtüşmemesinden kaynaklanıyor.

masında kullanılacak ideal bir araç olabileceği düşüncesi. Şimdilik araştırmacılar, bir fotonun kuantum durumu gibi basit şeyleri ışınlayabiliyorlar. Daha ileri gitmek için, daha karmaşık dolaşıklıkların kullanılması gerekecek. Kuantum internet ve onun kuantum yazılımı, bilim adamları için, atomların, moleküllerin ve zamanla belki de yaşam unsurlarının ışınlanması yolunda bir başlangıç olacak.

Kuantum internetinin planını oluşturma yolunda ilk adımı, 1997'de Innsbruck Üniversitesi'nden Ignacio Cirac ve Peter Zoller attı. Bu yıl, Lloyd ve MIT'den Selim Shahriar ve Massachusetts'teki Hava Kuvvetleri Araştırma Laboratuvarı'ndan Philip Hemmer, bu fikri gerçeğe daha da yakınlaştırdılar. Onların düşüncesi, bir çift dolaşık foton yaratıp optik fiber yoluyla birini Alice'e ötekini Bob'a göndermek. Alice ve Bob, süper soğutulmuş atomlar içeren lazer tuzaklarına sahipler. Bu tuzaklar, fotonları yakalayabiliyor. Lloyd ve arkadaşları, bir atomun ne zaman bir foton yakaladığını ona zarar vermeden saptayabileceğimizi söylüyorlar. Alice ve Bob'un eş zamanlı soğurmalarına bakarak atomların dolaşık çifti ne zaman yakaladığı-

nı bulabiliriz. Bu gerçekleştiğinde, atomlar, kendileri dolaşık olur; böylece Alice ve Bob bir çift dolaşık parçacığı paylaşırlar. Atomların elektrik yükü olmadığından, elektrik ve manyetik alanlardan etkilenmezler ve dış dünyadan korunmuş olurlar.

Alice ve Bob, yazılımı "raftan indirerek", onu iletilerini göndermede kullanabilirler. Fizikçiler, atom çiftlerini, kuantum mikrobilgisayarları arasında iletişimi sağlamada kullanabilirler. Bu, yararlı işlemler yapabilecek kuantum bilgisayarları oluşturmada gereksinim duyacakları şey.

Günümüzün kuantum bilgisayarları, kuantum bilgi işlemleri yapabilen; ancak onu paylaşamayan ilkel moleküller. Bunlardan en güçlüsü, New Mexico'daki Los Alamos Laboratuvarları'ndaki 7 kubitlik makine. Bu makinelerden pek çoğunu birbirine bağlayarak, yararlı kuantum hesaplamalar yapmak olanaklı olabilecek. Ağ gibi yaygın bir şebekeyle, tüm dünyadaki bilgisayarlarla muazzam işlem gücü elde edilebilir.

Küresel bir kuantum interneti, sandığından daha önce yapılandırılabilir. Lloyd, 6 ay içinde, çalışan bir dolaşıklık kaynağına sahip olmayı düşünüyor. İki yıl içinde de dolaşıklığı gönderebileceğini umuyor. Üç ayaklı bir internetse bir yıl daha sonra gelebilecek.

Şimdiden, dolaşık bilginin 21. yüzyıl için sağlayacağı olanakları düşünün. Microsoft gibi, tüm dünyaya dolaşıklık kaynağı olmayı düşünenler için de iyi haberler var. Kuantum yazılımları sadece bir kez kullanılabilir. Dolaşıklık ve kuantum ölçümlerinin kurallarına göre bir kere kullanmak, onu yok etmek anlamına geliyor. Bilgi işlem tarihinde ilk kez, yazılım kopyaları dolaşıklık karşısında çaresiz kalacaklar.