

Kuantulum internet

Dr. Mahir E. Ocak [*TÜBİTAK Bilim ve Teknik Dergisi*]

Günlük hayatta kullandığımız internet ağlarında bitlerde kodlanmış “klasik bilgi” aktarılır. Bir süredir üzerine arařtırmalar yapılan bir konuya kubitlerde (kuantum bitlerde) kodlanmış “kuantum bilginin” aktarıldığı ağlar kurmak.

Henüz tam anlamıyla gerçeğe dönüřtürülmüş devasa bir kuantum ağıнын kurulması bir hayal. Ancak yakın zamanlarda yaşanan gelişmeler, gelecek birkaç yıl içinde ufak çapta kuantum ağları kurmanın mümkün olabileceğine işaret ediyor.

y

Tamamen Güvenli İnternet

Kuantum internetin günümüzdeki klasik internete göre en önemli artışı, tamamen güvenli bilgi aktarımına imkân vermesi. Bu durumun nedenlerini anlayabilmek için bitler ile kubitler arasındaki temel farkı kavramak yeterli.

Klasik bitlerin alabileceği iki değer vardır: 0 ve 1. Benzer biçimde kubitlerin de “birbirinden bağımsız iki ayrı durumda” bulunabileceği söylenebilir: $|0\rangle$ ve $|1\rangle$. Ancak kubitler, klasik bitlerin aksine, kuantum mekaniği ilkeleleriyle uyumlu davranışların gözlemlenebildiği sistemler olduğu için bir kubitin bulunabileceği “tüm durumların sayısı” esasen sonsuzdur. Genel olarak a ve b iki karmaşık sayı olmak üzere bir kubitin durumu $|0\rangle$ ve $|1\rangle$ durumlarının herhangi bir lineer kombinasyonu olabilir: $a|0\rangle + b|1\rangle$. a 'nın ve b 'nin alabileceği sonsuz farklı değere karşılık gelen sonsuz farklı durum vardır.

Kubitlerle bilgi aktarımını bitlerle bilgi aktarımına göre daha güvenli yapan şey, kuantum mekaniği ilkeleleriyle uyumlu biçimde, kubitler üzerinde yapılan ölçümlerin sonuçlarının olasılığa dayalı olmasıdır. Bir bit üzerinde ölçüm yapıldığında 0 durumundaysa 0 durumunda olduğu, 1 durumundaysa da 1 durumunda olduğu bulunur. $a|0\rangle + b|1\rangle$ durumundaki bir kubit üzerinde ölçüm yapıldığındaysa $|a|^2$ olasılıkla $|0\rangle$ durumunda olduğu, $|b|^2$ olasılıkla da $|1\rangle$ durumunda olduğu bulunur. Üstelik kubitin durumu ölçüm sonucunda bulunduğu duruma “çöker”. Başka bir deyişle, ölçümden önce $a|0\rangle + b|1\rangle$ durumunda olan bir kubit, ölçümden sonra $|a|^2$ olasılıkla $|0\rangle$ durumundaki, $|b|^2$ olasılıkla da $|1\rangle$ durumundaki bir kübite dönüşür.

İki nokta arasındaki iletişimi gizlice dinlemeye çalışan birisi olduğunu düşünelim. Eğer bilgi bitlerle aktarılıyorsa, yapması gereken şey gayet basittir: önce iletişim hattına sızıp bitlerin durumunu belirlemek daha

Kubitler

Klasik bilgi ile kuantum bilgi arasındaki temel fark, bilginin kodlandığı ve işlendiği birimlerin çalışma biçimleridir. Klasik bilginin kodlandığı birimler bit olarak adlandırılır. Hem bitlerin yapısı ve davranışları hem de bitler üzerinde yapılan işlemler klasik fizikle açıklanır. Kuantum bilginin kodlandığı birimlerse kubit olarak adlandırılır. Hem kubitlerin yapısı ve davranışları hem de kubitler üzerinde yapılan işlemler kuantum fiziğiyle açıklanır.

Bir bitin alabileceği iki değer vardır: 0 ve 1. Dolayısıyla klasik bilgisayarlarda tüm bilgiler 0'lar ve 1'lerle kodlanır. Örneğin tam sayıları ele alalım. Eğer bilgisayar sadece üç bitle işlem yapıyorsa, bu bitlerin alabileceği sekiz ayrı değer vardır: 000, 001, 010, 011, 100, 101, 110, 111. Dolayısıyla üç bitle ancak 0'dan 7'ye kadar olan tam sayılar kodlanabilir. 0'dan 7'ye kadar olan sayıların iki tabanlı gösterimiyle üç bitin alabileceği sekiz ayrı değer arasında bire bir ilişki vardır. Örneğin, 3 ve 6 sayıları iki tabanında sırasıyla 11 ve 110 olarak yazılır. Dolayısıyla 011, 3 sayısını; 110 da 6 sayısını kodlamak için kullanılabilir.

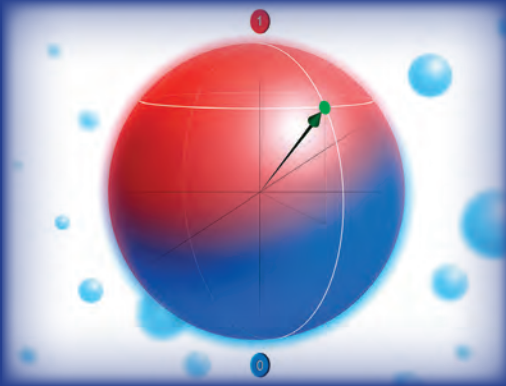
Bir biti sayının işaretini göstermek için kullanarak -örneğin 0'ı pozitif işareti, 1'i de negatif işareti göstermek için kullanarak- negatif sayılar da benzer biçimde kodlanabilir. Harfler, diğer semboller ve renkler de 0'lar ve 1'lerle kodlanır. Ancak kodlama yöntemi tam sayılarınkine göre biraz daha karmaşıktır. Günlük hayatta kullandığımız veri depolama aletleri sadece birkaç değil milyarlarca biti hafızasına kaydedebilir. Örneğin 1 terabaytlık (1 bayt=8 bit) bir harici disk, 8×10^{12} biti hafızasında saklayabilir.

Kubitlerin bitlerden temel farkı sadece 0 ve 1 değerlerine karşılık gelen durumlarda değil, bu durumların sonsuz farklı lineer kombinasyonunda da bulunabilmeleridir. 0'a ve 1'e karşılık gelen durumları $|0\rangle$ ve $|1\rangle$ ile gösterirsek, bir kubitin durumu genel olarak, a ve b iki karmaşık sayı olmak üzere, $a|0\rangle + b|1\rangle$ olarak ifade edilir. a 'nın ve b 'nin sağlaması gereken tek koşul $|a|^2 + |b|^2 = 1$ 'dir. Kubit, $a=1$ ve $b=0$ olduğunda $|0\rangle$ durumunda, $a=0$ ve $b=1$ olduğunda $|1\rangle$ durumdadır. Ancak a 'nın ve b 'nin sahip olabileceği sonsuz başka değerlere karşılık gelen sonsuz farklı durum daha vardır.

sonra da bulunduğu sonuçlara uygun yeni bitler hazırlayarak kendisi hiç araya girmemiş gibi bu bitleri alıcıya göndermek. Dinleyicinin yaptığı ölçümlerin sonuçları olasılığa dayalı olmadığı için gönderilen bitlerle alıcıya ulaşan bitler arasında herhangi bir farklılık olmaz. Bu yüzden bilginin bitlerle aktarıldığı bir sistemde herhangi birisinin varlığını belli etmeden dinleme yapması hiç de zor değildir. Günümüzde bu duruma karşı alınan önlem, bilgileri şifrelendirerek göndermek. Bu sayede iletişimi gizlice dinleyen birinin eline sadece şifrelenmiş bilgiler geçer. Sistemin güvenliğini sağlayan şeyse dinleyicinin şifreli metinleri çözmek için gerekli bilgilere sahip olmasıdır. Bu bilgiler olmadan şifreli metinlerin çözülmesi, imkânsız olmasa bile, çok zordur.

Bilginin kubitlerle aktarıldığı bir sistemdeyse durum çok daha farklıdır. Dinleyicinin önce kubitler üzerinde ölçüm yaptığını, daha sonra da bulunduğu sonuçlara uygun yeni kubitleri alıcıya gönderdiğini düşünelim. Ölçüm so-

nuçları olasılığa dayalı olduğu için alıcıya ulaşan kubitler, gönderilen orijinal kubitlerden farklı olacaktır. Örneğin, gönderilen bitin $0,6|0\rangle + 0,8|1\rangle$ olduğu durumu ele alalım. Dinleyici ölçüm sonucunda %36 olasılıkla $|0\rangle$ sonucunu %64 olasılıkla da $|1\rangle$ sonucunu bulur. Ancak bulunduğu sonuca bakarak kubitin ölçümden önceki durumunun ne olduğu hakkında bir çıkarım yapamaz. Eğer bulunduğu sonuçlara uygun kubitleri alıcıya gönderirse (ki dinleme yaptığını belli etmemek için önünde sonunda alıcıya bir şey göndermek zorundadır) alıcıya ulaşan kubit (%36 olasılıkla $|0\rangle$, %64 olasılıkla $|1\rangle$) gönderilen orijinal kubitten $(0,6|0\rangle + 0,8|1\rangle)$ farklı olacaktır. Bu yüzden bilginin kubitlerle aktarıldığı bir sistemde yetkisiz kişilerin varlığını belli etmeden herhangi bir iletişimi dinlemesi imkânsızdır. Bu durum, işleyişi kuantum mekaniği ilkeleriyle açıklanan bir internet ağının tamamen güvenli bir biçimde iletişim kurmaya imkân vereceği anlamına gelir.



Bir kubitin durumunun temsili gösterimi.

Kübit 0 veya 1 durumunda olabileceği gibi bu durumların herhangi bir lineer kombinasyonunda da olabilir.

Kuantum mekaniği bu durumdaki bir kubit üzerinde ölçüm yapıldığında $|a|^2$ ihtimalle $|0\rangle$ durumunda $|b|^2$ ihtimalle $|1\rangle$ durumunda bulunacağını söyler.

Bugüne kadar kubitlerle ilgili çok sayıda çalışma yapıldı. Günümüzde de kubit işlevi görebilecek sistemlerle ilgili yeni fikirler ortaya atılıyor, araştırmalar yapılıyor.

Kuantum mekaniği ilkelerine uyan, iki seviyeli herhangi bir sistemin kubit olarak kullanılması mümkündür. Örneğin, elektron spinleri, iki seviyeli sistemlerin bir örneğidir. Bir elektronun belirli bir yöndeki spinini belirlemek için bir ölçüm yapıldığını düşünelim. Sonuç olarak, spinin ya ölçüm yapılan yönle aynı yönde olduğu ya da ters yönde olduğu bulunur. Bu iki ihtimal, klasik bilgisayarlardaki bitlerin alabileceği iki değere (0 ve 1) karşılık gelir. Ancak bir elektronun belirli bir andaki spinini sadece bu iki yönde değil başka herhangi bir yönde de olabilir. Dolayısıyla bir elektronun spinini sadece 0 ve 1 durumlarını kodlamak için değil bu durumların herhangi bir lineer kombinasyonunu kodlamak için de kullanılabilir. Dolayısıyla elektronların spin durumları kubit olarak kullanılabilir.

Kuantum mekaniği ilkelerine uyan parçacıkların “varlığı ya da yokluğu” da “iki seviyeli sistem” olarak düşünülebilir ve kubit olarak kullanılabilir. Örneğin, fotonların varlığı ya da yokluğu veya elektronların varlığı ya da yokluğu da 0 ve 1 durumlarını kodlamak için kullanılabilir.

Kuantum Dolanıklık Nedir?

Klasik mekanikte, bir sistemin özellikleri içerdiği parçacıkların konumları ve hızları ile tanımlanır. Konum ve hız, zaman içinde değişen dinamik değişkenlerdir. Kuantum mekaniğinde ise durum tamamen farklıdır. Konum ve hız herhangi bir anlam ifade etmez. Parçacıkların belirli bir konumları ya da hızları yoktur. Kuantum mekaniğinde sistemin durumu, dalga fonksiyonu olarak adlandırılan fonksiyonlar kullanılarak tanımlanır. Bu fonksiyon belirli bir anda sistemin belirli durumlarda bulunma ihtimalleri hakkında bilgi verir.

Kuantum mekaniğine göre bir sistemin dalga fonksiyonu, o sistemi tanımlayan Schrödinger denkleminin herhangi bir çözümü olabilir. Ölçümler sonucunda elde edilebilecek sonuçların her biri Schrödinger denkleminin öz durumdur ve denklemin birbirinden bağımsız çok sayıda özdu-

rumu vardır. Bir sistemin belirli bir andaki dalga fonksiyonu, sistemin ölçümler sonucunda bulunabileceği öz durumların herhangi bir lineer kombinasyonu olabilir. Çok sayıda özdeş sistem üzerinde aynı ölçüm yapıldığı zaman sonuçlar dalga fonksiyonu tarafından tahmin edilen olasılıklara uygun çıkar.

Kuantum dolanıklık, birden fazla parçacık içeren sistemlerde görülür. Örneğin, iki elektrondan oluşan bir sistemi ve sadece bu elektronların bulunabileceği spin durumlarını ele alalım. Bir elektronun spinini iki öz durum ile ifade edilebilir. Bu durumları $|\uparrow\rangle$ ve $|\downarrow\rangle$ ile gösterelim. Bir elektronun spin durumu bu iki durumun herhangi bir lineer kombinasyonu olabilir. Örneğin, sonsuz sayıdaki muhtemel durumdan bazıları şunlardır: $(|\uparrow\rangle + |\downarrow\rangle)/\sqrt{2}$, $(|\uparrow\rangle - |\downarrow\rangle)/\sqrt{2}$, $(0.6*|\uparrow\rangle + 0.8*|\downarrow\rangle)$.

Kuantum Anahtar Dağıtımı

Günümüzde kubitlerin başarılı bir biçimde kullanılmaya başlandığı alanlardan biri klasik bilginin şifrelenmesi.

İnternet ağı üzerinden bilgi aktarımı yapmak istediğinizi düşünün. Başkalarının aktarılan bilgileri dinlemesi ihtimaline karşı önlem olarak bilginin şifrelenmesi gerekir. Peki ama nasıl? Tamamen güvenli olan bir yöntem, iki tarafın şifreleme için “tek kullanımlık bir anahtar belirlemeleri” ve bu anahtarı başka hiç kimsenin bilmemesidir. Yöntem kısaca şöyle işler. Diyelim ki aktarılmak istenen bit dizisi 10110001, şifreleme için kullanılacak anahtar da 1100001 olsun. Gönderici, önce iki bit dizisindeki karşılıklı bitleri tek tek birbiriyle toplayarak şifrelenmiş bir dizi üretir: 10110001+1100001=0111000 (toplama mod 2’de yapılıyor). Daha sonra şifrelenmiş diziyi internet üzerinden gönderir. Alıcı şifrelenmiş diziden anahtarı çıkararak şifrelenmemiş bit dizisini elde eder: 0111000-1100001=1011001. Bu yöntemin güvenliğini sağlayan şey, şifreleme için kullanılan anahtarı gönderici ve alıcıdan

başka hiç kimsenin bilmemesidir. Yetkisiz birisi şifreli bit dizisini ele geçirse bile hangi anahtar kullanılarak şifreleme yapıldığını bilmediği için şifreyi çözemez. Ayrıca, her bir aktarım için farklı anahtarlar kullanıldığından çeşitli şifreli bit dizilerini birbiriyle karşılaştırarak bir fikir edinilmesi de mümkün değildir.

Klasik bilginin aktarılmasında kubitlerin yararlı olduğu nokta, kullanılacak anahtarın belirlenmesidir. Gönderici ve alıcı, kubitlerin aktarıldığı bir ağ üzerinden iletişim kurarak şifreleme için tek kullanımlık anahtarı belirleyebilirler. Böylece, herhangi birisinin varlığını belli etmeden ağa sızması mümkün olmadığı için, sadece gönderici ve alıcı tarafından bilinen tamamen gizli bir anahtarın oluşturulması mümkün olur. Bu sürece kuantum anahtar dağıtımı denir.

Geçtiğimiz yıl Genova Üniversitesinden Alberto Baron ve çalışma arkadaşları, fiber optik kablolar üzerinden saniyede 6,5 kilobit hızla 400 kilometre uzaklığa kuantum anahtar dağıtımı yapmayı başardıklarını açıkladılar. Şu an ticari olarak satışı yapılan bazı sistemlerse yaklaşık 50 kilometre mesafeye kuantum anahtar dağıtımı yapmaya imkân veriyor.

İki elektronun spin öz durumları da farklı elektronların spin öz durumları kullanılarak yazılabilir. Bir elektronun spininin iki öz durumu olduğu için iki elektronun spinlerinin farklı dört öz durumu olabilir: $|\uparrow\rangle|\uparrow\rangle$, $|\uparrow\rangle|\downarrow\rangle$, $|\downarrow\rangle|\uparrow\rangle$, $|\downarrow\rangle|\downarrow\rangle$. Bu gösterimde ilk simge birinci elektrona, ikinci simge ise ikinci elektrona karşılık gelir. Örneğin $|\uparrow\rangle|\downarrow\rangle$ durumundaki bir sistemde, birinci elektron $|\uparrow\rangle$ durumunda ikinci elektron ise $|\downarrow\rangle$ durumundadır. $|\downarrow\rangle|\uparrow\rangle$ durumundaki bir sistemde ise birinci elektron $|\downarrow\rangle$ durumunda ikinci elektron ise $|\uparrow\rangle$ durumundadır. Tek parçacıklı sistemlerde olduğu gibi, sistemin herhangi bir andaki durumu bu dört öz durumun herhangi bir lineer kombinasyonu olabilir. Bu lineer kombinasyonların bazıları dolanık durumlar olarak adlandırılır. Örneğin $(|\uparrow\rangle|\downarrow\rangle - |\downarrow\rangle|\uparrow\rangle)/\sqrt{2}$ dolanık bir durumdur. Bu durumdaki bir sistemdeki elektronların spin durumları birbirinden bağımsız değildir.

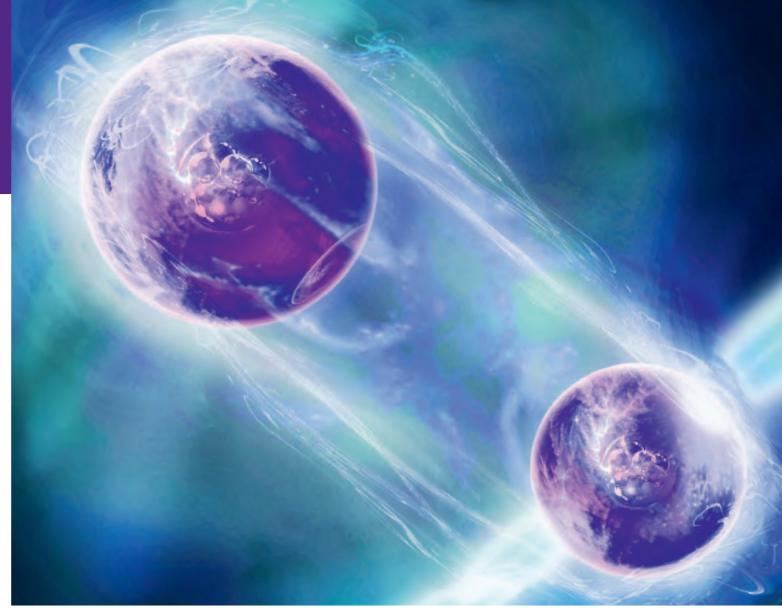
Ne birinci elektron $|\uparrow\rangle$, ikinci elektron $|\downarrow\rangle$ durumunda ne de birinci elektron $|\downarrow\rangle$, ikinci elektron $|\uparrow\rangle$ durumundadır. Parçacıkların spin durumu dolanık olduğu için biri üzerinde yapılan ölçüm diğerini de etkiler. Örneğin, ölçüm sonunda birinci parçacığın $|\uparrow\rangle$ durumunda olduğu bulunursa ikinci parçacığın durumu, $|\downarrow\rangle$ durumuna “çöker”. Aynı şey dolanık olmayan durumlar için doğru değildir. Örneğin, $(|\uparrow\rangle|\uparrow\rangle + |\downarrow\rangle|\downarrow\rangle)/\sqrt{2}$ durumu dolanık değildir. İkinci parçacık, birinci parçacığın durumundan bağımsız olarak $|\uparrow\rangle$ durumundadır. Dolayısıyla, birinci parçacık üzerinde yapılan bir ölçüm ikinci parçacığın durumunu etkilemez.

Dolanıklıkla Bilgi Aktarımı

Kuantum anahtar dağıtımı, şimdilik sadece klasik bilgiyi şifrelemenin güvenli bir yolunu sağlıyor. Ancak gelecekte bilgiyi kodlamak, depolamak ve aktarmak için tamamen kuantum mekaniksel olgulardan yararlanan internet ağları kurmak mümkün olabilir.

Bir kuantum internet ağı için gerekli olan en temel şey, kubitlerde kodlanmış bilgiyi ağ üzerindeki bir noktadan diğerine aktarabilmek. Her ne kadar kuantum anahtar dağıtımı sırasında yapılanla tam olarak aynı şey olsa da fiber optik kablolar üzerinde bilgi taşıyan fotonlar büyük miktarda bilginin hızlı bir biçimde aktarılmasına uygun değil. Çünkü fotonlar yol alırken saçılabilir, soğurularak yok olabiliyor ya da dedektörler tarafından kaydedilmeyebiliyorlar. Bu yüzden, büyük miktarda bilgiyi hızla aktarabilmek için çok daha iyi bir yöntem ihtiyacı var.

Günümüzde kuantum internet ile ilgili araştırmalarda bilgiyi aktarmak için odaklanılan ana yöntem kuantum dolanıklıktan yararlanmak. Birbirine dolanık hâldeki iki sistemden biri üzerinde yapılan ölçüm, aralarındaki



mesafe ne olursa olsun diğer sistemi de etkiler. Dolayısıyla bir hattın iki ucundaki kubitleri birbiriyle dolanık hâle getirerek bilgi aktarımı yapmak mümkün. Üstelik bu yöntem kubitlerin bir yerden başka bir yere taşınmasını da gerektirmez.

Dolanıklıktan yararlanarak bilgi aktarımı yapabilmek için öncelikle birbirine çok uzak iki kubitleri birbiriyle dolanık hâle getirmek gerekiyor. Bu amaçla başvurulan yöntem, hattın iki ucundaki “madde kubitleri”ni fiber optik kablolarla yol alan “ışık kubitleri” aracılığıyla dolanık hâle getirmek. Bu konu üzerinde bugüne kadar yapılmış çeşitli başarılı çalışmalar var.



Avusturya'daki Kuantum Optik ve Kuantum Bilgi Enstitüsünde çalışan Ben Lanyon ve arkadaşları, Ocak ayında yayımladıkları bir makalede fiber optik kablolar üzerinden 50 kilometre mesafeye dolanıklık dağıtımını yapmayı başardıklarını açıkladılar. Araştırmacıların geliştirdiği yöntemde, madde kübiti olarak bir iyon kapanının içinde hapsolmuş kalsiyum iyonları kullanılıyor. Lazerler kullanılarak iyonun enerji seviyelerinde bir kübit kodlanırken polarizasyon durumlarında bir kübit kodlanmış bir foton (ışık kübiti) da yayılıyor. Bu süreç sonunda yayılan foton ile, iyondaki kübitler birbiriyle dolanık hâlde. Kalsiyum iyonundan yayılan fotonun dalga boyu (854 nanometre) fiber optik kablolarla taşınmaya uygun olmadığı için, foton doğrudan fiber optik kabloya aktarılamıyor. Bu yüzden, iyondan yayılan foton, fiber optik kabloya aktarılmadan önce, doğrusal olmayan kristaller yardımıyla Telekom dalgaboylarından birine sahip başka bir fotona dönüştürülüyor. Araştırmacılar, kübitlerde bilgi kodlandıktan ve kristalden çıkan foton fiber optik kabloda 50 kilometre yol aldıktan sonra yaptıkları ölçümlerde madde kübiti ile ışık kübitinin hâlâ dolanık hâlde olduğunu görmüşler.

Araştırmacıların bir sonraki hedefi bu yöntemi kullanarak aralarında 100 kilometre olan iki madde kübitini birbiriyle dolanık hâle getirmek. Bu amaçla iki madde kübitinin tam ortasına bir "istasyon" yerleştirilecek. İstasyonda, iki ayrı uçtan gelen, madde kübitleriyle dolanık hâldeki fotonlar üzerinde ölçüm yapılacak. Bu sırada madde kübitleriyle ışık kübitleri arasındaki dolanıklık yok olurken madde kübitleri birbiriyle dolanık hâle gelecek.

Dolanıklık değiş tokuşu olarak adlandırılan bu süreç sonunda, iki madde kübitini kullanarak bilgi aktarmak mümkün hâle gelecek.

İki nokta arasında kuantum bilgi aktarımıyla ilgili başarılı çalışmalar yapan bir başka araştırma grubu da Hollanda'daki Delft Üniversitesinde çalışmalar yapıyor. Prof. Dr. Ronald Hanson ve öğrencileri, madde kübiti olarak elmasların içine hapsolmuş elektronları kullanıyorlar. Bir elmasın yapısına karışan azot atomları, iki komşu karbon atomunu yerinden eder. Bu karbon atomlarından birinin yerini azot atomu alırken diğeryse boş kalır. Ortaya çıkan yapıya azot-boşluk (NV) merkezi denir. Deneylerde madde kübiti olarak kullanılan elektronlar, bu NV merkezlerinin içinde "serbest hâlde" bulunuyor. Bu yöntemde bilgi elektronların spininde kodlanıyor. Bu süreçte tıpkı iyon kübitinde olduğu gibi bir foton yayılıyor. Fotonda kodlanmış kübit ile elektronda kodlanmış kübit birbiriyle dolanık hâlde oluyor.

Araştırmacılar, deneyler sırasında, fiber optik kabloyla birbirine bağlı iki NV merkezini aralarında 1,3 kilometre mesafe olacak şekilde konumlandırmışlar. İki NV merkezinden yayılan fotonlar hattın ortasına geldiğinde dolanıklık değiş tokuşu gerçekleşiyor ve madde kübitleri birbiriyle dolanık hâle geliyorlar. Bu yöntemle ilgili en önemli sorun, yayılan 637 nanometre dalgaboylu fotonların fiber optik kablolarda fazla yol alamaması. Bu yüzden bu yöntemle birkaç kilometreden daha uzağa dolanıklık aktarımı yapmak henüz mümkün değil. Araştırmacılar bu sorunu aşmak için Lanyon ve arkadaşlarının yaptığı gi-

bi doğrusal olmayan kristaller kullanarak yayılan fotonu Telekom dalgaboylu bir fotona dönüştürmeyi planlıyorlar. Bu sayede 30 kilometre mesafeye dolanıklık aktarımı yapmanın mümkün hâle geleceğini düşünüyorlar. Hanson ve arkadaşlarının bir diğer hedefiyse, üç ayrı şehirdeki madde kubitlerini birbiriyle dolanık hâle getirmek.

Lanyon ve Hanson gruplarının üzerinde çalıştığı sistemlerin bir özelliği, hattın iki ucundaki sistemlerin aynı tür olması. Ancak kuantum internet tam anlamıyla gerçeğe dönüştürüldüğünde çok farklı türde sistemler ağ üzerinde yer alacaktır. Bu yüzden sadece benzer sistemler arasında değil farklı sistemler arasında da bilgi aktarımı yapmaya imkân veren yöntemlere de ihtiyaç var. Bu amaçla çalışmalar yapan araştırma gruplarından biri İsviçre'deki Basel Üniversitesi'nden Grimau Puigibert ve arkadaşları. İtalya'daki Calgary Üniversitesinden Wolfgang Tittel'in grubuyla ortak yaptıkları çalışmalar sonucunda iki ayrı türde malzemelerde saklanan kubitleri dolanık hâle getirmeyi başarmışlar.

Araştırmacıların yaptıkları deneylerde, önce bir kaynaktan birbirine dolanık hâlde iki foton yayılıyor. Bu fotonların birinin dalgaboyu 1535 nanometre, diğerinin kiye 794 nanometre. 794 nanometre dalgaboylu foton tulyum katkılı lityum niyobat (LiNbO_3) kristaliyle etkileşime giriyor ve böylece fotonun durumu kristalde "kaydediliyor". 1535 nanometre dalgaboylu fotonu erbiyum katkılı bir fiberin içine giriyor ve bu fotonun durumu da fiber de kaydediliyor. Her iki hafıza da fotonları bir süre sonra yeniden salacak biçimde tasarlanmış. Araştırmacılar hafızalardan yayılan fotonları incelediklerinde hâlâ birbirleriyle dolanık hâlde olduğunu görmüşler. Bu durum fotonlar salınmadan önce hafızaların da birbiriyle dolanık hâlde olduğu anlamına geliyor. Dolayısıyla başlangıçta kaynaktan yayılan fotonlar arasındaki dolanık hafızalar tarafından muhafaza edilebiliyor.

Bu deneylerle ilgili bir diğer önemli nokta 1535 nanometre dalgaboylu fotonların fiber optik kablolar üzerinden, 794 nanometre dalgaboylu fotonların ise uydular üzerinden iletişim için uygun olması. Bu durum özellikle büyük çapta bir kuantum internet ağı kurulabilmesi açısından çok önemli. Çünkü kıtalararası bilgi aktarımı yapabilmek için dolanıklık dağıtımının atmosfer içinden de yapılabilmesine ihtiyaç var. 2017 yılında Çin Bilim ve Teknoloji Üniversitesi'nde çalışan Jian-Wei Pan ve öğrencile-

ri, Çin'e ait bir uydu aracılığıyla Tibet Platosu ile Güneybatı Çin'deki bir bölge arasında dolanıklık dağıtımı yapmayı başarmıştı. Ancak uydular, kuantum bilgi aktarımında kullanılmak için yine de çok pahalı bir seçenek gibi duruyor. Kuantum bilgiyi atmosfer içinden aktarmanın daha ucuz bir yolu drone kullanmak olabilir. Nanjing Üniversitesinde çalışan Shi-Ning Zhu ve arkadaşları Mayıs ayında, 35 kilogram kütleli bir drone aracılığıyla aralarında 200 metre mesafe olan iki sistem arasında dolanık fotonlar aktarmayı başardıklarını açıkladı. Üstelik aktarım günışığında, karanlıkta ve hatta yağmurlu havalarda bile başarıyla yapılabilir. Araştırmacılar, daha büyük drone'ların kullanılmasıyla, aynı biçimde 300 kilometre mesafeye aktarım yapmanın da mümkün olabileceğini belirtiyorlar.

Tüm dünyayı birbirine bağlayan bir kuantum internet ağı kurmak uzak bir hayal. Ancak bu hayali gerçeğe dönüştürmek için gerekli teknolojiler yavaş yavaş da olsa geliştiriliyor. Gelecek birkaç sene içinde tüm dünyayı olmasa da aralarında 50-100 kilometre olan birkaç şehri birbirine bağlayan bir kuantum internet ağı kurmak mümkün olabilir.

Dünya çapında bir kuantum internet ağı kurmak için aşılması gereken birkaç engel var. Birincisi kuantum bilgiyi uzun süre muhafaza edebilecek güvenilir hafıza cihazlarına ihtiyaç var. Ayrıca bilginin aktarıldığı noktalar arasındaki mesafenin isteğe göre artırılmasının mümkün hâle gelmesi de gerekiyor. Söz konusu olan klasik bilgi olduğunda çok uzak noktalara aktarım yapmak zor değildir. Eğer sinyal yolda zayıflıyorsa yeniden güçlendirebilirsiniz. Yapmanız gereken tek şey, hat üzerindeki bir noktada zayıflamış sinyaldeki bilgiyi okumak daha sonra aynı bilgiyi daha güçlü bir sinyalle hedefine göndermektir. Ancak aynı şey kuantum bilgi ile yapılamaz. Çünkü, ölçüm sonuçlarının olasılığa dayalı olması, bilgiyi okuyup daha sonra daha güçlü bir sinyalle yeniden göndermeyi imkânsızlaştırır. Çevresel etkenler sebebiyle kuantum bilginin kaybolmasının önüne geçmek ve bilgiyi çok uzak mesafelere aktarabilmek için karmaşık teknolojilere ihtiyaç var. Muhtemelen gelecekte bir kuantum internet ağının kurulması için aşılması gereken en büyük zorluk da bu olacak. ■

Kaynak

Ananthaswamy, Anil, "The Quantum Internet Is Emerging, One Experiment at a Time", *Scientific American*, <https://www.scientificamerican.com/article/the-quantum-internet-is-emerging-one-experiment-at-a-time/>, 19 Haziran 2019.