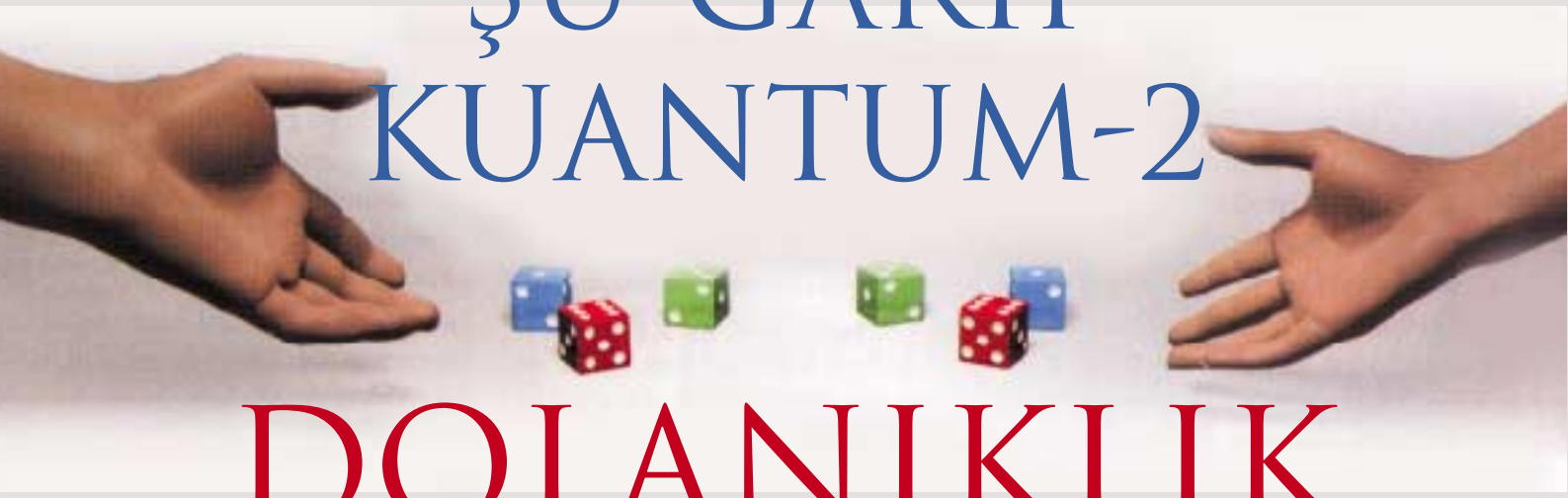
ŞU GARİP KUANTUM-2



DOLANIKLIK

Geçen ay, kuantum yasalarına uyan mikroskopik ölçekteki sistemlerin üst üste gelme özelliğinden bahsetmiştik. Herhangi bir sistem, olası durumlarının her birinde aynı anda bulunabiliyordu. Bir elektron aynı anda değişik yerlerde bulunup değişik hızlara sahip olabilir. Ya da elektronun spini, bir başka deyişle mıknatıslık doğrultusu, yine aynı anda farklı yönlerde olabilir. Üst üste gelme, kuantum yasalarının bize en garip gelen özelliği. Dolanıklıksa bu garipliklerin bir adım ötesi: İki farklı sistemden oluşan bir toplam sistemin sahip olduğu kuantum durumlarında, alt sistemlerin durumları arasında ilişki (korelasyon) varsa, iki sistemin dolanık olduğunu söylüyoruz.

Dolanıklığı, yukarıdaki gibi pek anlam ifade etmeyen bir cümleyle anlatmak yerine örnekle açıklamak daha uygun olur. Tek kubitlik bilgi taşıyabilen A ve B parçacıklarını düşünün. A ve B iki elektron olabilir (spinleri yukarıysa '1', aşağıysa '0'), ya da iki foton (kutuplaşma yataysa '1', dikeyse '0'), ya da tek kubitlik bilgi taşıyabilen başka sistemler de olabilir. A ve B'nin olası durumlarını sırayla yazarsak (yani önce A'nın durumu sonra B'nin), böyle bir sistem dört tane farklı klasik durumda bulunabilir: '00', '01', '10' ve '11'. Fakat kuantum fiziğine göre, iki parçacık bu dört durumun değişik olasılıklarla üst üste gelmesiyle oluşabilecek herhangi bir durumda bulunabilir. Örneğin, genellikle $|00\rangle + |11\rangle$ olarak gösterilen durumda, yani A ve B'nin her ikisinin de '0', ya da her ikisinin de '1' olduğu durumda parçacıklar dolanıktır. Dolanıklığın yalnız bu şekilde olması gerekmiyor; sonsuz sayıda değişik dolanıklık türü var.

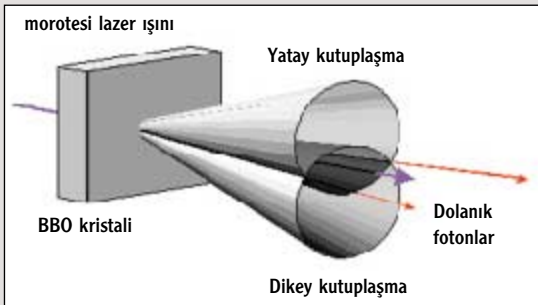
Dolanıklığı anlatmak kadar resimle göstermek de zor. Bu yazıya eşlik eden şekillerde, parçacıkların iki olası durumunu iki farklı renkle göstermeye özen gösterdik (kırmızı ve mavi). Her iki renkteki olasılığın, aynı anda gerçekten var olduğunu tekrar edelim. Dolayısıyla, parçacıkların herhangi biri üzerinde ölçüm yapılırsa, o zaman 'kırmızı' ve 'mavi' renkle gösterilenden yalnızca birisi gerçeklik kazanır. Ölçüm, sistemin içinde bulunduğu durumu değiştirir ve ne sonuç elde edilmişse, ona uygun yeni bir duruma sokar.

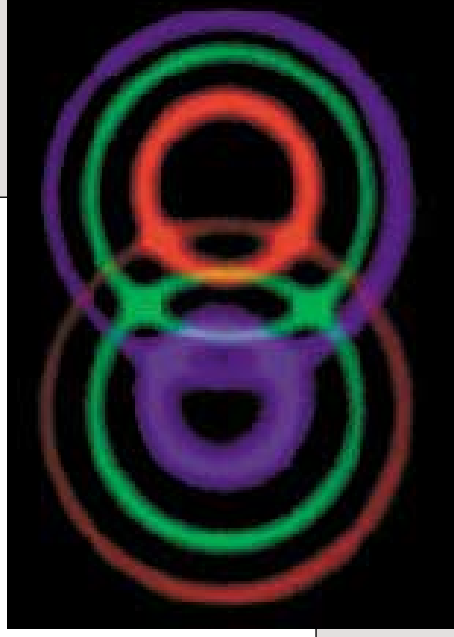
Yukarıda bahsettiğimiz iki dolanık kubit örneğinde, A üzerine yapılan ölçüm '1' değerini vermişse, o zaman B kubiti de '1' değerini alır. Dolanıklığın en ilginç yanı bu. Parçacıklardan biri üzerinde yapılan ölçüm, diğer parçacığın durumunu etkiliyor. Albert Einstein, Boris Podolsky ve Nathan Rosen, 1935 yılında yayımladıkları ünlü makalelerinde böyle bir şeyin büyük sorunlar yaratacağına dikkat çekmişlerdi. Çünkü, A'nın ölçümünün B'yi etkilemesi olayı, bunlar birbirinden çok uzakta da olsa gerçekleşiyor. Sorunu daha dramatik yapmak için abartırsak, A'nın Dünya'da kaldığını, B'nin de binlerce ışık yılı uzaklıktaki komşu bir galaksiye götürüldüğünü düşünün. Bu kubitler ne kadar uzakta olsalar da, henüz üzerlerinde bir ölçüm yapılmamışsa dolanık kalmaya devam ederler. Daha sonra bunlardan biri üzerinde yapılan ölçüm, diğerini anında etkileyecektir!

Aynı orbitali paylaşan iki elektronun spinleri dolanıktır. Eğer soldaki yukarı spine sahipse sağdaki aşağı (mavi renkle gösterilen durum), fakat eğer soldaki aşağı spine sahipse, soldaki de yukarı spine sahiptir (kırmızı renk). Her iki durum aynı anda eşit olasılıkla (%50-%50) gerçekleşir.

Neler oluyor? Hiç bir şeyin ışıktan hızlı yol alamayacağını söyleyen kurala ne oldu? Aşağıda açıklayacağımız gibi, bu olay ışık hızıyla ilgili kurala aykırı değil. Ama Einstein başta olmak üzere bir çok bilim adamı, kuantum fiziğinin dolanıklığa izin vermesinden ötürü rahatsızlık duymuşlardı. Einstein, parçacıklardan biri üzerinde yapılan ölçümün diğerini anında belirlemesine "hayalet etki" adını vermişti. Çünkü, daha sonra 70 ve 80'li yıllarda yapılan deneylerin de onayladığı gibi, böyle bir etkinin gerçekten var olduğunu ama aynı zamanda deney aletleriyle algılanamaz olduğunu söyleyebiliyoruz. Gerçek bir "hayalet"!

Işıktan Hızlı Mesaj İletilebilir mi?





Çok sayıda dolanık foton çifti üretmek için kullanılan yöntemlerden biri. Özel bir kristal, üzerine gönderilen morötesi lazerin fotonlarını soğurur ve hemen arkasından daha düşük enerjili iki foton yayınlar. Çıkan fotonlardan biri üst konilerden yatay kutuplaşmış olarak, diğeri de alt konilerden dikey kutuplaşmış olarak çıkar. Fotoğraftaki iki yeşil koninin kesiştiği doğrultularda çıkan foton çiftlerinin kutuplaşmaları dolanıktır. Fotoğraf, üç değişik renkte filtre kullanılarak elde edilmiş ve sadece bu renkteki fotonların bir saat içinde oluşturduğu görüntüyü gösteriyor.

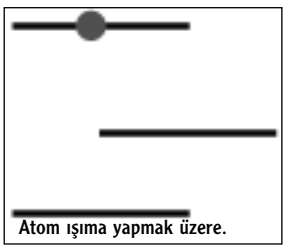
Özel görelilik kuramı yalnızca "ışığın boşluktaki hızından daha hızlı bir şekilde mesaj iletilemez" der. Her ne kadar yalnızca mesajlardan bahsediyor olsa da, bu ifade, ışıktan hızlı giden uzay gemilerinin yapılması önündeki en büyük engel (çünkü gemiye bir postacı bindirebilirsiniz). Bugüne kadar çok sayıda "ışıktan hızlı" olaylar gözlemlendi, ama hiç birinde yukarıda verdiğimiz ifadeye aykırılık bulunamadı. Dolanık parçacıklar aracılığıyla iletilen "hayalet etki" de bunlar arasında.

Öncelikle mesajdan ne kast ettiğimizi varsayımsal bir örnekle açıklayalım: Berna en az dört ışıkyılı uzaklıktaki komşu yıldızdaki bir gezegene (Borg gezegeni) yolculuğa çıkacak. Yolculuktan hemen önce Ali, Berna'ya evlenme teklif ediyor. Berna, düşünmesi gerektiğini, Borg'a vardığında cevabını vereceğini söylüyor. Fakat, ışık Borg'dan Dünya'ya ancak dört yılda ulaşıyor. Bu nedenle Ali, cevabın ne olduğunu Berna'nın karar vermesinden dört yıl sonra öğrenebilir. Özel görelilik kuramı, Ali'nin bu bilgiyi daha erken öğrenemeyeceğini söylüyor. Buradaki mesaj mümkün olan en basit şey, bir bitlik bir bilgi: Cevap ya "evet" olacaktır ya da "hayır". Berna'nın yapması gereken, mesajını doğru bir şekilde ulaştırıp, Ali'nin cevabını doğru anladığından emin olmak. "Hayır" demek istemişken, Ali'nin "evet" anlamasına engel olması gerekir. Dola-

Dolanık Parçacıklar Nasıl Elde Edilir?

Dolanık parçacıkların kullanıldığı pratik uygulamalarda, iletişim hızı açısından çok sayıda dolanık parçacık çifti üretmek ve bunları yine çok hızlı bir şekilde iletmek büyük önem taşıyor. Bu iş için fotonlar en ideal seçim. Optik teknolojisinin çok ilerlemiş olması nedeniyle, yüksek oranda değişik şekillerde dolanmış fotonlar elde etmek mümkün. Üstelik, halen kullanılmakta olan fiber optik kablolar, bu fotonları uzak yerlere taşımak için oldukça uygun.

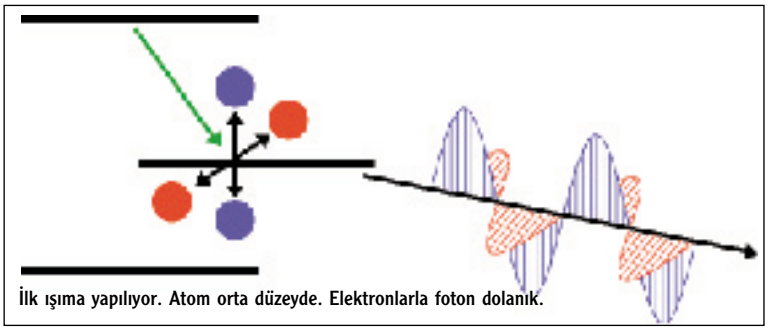
Dolanık fotonlar elde etmek için kullanılan yöntemlerden biri, bazı atomlarda görülen özel bir tip ışıma şeklinden yararlanıyor. Çağlayan (cascade) ışıması olarak adlandırılan bu ışıma tipinde, yüksek enerjili, uyarılmış bir atom birbirinin peşi sıra iki foton yayınlıyor. Şekilde tüm olay şematik olarak gösteriliyor. Şekilde gösterilen üç raf (yatay çizgiler), atomun değişik enerji düzeylerini sembolize ediyor. Her bir düzeyde, atomun elektronları o düzeye özgü yörüngelerde bulunur. Eğer atom bir düzeyden daha alttaki bir düzeye geçerse, bir foton yayınlanır ve aradaki enerji farkı foton tarafından taşınır.

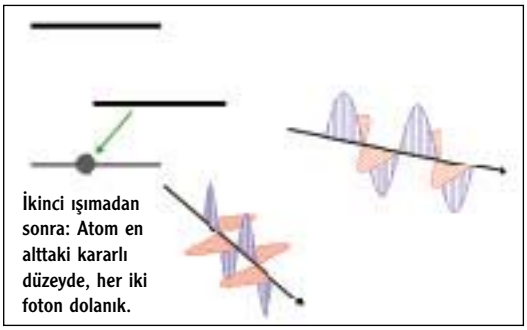

Atom ışıma yapmak üzere.

Çağlayan ışımasının görüldüğü sistemlerde en üst düzeyden en alt düzeye doğrudan bir geçiş söz konusu değil. Atom, önce üst düzeyden ortadaki bir düzeye, daha sonra da buradan en alttakine geçiyor. Bunun sonucu olarak, kısa aralıklarla art arda iki foton yayınlanıyor. İlk ışımada, yani üst düzeyden orta düzeye geçiş sonrasında, çıkan fotonun kutuplaşması nedeniyle, atomdaki elektronlar titreşmeye başlıyorlar. Fotonun kutuplaşmasıyla elektronların titreşme doğrultusu aynı olmak zorunda. Eğer foton yatay yönde kutuplaşmışsa, elektronlar yatay yönde (kırmızı renkle gösterilen durum), fakat eğer foton dikey kutuplaşmışsa elektronlar da dikey yönde titreşiyorlar (mavi renk). Kuantum yasalarına göre, atom her iki duruma aynı anda ve eşit olasılıklarla geçiyor. Kısacası, foton ortaya çıktığı anda, atom ile foton dolanık duruma giriyor.

Bu aşamadan sonra, orta düzeyden en alt düzeye ışıma gerçekleşiyor. Burada da çıkan fotonun kutuplaşması, elektronların ışımadan önce titreştikleri doğrultuyla aynı. Sonuçta ortaya çok kısa bir zaman aralığında, kutuplaşmaları dolanıklaşmış iki foton çıkıyor. Bundan sonra elektronik bir devre yardımıyla iki fotonun ne kadar bir zaman aralığıyla ortaya çıktığı ölçülüyor. Eğer fotonlar neredeyse aynı zamanda ortaya çıkmışsa, o zaman bunların aynı atomdan çıktıkları ve dolayısıyla dolanık oldukları düşünülerek, kullanılmak üzere fiber optik kablolara gönderiliyor.

Ortaya iki fotonun çıktığı ışıma türlerinin çoğunda fotonlar dolanıktır. Örneğin, bir elektron ve karşıt maddesi olan pozitron birleşerek birbirlerini yok ettiğinde de ortaya iki tane dolanık yüksek enerjili foton çıkar. Dolanıklığı sınamak için yapılan ilk deneylerden biri, bu sistem üzerine çalışmış. Bunun dışında kutuplaşmaları yerine enerjileri dolanık olan fotonlar da yüksek verimleri nedeniyle deneylerde kullanılıyor.


İlk ışıma yapılıyor. Atom orta düzeyde. Elektronlarla foton dolanık.


İkinci ışımadan sonra: Atom en alttaki kararlı düzeyde, her iki foton dolanık.

nık parçacıklar yardımıyla böyle bir mesaj gönderilebilir mi?

Önce kaba bir yaklaşımla başlayalım. Dolanık iki parçacığı Ali'yle Berna'nın paylaştığını (bunu Berna ayrılmadan yapmışlar) varsayalım. Berna'nın kendi parçacığı üzerinde yaptığı ölçümün sonucu, anında Ali'nin parçacığına iletilecek. Berna cevabını böyle gönderebilir mi? Sorun şu: Berna ölçümü yapınca eşit olasılıkla '0' ya da '1' elde eder. Ama hangisini elde edeceğini seçemez. Yani, Berna'nın cevabı ne olursa olsun, ölçüm sonunda elde ettiği değer (ve Ali'nin okuyacağı değer) cevaptan bağımsız olacaktır. Her ikisi de aynı değeri buluyor, ama bunun Berna'nın cevabıyla hiç bir ilgisi yok. Kuantum yasalarının bir özelliği burada önemli. Yapılan ölçümün sonucu, diğer her şeyden bağımsız olarak belirleniyor. Ölçüm sürecini ve sonucunu etkilememiz olanaksız. Yazı tura atarken hileli para kullanarak olasılıkları değiştirebiliriz; ancak, kuantum yasaları ölçüm sırasında böyle bir hileye izin vermiyor.

İki dolanık kubit. Biri '1'ken diğeri de '1'; biri '0'ken diğeri de '0'.

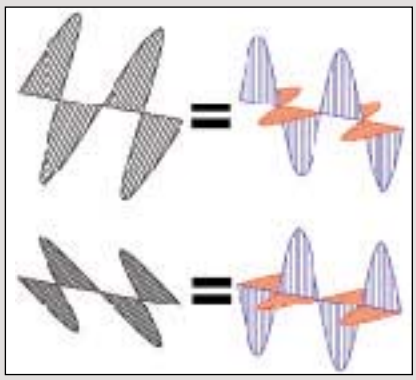
Fakat Berna, ölçümü nasıl yapacağını seçebilir. Berna'nın elinde kutuplaşmaları dolanıklaşmış fotonlardan birinin olduğunu düşünelim. (Diğer tür parçacıklarla da aynı şey yapılabilir.) Eğer cevabı "evet"se, kutuplayıcısını yatay konuma getirerek ölçümü alır. Ölçüm sonucunda, hem Berna'nın hem de Ali'nin fotonu ya yatay ya da dikey kutuplaşmış duruma girer. Eğer cevabı "hayır"sa, bu defa Berna, kutuplayıcısını 45 derece açıyla konumlandırarak ölçüm yapar. Bu defa, her iki foton ya 45 derece ya da 135 derece açıyla kutuplaşma durumuna geçer.

Ali ise, Berna'nın ölçümü nasıl aldığını anlamak istiyor. Elindeki fotonun, dört olası durumdan yalnızca birinde bulunduğundan emin: Ya kutuplaşma doğrultusu yatayla 0 ya da 90 derece açı

Fotonların Kutuplaşma Durumları

Kutuplaşma (polarizasyon) ışığın, büyük olasılıkla şimdiye kadar hiç fark etmediğiniz bir özelliği. Gerçi kutuplaşmadan yararlanan bazı uygulamalar hayatımıza girmiş durumda: Fotoğrafçılar, yüzeylerden yansıyan istenmeyen ışığı engellemek, sinemacılarsa üç boyutlu filmleri göstermek için kutuplaşmayı kullanıyorlar. Ama, gözümüzün kutuplaşmayı algılayamaması nedeniyle, böyle bir şeyin varlığını normal yollardan hissetmemiz olanaksız.

Işığın bir elektromanyetik dalga olduğunu ve beraberinde sürekli yön değiştiren elektrik ve manyetik alanlar taşıdığını çoğunuz duymuşsunuzdur. Kutuplaşma, bu elektrik alanın doğrultusuna deniyor. Elektrik alan, ışık-madde etkileşmesinin temel mekanizmasını oluşturur. Işık bir madde içinden geçerken, elektronlara elektrik alanın ters yönünde bir kuvvet uygulanır. Alan büyüklüğünü ve yönünü sürekli değiştirdiği için, elektronlar da sabit bir yönde sürekli hızlanmak yerine, ortalama bir konum etrafında titreşme hareketi yapar. Böylece ışığın taşıdığı enerji elektronlara aktarılır (ışığın soğurulması). Bunun tam tersi de geçerli: Başka bir nedenle titreşmeye başlamış bir elektron, çevreye bir elektromanyetik dalga yayabilir (ışığın yayınlanması). Bu ilişki nedeniyle ışığın kutuplaşma doğrultusuyla, elektronun titreşme doğrultusu aynı olmak zorunda.



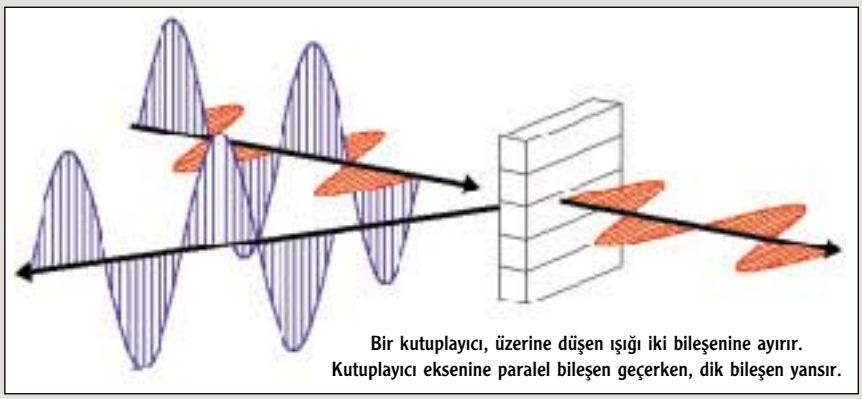
Herhangi bir ışık demeti, yatay ve dikey kutuplaşmış iki farklı demetin üst üste gelmesi olarak düşünülebilir.

Işığın klasik kuramına göre kutuplaşma doğrultusu, ışığın yayıldığı yöne dik olmalı. Bu kısıtlama göz önüne alındığında bile, çok sayıda farklı kutuplaşma durumu var. Doğrusal kutuplaşmada elektrik alan yalnızca bir yönde ve bunun tam tersi yönde olabiliyor, dolayısıyla etkileşen elektronlar da bu doğrultu boyunca titreşiyorlar. Dairesel kutuplaşmadaysa, elektrik alanın büyüklüğü değişmeden yalnızca yönü değişiyor, dolayısıyla etkileştiği elektronların dairesel bir yörünge çizmesine neden oluyorlar. Bunun dışında elektrik alanın hem büyüklüğünün, hem de yönünün değiştiği eliptik kutuplaşma türleri de var.

Her ne kadar çok sayıda kutuplaşma türü olsa da, herhangi bir ışık demetinin yatay ve dikey yönde kutuplaşmış iki farklı ışık demetinin üst üste gelmesiyle oluştuğu düşünülebilir. İşte, kuantum dünyasında çok sık karşılaştığımız ve en garip şey olduğunu iddia ettiğimiz "üst üste gelme" kavramı böyle bir olgudan ödünç alınmış. Maddeyle etkileşirken, yatay kutuplaşmış bir ışık demeti elektronları yatay yönde titreştirir, dikey yönde kutuplaşmış olan demet de dikey yönde titreştirir. Eğer her iki demet de aynı anda aynı yerden geçmekteyse, elektronlar iki demetin bir çeşit "toplam" etkisi altında farklı bir doğrultuda titreşecektir.

Üstelik, kutuplayıcı (polarizör) olarak adlandırılan malzemeler yardımıyla bir ışık demeti yatay ve dikey kutuplaşmış bileşenlerine ayrılabilir. Kutuplayıcı malzemelerin özelliği, elektronlarının hareket serbestisinin belli doğrultularda daha az, diğer doğrultularda daha çok olması. Bu nedenle malzemenin ışığa verdiği tepki (geçirme, soğurma ve yansıtma) ışığın kutuplaşmasına bağlı. İdeal bir kutuplayıcı yalnızca belli bir doğrultuda kutuplaşmış ışığı geçirir (bu doğrultuya kutuplayıcının geçirme ekseni diyelim), buna karşın dik yönde kutuplaşmış ışığı ya soğurur, ya da yansıtır.

Su ve cam gibi saydam maddelerin yüzeyleri ideal olmayan kutuplayıcılara iyi bir örnek. Suyun üzerine ışık düştüğü zaman, ışığın bir kısmı suya girer, bir kısmı da yansır. Yansıyan ışığın önemli bir kısmı (ama tamamı değil) suyun yüzeyine paralel doğrultuda kutuplaşmıştır. Bu gibi yüzeylerden yansıyan ışıktan rahatsız olan fotoğrafçılar, geçirme ekseni dik olan bir kutuplayıcı filtre yardımıyla yansıyan ışığın önemli bir kısmını engelleyebilir.



Bir kutuplayıcı, üzerine düşen ışığı iki bileşenine ayırır. Kutuplayıcı eksenine paralel bileşen geçerken, dik bileşen yansır.

Fotonlar

Kuantum kuramına göre ışık, bölünemez en küçük parçası olan fotonlardan oluşmuştur. Bu düşünce bize çok da yabancı değil. Nasıl su, su ol-

yapar (ki bu durumda Berna'nın cevabı evettir), ya da 45 ya da 135 derece açı yapar (bu durumda da Berna'nın cevabı hayırdır.) Ne yazık ki, Ali'nin yalnızca tek bir ölçüm yapma hakkı var. Bu ölçümü yaptıktan sonra fotonunun durumu hakkındaki bilgi tamamen kaybolur. Ali, Berna'nın ölçümü nasıl yaptığını anlayabilir mi?

Ne yazık ki hayır. Ali'nin kutuplayıcısını yatay konuma getirip ölçümü aldığını düşünün: Berna'nın cevabı evetse, Ali Berna'nınkiyle aynı sonucu bulur (yatay ya da dikey). Ama, Berna'nın cevabı hayırsa Ali'nin fotonu durumunu değiştir ve yine yatay ya da dikey sonuçlarından birini verir. Ali elde ettiği tek bitlik deney sonucundan (yatay ya da dikey) Berna'nın niyetini anlayamaz. Deney, çok sayıda parçacık çiftiyle tekrarlansa bile durum değişmez. Üstelik Ali, ne yaparsa yapsın, Berna'nın bir ölçüm yapıp yapmadığını bile anlayamaz.

Kopyalamak Yasaktır Teoremi

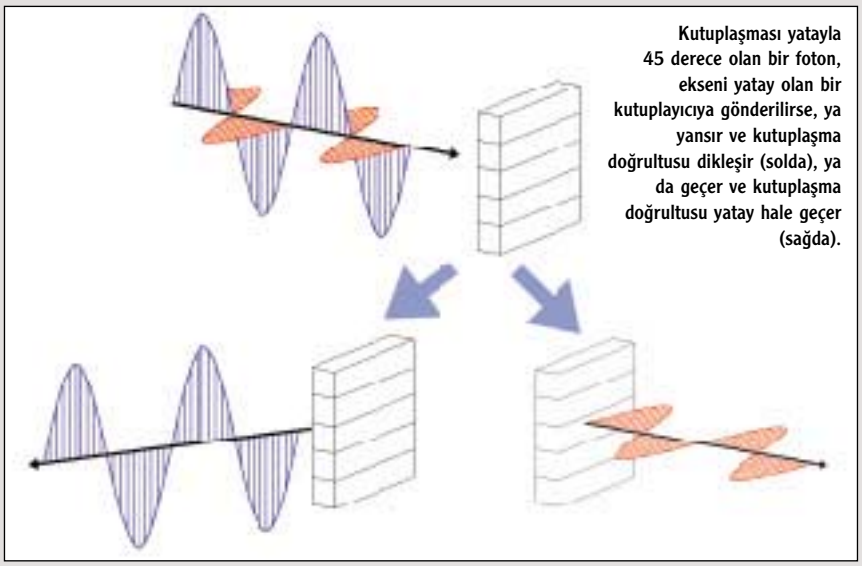
Geçen ay bahsettiğimiz, bilinmeyen bir kuantum sisteminin özdeş kopyalarının oluşturulamayacağını söyleyen kopyalama yasağı teoreminin anlamı, bu olayda daha iyi anlaşılıyor. Eğer Ali, elindeki fotonunun özdeş kopyalarını çıkarabilseydi, o zaman Berna'nın niyetini anlayabilirdi. Şöyle: Ali, elindeki fotonun 1000 tane kopyasını çıkartır. Bunlardan ilk 500 tanesinde kutuplayıcısı yatay konumdayken ölçüm yapar. Son 500 tanesinde de 45 derece açıyla ölçüm alır. Eğer ilk 500 ölçümün sonucu aynıysa (hepsi yatay ya da hepsi dikey) Berna'nın cevabı evettir. Fakat, son 500 ölçüm aynıysa cevap hayırdır. Ne yazık ki Ali, elindeki fotonun değil 999 kopyası, tek bir kopyasını bile çıkartamaz. Kopyalama yasağı kuralı buna engel oluyor. Yani, zavallı Ali dört yıl daha bekleyip sonucu normal yollardan öğrenmek zorunda. Sonuç olarak, kuantum bilgisayarlar için pek hoş olmayan kopyalama yasağı teoremi, aynı zamanda ışıktan hızlı haberleşmeyi engelleyen bir kural.

ma özelliği taşıyabilen en küçük birimi olan su moleküllerinden oluşmuşsa, foton da ışığın ışık denebilecek en küçük birimidir.

Peki, bir kutuplayıcıya (çok sayıda fotondan oluşan) ışık göndermek yerine yalnızca tek bir foton gönderilirse ne olur? Bu soruyu cevaplayabilmek için iki temel kuralı göz önünde bulundurmamız gerekir. Birincisi, normal parlaklıkta bir ışık demeti çok sayıda fotondan oluşur. Bu nedenle bu demet içindeki fotonların tek tek davranışları, tüm ışık demetinin davranışını belirler. Örneğin, kutuplaşma doğrultusu kutuplayıcının eksenine paralel olan ışık kutuplayıcı malzemeyi geçer. Öyleyse, bu ışık demeti içindeki tüm fotonlar da kutuplayıcıyı geçer. Buna karşın, eğer ışık demetinin kutuplaşma doğrultusu kutuplayıcınınkine dikse, ışığın hepsi yansır (ya da soğurulur ama biz yansıdığını varsayacağız). O halde bu demet içindeki fotonların hepsi kutuplayıcıdan yansır.

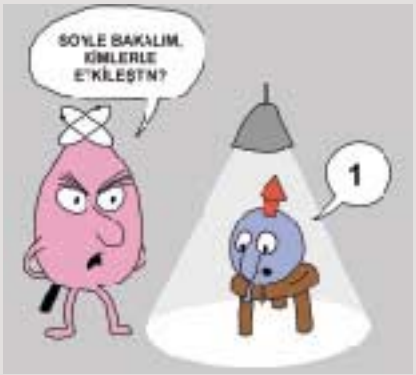
Yukarıda söylemeye çalıştığımız şu: kutuplayıcının eksenini yere yatay gelecek şekilde doğrultalım. O zaman, yatay kutuplaşmış olan foton geçer, dikey kutuplaşmış olan da yansır. Bu bize en azından klasik bir iletişim olanağı sunuyor. Yatay kutuplaşmayı '1', dikey olanı da '0' olarak düşünürsek, herhangi bir mesaj arka arkaya gönderilen çok sayıda fotonun kutuplaşma durumlarına kodlanabilir. Mesajı okuyan birisinin tek yapması gereken şey, bir kutuplayıcı kullanarak geçen fotonları '1', yansıyanları da '0' olarak yorumlamak.

Peki kutuplayıcı üzerine gelen fotonun farklı bir kutuplaşma doğrultusu varsa ne olur? Burada ikinci temel kuralı da göz önüne almamız gerekiyor: Foton bölünemez! Örnek olarak, fotonun kutuplaşma doğrultusuyla, kutuplayıcının ekseni arasındaki açının 45 derece olduğu bir deneyi düşünelim. Böyle fotonlardan oluşan bir ışık demetinin yarısı kutuplayıcıdan geçer, yarısı da yansır. (Daha doğrusu ışığın taşıdığı enerjinin yarısı geçer, yarısı da yansır.) Ama, tek bir foton için bu söz konusu değil, çünkü fotonun yarısı diye bir şey yok. O halde böyle bir foton ya kutuplayıcıyı tüm olarak geçmeli ve geçtikten sonra kutuplaşma doğrultusu yatay olmalı, ya da foton tüm olarak yansımalı ve yansımadan sonra kutuplaşma doğrultusu dik olmalı. Buna ek olarak, fotonların geçme ve yansıma olasılıkları da % 50 - % 50 olarak eşit olmalı (yansıyan enerji geçen enerjiye eşit olduğu için).



Kutuplaşması yatayla 45 derece olan bir foton, ekseni yatay olan bir kutuplayıcıya gönderilirse, ya yansır ve kutuplaşma doğrultusu dikleşir (solda), ya da geçer ve kutuplaşma doğrultusu yatay hale geçer (sağda).

Kuantumca'da yukarıdaki olayı şöyle anlatıyoruz: Foton kutuplayıcıya gelirken hem '1' (yatay) hem de '0' (dikey) durumlarının her ikisinde birden bulunuyordu (üst üste gelme). Ama kutuplayıcıya ulaştığı anda bir "ölçüm" alındı (kutuplaşma doğrultusunun ölçümü) ve iki olasılıktan birisi o anda gerçekleşti.



Kuantum sorgulama çok zordur.

Ya foton kutuplayıcıyı geçti ve '1' durumuna girdi. Önceki durumu hakkında bütün bilgi silindi. Bu arada kutuplayıcıyı kullanan adam fotonun geçtiğini görünce bunu '1' olarak yorumladı (ölçüm sonucu '1').

Ya da foton yansıdı ve '0' durumuna girdi. Önceki durumu hakkında bütün bilgi silindi ve adam fotonun yansıdığını anlayınca bunu '0' olarak yorumladı (ölçüm sonucu '0').

Tüm kuantum sistemlerinde yukarıda bahsettiğimiz olay benzer şekilde tekrarlanıyor. Adına "ölçüm" deyin ya da başka bir şey, bir sistem hakkında bilgi sahibi olmaya yeltendiğinizde, sistemi geri dönülmez bir şekilde değiştiriyorsunuz. Sonuçta, elinize bir değer, bir ölçüm sonucu geçiyor ama bunun sistemin ölçümden önceki durumuyla hiç bir ilgisi yok (elde ettiğiniz olası değerlerden yalnızca birisi). Üstelik, ikinci bir ölçüm yapma şansınız da kalmıyor, çünkü sistem artık o eski sistem değil; sanki sistem "benden başka bilgi alamazsınız" der gibi önceki durumuyla ilgili bütün bilgiyi siliyor.

Kuantum Kriptografi

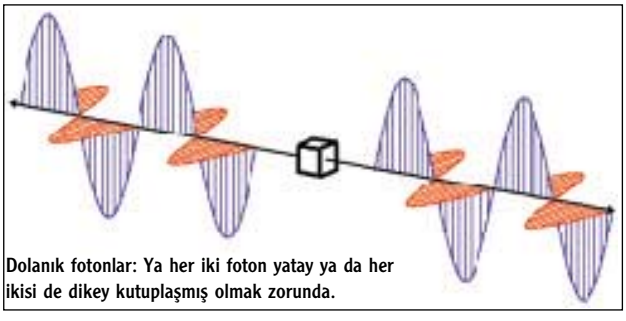
Her ne kadar dolanık parçacıklar ışıktan hızlı mesaj göndermek için kullanılamasa da, önemli bir fonksiyonu gerçekleştiriyor. Eğer Ali'yle Berna ölçümlerini aynı şekilde (aynı kutuplayıcı açısıyla) almışlarsa, elde ettikleri sonuçlar aynı olmak zorunda. Yani, ya her ikisi de '0' değerine sahip, ya da '1' değerine. Eğer, bu tip bir ölçüm çok sayıda dolanık parçacık çifti üzerinde uygulanırsa, iki kişi '0' ve '1'lerden oluşmuş aynı rasgele sayı dizisini elde eder.

Böyle bir rasgele sayı dizisi gönderilecek bir mesajı şifrelemek için kullanılabilir (detaylar için "Tek Kullanımlık Gürültü" yazısına bakınız). Bu sistemin pratik uygulamalarında Ali'yle Berna Dünya'dadır. İstedikleri zaman birbirlerine dolanık parçacıklar gönderebilirler; bunun yanı sıra normal iletişim kanallarıyla haberleşebilirler (telefon, İnternet vs.). Dolanık parçacıklar yardımıyla, başka hiç kimsenin bilmediği özdeş iki rasgele sayı dizisi elde ederler, sonra da kutuda bahsettiğimiz yöntemi kullanarak şifreli mesajlarını normal iletişim kanallarından gönderirler.

Peki, Ali'yle Berna, ellerindeki sayı dizilerinin başka hiç bir kimsenin bilmediğinden nasıl emin olabilir? Oxford Üniversitesinden Artur Ekert, bunu sağlamak için bir protokol geliştirdi ve denedi. Protokolde, Ali 1000 tane dolanık parçacık çifti hazırlar. Her çiftten birini kendi alarak, diğerini Berna'ya gönderir. Sonra, her ikisi de ellerindeki 1000 parçacık üzerinde ya yatay yönde ya da 45 derece açıyla ölçüm alırlar. Ölçüm aldıkları doğrultuları kendileri belirlerler ve bunu rasgele bir şekilde yapmaya özen gösterirler. Bu bittikten sonra, hangi yönde ölçüm aldıklarını birbirlerine açıklarlar (ama ölçüm sonuçlarını kendilerine saklarlar). Eğer Ali ve Berna, ölçümü aynı yönde almışlarsa, elde ettikleri değerler aynı olmalı. Bu da, toplam 1000 ölçümün yaklaşık yarısı, yani 500 kadar ölçüm değerinin ortaklaşa paylaşıldığını söylüyor.

Böylece Ali ve Berna'nın elinde yaklaşık 500 tane ölçüm değeri var. Başka birinin bu değerleri bilmediğinden emin olmak için, bu 500 bitin bir kısmını, (diyelim ki rasgele 100 tanesini) birbirlerine açıklarlar (diğer 400 taneyi saklarlar). Eğer bu 100 bit gerçekten aynıysa başka birinin dinlemediğinden, dolayısıyla da diğer 400 taneyi kendilerinden başka birinin bilmediğinden emin olurlar. Neden mi? Meraklı birisinin bilgi kazanmak için tek yapabileceği, Berna'ya giden fotonları alıp, bunlar üzerinde kendi ölçümünü almak, daha sonra da bu fotonu Berna'ya göndermek. Fakat Meraklı, Berna'yla aynı değeri bulmak istiyorsa, ölçümünü de Berna'nın seçtiği doğrultularda yapmalı. Eğer Berna, bu ölçüm doğrultularına gerçekten rasgele karar veriyorsa, Meraklı'nın bunu başarması mümkün değil.

Sonuçta, Ali'yle Berna'nın karşılaştırdıkları sayılarda farklılıklar olacaktır. Böyle bir farklılık görüldüğü anda, başka birinin iletişimi dinlediği anlaşılır ve ellerindeki diziler kullanılmaz. (Zaten, her ikisinde farklı diziler olduğu için şifreli iletişime geçemezler). Bu durumda, Meraklı'nın dinlemediği başka uygun bir an bulup tekrar denemeleri gerekir.



Dolanık fotonlar: Ya her iki foton yatay ya da her ikisi de dikey kutuplaşmış olmak zorunda.

Tek Kullanımlık Gürültü

Berna sesini bir kasete kaydederek, Ali'ye gizli bir mesaj göndermek istiyor. Her ikisinin ellerinde birbirinin kopyası iki kaset var. Kasetleri geçmişte bir gün, televizyondaki yayın olmayan (karlı) kanallardan birini açarak kaydetmişler. Berna mesajını nasıl gönderir?

Doğal olarak, böyle bir sorunla günlük hayatınızda karşılaşmazsınız. Göndereceğiniz gizli bir mesajınız varsa, gider kendisine doğrudan söylersiniz. Ama, sorunun cevabında vereceğimiz yöntem (one time pad), klasik şifreleme sistemleri arasında güvenilirliği kanıtlanmış tek sistem. Bu nedenle, eğer yöntemi pratik olarak uygulamak mümkün olursa, şifrelemeye ihtiyacı olan herkesin tercih edeceğine kesin gözüyle bakılabilir.

Cevap: Berna mesajını okurken, bir yandan da gürültü içeren kaseti çalar ve her iki sesi aynı anda kaydeder. Sonra da bu kaydettiği kaseti Ali'ye gönderir, ama orijinal gürültüyü içeren kaseti saklamaya özen gösterir (ya da imha eder). Kaset yolda istenmeyen meraklı kişilerin eline geçse bile, bunlar gürültüden Berna'nın sesini ayırt edemezler. Hatta, gürültü seviyesi yeterince yüksekse, içinde bir insan sesi olup olmadığını bile anlayamazlar.

Ali şifreli kaseti aldığında, kendisinde bulunan orijinal gürültü kasetini de kullanarak ikisi arasındaki farkı bulmaya, yani şifreden gürültüyü çıkarmaya çalışır. Bunu dinleyerek yapamaz ama bilgisayarlar yardımıyla bunu yapabilmek mümkün. Çıkarma işlemini yaptıktan sonra geride kalan, Berna'nın mesajıdır.

Sistemin dezavantajı, yalnızca tek bir defa kullanılabilmesi. Ali cevap vermek istediğinde aynı gürültüyü kullanamaz. Eğer kullanırsa ve hem Berna'nın şifreli mesaj kaseti, hem de Ali'nin cevap kaseti Meraklı'nın eline geçmişse (bu olasılık her zaman var), Meraklı iki kasetteki sesleri birbirinden çıkararak gürültüyü tamamen ortadan kaldırabilir. Ortaya çıkan yeni ses kaydında, yalnızca Berna ve Ali'nin sesleri üst üste gelmiş olacaktır. Bu durumda her ikisinin söyledikleri çok zor olmayan bir analizden sonra anlaşılabilir.

Tek kullanımlık olmasının getirdiği bir dezavantaj, gönderilecek her yeni mesaj için farklı bir gürültü kasetine gereksinim duyulması. Eğer Ali'yle Berna akıllılık edip önceden yüzlerce gürültü kaseti kaydetmiş ve paylaşmışlarsa sorun yok. Ama bunlar kullanılıp bittiğinde, mutlaka tekrar bir araya gelip yeni gürültüler kaydetmek zorundalar. Gerçek uygulamalar için bu olanaksız. Örneğin, İnternette kredi kartı numarasını iletmek için bu yöntemi kullanamazsınız.

Dolanık parçacıkları kullanan kuantum kriptografi, bu sorunu tamamen ortadan kaldırıyor. İki kişi daha önce hiç karşılaşmamış olsa bile, normal iletişim kanallarını kullanarak aynı gürültüyü içeren iki özdeş kaset hazırlayabiliyorlar. Üstelik bu kasetin kopyalarının başka hiç bir kimsede olmadığından emin olabiliyorlar. Böylece, bu gürültüyü kullanarak, yine başkalarının dinleyemeyeceğinden emin olarak tek bir mesaj gönderebiliyorlar.

Doğal olarak, bu sistemin pratik uygulamalarında sesli kasetler kullanılmayacak. Dolanık parçacıklar üzerinde yaptıkları ölçümlerde, Ali ve Berna 0 ve 1'lerden oluşan ve yalnızca ikisinin bildiği ortak bir diziye sahip olur. Dizinin özelliği, gürültü gibi, sayıların tamamen rasgele olması. Sonra, Berna mesajını sayısal olarak kodlayıp rasgele dizideki sayılarla toplar. Bu durumda, elde ettiği mesaj da tamamen rasgele olacaktır. Şifreyi alan Ali, elinde kopyası bulunan rasgele diziyi bundan çıkararak orijinal mesajı okuyabilir.

Dr. Sadi Turgut
ODTÜ Fizik Bölümü

Kaynaklar
Turgut, S., "Parcacıklar Telepati Yaparlar mı? Bilim ve Teknik Dergisi, Ekim 2000 s.40
www.qubit.org