

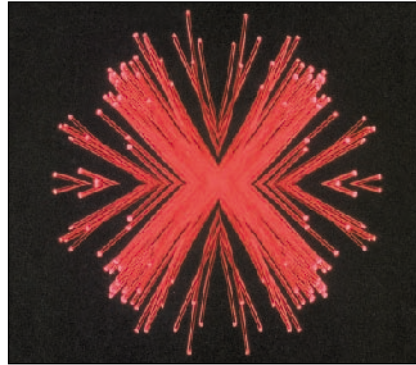
Hayal Gerçeklerin Gücü Kuantum Bilgisayarlar

Uygarlığımızın ulaştığı dorukları, teknolojik atılımlarımızı, hep olanaklarımızın bir adım ötesinde koşan gereksinmelerimize borçluyuz. Bilgi çağında gereksinmelerimiz baş döndürücü bir hızla arttı. Bilgisayarlar, neredeyse olağan ev eşyaları haline geldi. Bu aygıtlar bize yalnızca oturduğumuz yerden faturalarımızı ödemek, bütçemizi yapmak, mektuplarımızı yazmak, ödevlerimizi hazırlamak, ya da eğlenmek olanağı vermiyor. Artık bilgisayarlarımızı birbirine bağlamak gereksinmesini duyuyoruz. İnternet, bu gereksinmenin bir ürünü. Oturduğunuz yerden günlük gazetenizi okuyorsunuz, dünyanın herhangi bir yerinde çıkan dergiyi izleyebiliyorsunuz. Krediyi alışveriş yapabiliyorsunuz. Ancak böylesine muazzam bir bilgi alışverişini düzenlemek, yönetmek kolay değil. Üstelik uzmanlara göre İnternet'in yaygın kullanımı daha yeni başladı sayılır. Toplam kullanma hacminin önümüzdeki yıllarda 10 kat artması bekleniyor. Büyük, süperhızlı bilgisayarların bile bu yükü kaldırmakta zorlanacağı sanılıyor.

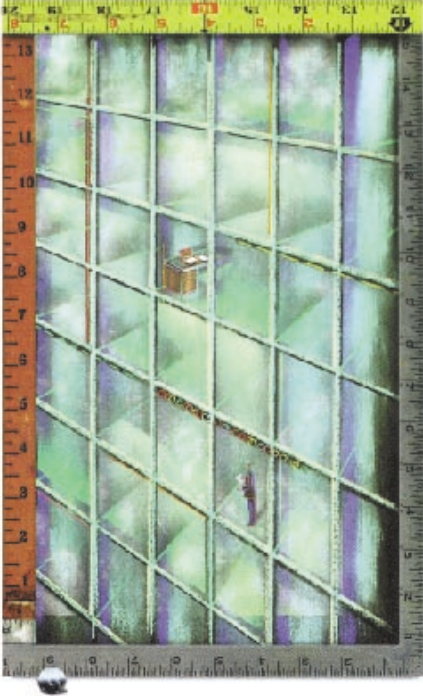
İnternet olsun, sivil, askerî, "olağan" haberleşme ya da bilgi iletişiminin, varolan bilgisayar teknolojisine getirdiği yük, bazı özel gereksinmelerin istediği hesaplama gücü ve hızı yanında solda sıfır kalıyor. Doğanın sınırlarını çözmek için gereken hesapları yapabilmek, en hızlı süper bilgisayarların binlerce yılı-

nı gerektiriyor. Örneğin atomları oluşturan temel parçacıkların işleyişini çözmek, akılların alamayacağı karmaşıklıkta hesaplar gerektiriyor. Çünkü bu dünya, bildiğimiz, tanıdığımız makroskopik dünyadan çok farklı. Bu dünyanın kuralları, ilkeleri, yasaları, büyük ölçekli dünyanın ilişkileri üzerine kurulmuş düz mantığımızın kabul edebileceği şeyler değil.

Kuantum dünyasının sihirli anahtarı, işte bu bize ters gelen belirsizlik. Alman Fizikçi Werner Heisenberg'in ortaya koyduğu "belirsizlik ilkesi" uyarınca bir parçacığın durumu, hiçbir zaman kesin bir değerle belirlenemiyor. Yani konumundaki belirsizlikle, hızındaki belirsizliğin carpımı, her zaman sıfırdan büyük olmak zorunda. Bu nedenle parçacığın hızını belirlemek için yapılan gözlem, parçacığın konumunu değiştirir. Dolayısıyla, örneğin bir protonun çevresinde dolanan tek bir elektronun



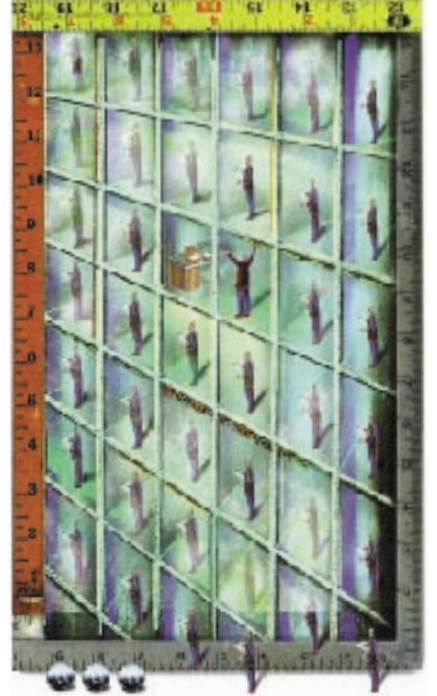
bile yörüngesini kesin olarak belirlemek, ya da elektronun belli bir anda nerede bulunduğunu saptamak olanaksız. Bu nedenle elektronun yörüngesi, bir olası yörüngeler bulutu olarak değerlendiriliyor. Kuantum kuramına göre, parçacıkların etkileşimlerini yöneten temel kuvvetler, aslında birer kuantum alanı, bu alanın akış düzgünlüğündeki küçük bozulmalar bir parçacık olarak "yorumlanıyor". Kuramcılar karşılıklı engelleri aşabilmek için madde- nin gözleme bağlı olarak bazen parçacık, bazen de dalga biçiminde davranabildiğini vurguluyorlar. Bizlere acayip gelen böylesine bir açıklama da şu: Gerçek olarak algıladığımız şey, aslında üst üste binmiş değişik gerçeklerden, gözlem koşullarımızın belirlediği bir seçim. Avusturyalı Kuantum kuramcısı Erwin Schrödinger, parçacıkların konumunun tek bir değer yerine tüm değişkenlerin olası durumlarını kapsayan bir dalga fonksiyonu ile açıklanabileceğini kanıtladı. Bir ölçüm yapıldığında bu dalga fonksiyonu "çöküyor" ve olası konumlardan yalnız birisi ölçümümüze takılı kalıyor. Bu açıklamanın modern biçimi olan "çoğul dünyalar" yorumu çok sayıda paralel gerçeklik içeriyor. Yorumu göre gözlemci, ancak içinde rastlantısal olarak bulunduğu konumu algılayabiliyor. Bu paralel gerçekler sürekli bir uyum içinde. Ancak bu uyum çok çabuk bozulabiliyor. En küçük bir etki,



1. İş merkezinde odalardan birinde çantanızı unuttuğunuzu düşünün. Yapacağınız, odaları teker teker dolaşmak. Yani, hareketleriniz birbirini izleyecek. Tıpkı bir bilgisayarın yaptığı gibi...



2. İsterseniz aramayı hızlandırabilirsiniz: Her kat için bir arama ekibi oluşturulur; sonra da herkes toplanıp, sonuçlar karşılaştırılır. Sıradan bilgisayarlar,bunu da yapabilirler. Biraz daha pahalı olsa da...



3. Kuantum dünyasındaysa, kendinizin oda sayısı kadar kopyasını yapabilirsiniz. Her kopyanız odalarda aynı anda çantanızı arayabilir ve anında bulabilir. Çantayı bulan kopyanız dışındaki tüm ötekiler yok olur...

bu uyumu bozuyor ve biz ancak içinde kaldığımız gerçeği görebiliyoruz.

Kuantumun bu kuramsal belirsizliklere rağmen sergilediği deneysel başarı, bu çok gerçeklik ortamında hesaplama yöntemlerine olan ilgiyi yoğunlaştırıyor. Şimdi büyük ölçekli dünyada da kuantum bilgisayarlar abartılı beklentilerin konusu. Bilgi işlem sürecine bu radikal yaklaşım öylesine büyük ufuklar açıyor ki, gökbilimcilerden, askerlere; çekirdek fizikçilerinden haber alma örgütlerine kadar giderek çoğalan sayıda "müşteri", son yıllarda hızlanan araştırmaların ürünlerini sabırsızlıkla bekliyor. Bu alanda yapılan ilk örnekler, beklentiler karşısında gülünç kalacak kadar ilkel. Araştırmacıların heyecanla birbirlerine bildirdikleri, ya da resmi ve askeri laboratuvarların kısıncıklıkla gizlemeye çalıştıkları ilk kuantum bilgisayarların şimdilik yapabildikleri, örneğin, dört isim arasından belirli özellikler taşıyan birini seçmek. Ama bunu, en hızlı bilgisayarlardan çok daha hızlı biçimde yapabiliyorlar. Bu bile kuantum bilgisayar dünyasında sevinç çığlıklarının yankılanmasına yol açıyor.

Klasik bilgisayarlar "bit" denen ve "0" ile "1"den oluşan iki farklı

sayının çeşitli dizilimleri temelinde işlem görüyor. Kuantum bilgisayarların "kubit" (kuantum bit) denen işlem birimiye, bekleneceği gibi biraz değişik: Bir kubit aynı anda hem "1", hem de "0".

Peki bu kuantum bilgisayarları neden bu kadar çekici? Kendinizi, büyük bir şirketin bir gökdeleni kaplayan merkezinde çalışan bir yönetici olarak düşünün. Diyelim ki kapıdan çıkarken birden değerli kâğıtlarınızın, o gece mutlaka incelemeniz gereken hesapların bulunduğu çantanın, elinizde olmadığını fark ettiniz. Düşünüyorsunuz, çantanın o gün girip çıkmış olduğunuz yüzlerce odadan hangisinde kalmış olabileceğini çıkartamıyorsunuz. Yapılacak şey, odalara tek tek girip çıkarak, kayıp çantanızı aramak. Yani, bir bilgisayar gibi adım adım ilerlemek. Bilgisayarınız,



Kuantum bilgisayarlar dev boyutlu süper bilgisayarlara olan gereksinmeyi ortadan kaldıracak.

benzer bir görevle karşılaştığında ne yapar? "0" ve "1" den oluşan uzun dizileri teker teker tarayarak sonunda aranan yanıtı bulur. İkinci bir yöntem, yardımcıların tek tek katlara dağıtmak, sonra oturup onların dönmesini beklemek ve elde ettikleri sonuçları karşılaştırmak. Sıradan bilgisayarlarla buna benzer işlemler de yapabilirsiniz. Bilgisayarınız yapılacak işi daha küçük parçalara böler, ve işlemleri paralel olarak, ayrı bilgi işlemciler kullanarak yerine getirir. Doğal olarak bu yöntem önemli ölçüde eşgüdüm ve iletişim gerektirdiği için oldukça pahalı.

Şimdi de, şöyle bir olanağı düşünün. Binada kaç oda varsa kendinizin o sayıda kopyasını anında yaratabileceksiniz; bu değişik kopyalarınızın her biri, aynı anda binanın tüm odalarına girip etrafa bakacak. Ve işin en hoş yanı, aramanın sonunda yalnızca çantayı bulan kopyanız ayakta kalacak, bütün ötekiler ortadan kayboluverecek... İşte kuantum bilgisayarlardan beklenen şey de, tamına bu. Çünkü, mikroskopik ölçekteki "şirket"lerin görevlileri yani atomlar ve parçaları birden çok gerçeklik içinde bulunabiliyorlar. Yani aynı anda hem orada, hem burada; hem hızlı, hem ya-

vaş; hem aşağı, hem de yukarı bakıyor olabiliyorlar. Bu atom durumlarının her birini farklı bir sayı, ya da veriyi temsil ediyor kabul edebiliriz. Böylelikle de bir grup atomu, tüm bu değişik kuantum durumlarından yararlanarak, bir sorunun olası yanıtlarının tümünü aynı anda araştırmak için seferber edebiliriz. Akıllıca bir iki yöntemle de, doğru yanıtı temsil eden atom durumunu ya da birleştirimini (superposition) öne çıkarabiliriz.

Gününç derecede basit bir iki işlem-den ötesini yapabilecek bir kuantum bilgisayar, bugünden yarına gerçekleştirilebilecek bir şey değil. Ancak hızlanan çalışmalar, işe yarar bir örneğin de üç-dört yıl sonra ortaya çıkabileceğini gösteriyor. Ama bu, kuantum bilgisayarların normal yaşantımız içinde yerlerini sağlama aldıkları anlamına gelmiyor. Çünkü ister kuantumu, isterse normali olsun, bir bilgisayar, pratik bir işlem yapmak için programlanmadıkça bir işe yaramaz. Bazı araştırmacılar, kuantum bilgisayarların, büyük ölçekli bir dünyanın gerektirdiği hesapların üstesinden gelebileceklerinden, ya da en azından bu hesapları normal bilgisayarlardan daha hızlı yapabileceklerinden kuşkuludur. Çünkü günlük yaşamımızda karşı karşıya geldiğimiz sorunların çoğu, bir makinenin parçaların bir araya toplanması gibi, bir algoritma kuramına göre hesaplamaların birbirini izleyen bir sırada teker teker yapılmasını gerektiriyor. Yani işlemi gerçekleştiren görevliler arasında, sonuca varmak için bir işbölümü gerekiyor. Bir kuantum bilgisayarın yapabileceği türden bir işte, çok sayıda görevliden yalnızca birinin, ötekilerden bağımsız olarak, istenen işi başından sonuna kadar yapabilmesi temeline dayanıyor. Yanlış sonuçlara doğru yönelmiş öteki görevlilerin tümünün doğru yanıtı "çökmeleri" gerekiyor. Kuantum bilgisayarları ötekilerden ayıran fark, işte bu "yanlışların kaybolması". Bu beceri de atomların hem parçacık hem de dalga gibi davranabilme özelliklerinden kaynaklanıyor. Atom durumları, yani dalgalar, birbirlerini güçlendirecek (doğru) ya da yok edecek (yanlış) biçimde üst üste gelebiliyorlar. .

Bu tür bilgisayarlar, bize pratik ne sağlayacak? Aslında uzun yıllar kuantum bilgisayarlara, atomaltı dünyanın karmaşık hesaplarını yapacak garip bir araç olarak bakıldı. Ancak, 1994 yılında



Kuantum mantığı 1

Üç yolcu ayaklarını yere vuruyor. Dördüncüsü katıldığında minibüs sallanmaya başlıyor.



Kuantum mantığı 2

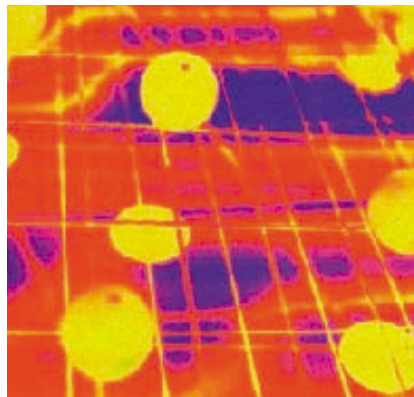
Sallanmadan korkan ilk üç yolcu vurmaktan vazgeçiyor ve minibüs de artık sallanmıyor.



Kuantum mantığı 3

Üç kişi daha ayak vurunca araç yeniden sallanıyor. Etkileşim bir işlem biçimi oluyor.

AT&T araştırmacısı Peter Shor, kendi olağan dünyamızın zorlu bir matematik sorununun da , kuantum bilgisayarlarınca çözülebileceğini öne sürdü. Sorun, büyük sayıların, 1,3,5,7.. gibi asal (kendinden başkasıyla bölünemez) çarpanlarını bulabilmek. "E, bunda ne var?" diyeceksiniz. Bunları ilkokulda öğrenmedik mi? Ama bu sayılar biraz uzun olunca iş değişiyor: Şöyle 250 ya da daha çok haneli türünden... Bunların asal çarpanlarını bulmak, süper bilgisayarlar için bile bir karabasan. Shor, karışık bir dizinin, kendini tekrarlamaya başladığı noktaların bulunmasıyla işin büyük ölçüde kolaylaşacağını düşündü. Bunu yapmak için gereken şey, dizinin tüm unsurlarını kubitlere yüklemek. Dizinin birbirine eş –yani tekrarlanan– bölümlerini temsil eden durumları yansıtan kubitler bir araya gelerek birbirleri-



ni güçlendirecek, bir süre sonra da tüm ötekileri kovarak yanıtı ortaya koyacaklardı. Kuramsal olarak 5000 kubitlik bir bilgisayarın, normal bir süper bilgisayarın 10 milyar yılda yapabileceği bir hesaplamayı, yalnızca 30 saniyede yapabileceği hesaplanıyor. Shor, bu başarısından dolayı 1998 yılında, alanlarında olağanüstü işler başaran bilim adamlarına verilen Fields Madalyası'nı aldı.

Herhalde kuantum bilgisayarın bu hünerinin en çok kimi heyecandırdığını tahmin ettiniz. Elbette ki, ABD'nin haber alma örgütlerinden en esrarengizi olanı: Ulusal Güvenlik Konseyi (NSC). Bu örgütün uzmanlık alanı, dost düşman tüm ülkelerin gizli haberleşmelerini dinleyerek, süper bilgisayarların yardımıyla şifrelerini çözmek. Bu şifrelerde kullanılan sayı dizileri, tam da kuantum bilgisayarların hoşlanacağı türden. En az 250 haneli...

Başka müşterilerin de gözleri parlamıyor değil. Çünkü bu bilgisayarlar, banka hesapları, kredi kartı işlemleri, uydu iletişimi gibi alanlarda da yepyeni ufuklar açıyor.

Gelgelelim, şifre kırıcı kuantum bilgisayarlar, 21. yüzyıl için bile zorlu bir hedef. Şimdilik, bir kubitlik "bilgisayarlar" başarı sayılıyor. Bunların bile boyutları bir hayli büyük. Önemlice bazı problemleri klasik bilgisayarlardan ancak biraz daha hızlı çözebilecek kuantum bilgisayarların bile, en az 50 kubit içermesi gerekiyor. Haber alma örgütlerininse biraz daha beklemleri gerekecek. İstedikleri türden hesapları yapabilecek kuantum bilgisayarların, (örneğin 100 000 kubitlik) bir hangar büyüklüğünde olacağı hesaplanıyor. Olsun; NSC için sorun değil. Araştırmaları hızlandırmak için keşenin ağızını açmış bile.

Araştırmacılar içinse temel sorun bilgisayarların boyutu değil. İleride, katı hal kristalleri ve silisyum üzerine basılmış optik dalga yönlendiriciler sayesinde, kubitlerin normal bilgisayar işlemcileri boyutlarına indirilebileceğini söylüyorlar. Onları asıl düşündüren, kubitleri birbirleriyle nasıl bağlayabilecekleri. Kaliforniya Teknoloji Enstitüsü (Caltech) araştırmacılarından Jeff Kimble, tek kubitlik iki ünitiden oluşan bir kuantum bilgisayar "ağı" üzerinde çalışıyor. Henüz başaramamış ama kendine güvenli. İletişim aracı olarak Kimble, foton üzerinde duruyor. Bir odacık içinde elektromanyetik alanların aynı anda

iki farklı kuantum durumunda tuttuğu tek bir atom düşünün. Elektromanyetik alanlarla oynanarak atom, bir foton yayınlamaya zorlanacak. Foton da, tıpkı çıktığı atom gibi aynı anda iki ayrı kutuplanma durumunda bulunacak. Kuantum hesap mantığına göre, atomun durumundaki bir değişiklik, fotonun durumunu da etkileyecek ve böylece atomla fotonu, "iki kubitlik" bir sistem olarak işlev görecektir. Daha önemlisi, atom-foton kubit sisteminin fotonu, ışık hızıyla başka bir atoma çarparak onu da bir kubit durumuna sokabilecek, böylelikle kuramsal olarak, her biri bir kubit anlamına gelen atom-foton-atom... gibi istendiği kadar uzatılacak zincirler oluşturulabilecek.

İş bununla da bitmiyor. Daha önce gördük ki, parçacıkların aynı anda birden çok kuantum durumunda bulunması için, çoklu durumların bir uyum (coherence) içinde bulunmaları gerekiyor. Oysa gene gördük ki en ufak dış etki, örneğin sisteme yalnızca bir fotonun değmesi bile bu uyumu bozuyor ve parçacık tek bir duruma "çöküyor".

Bazı araştırmacılar, atom, elektron, ya da iyon gibi bilgi taşıyıcıları arasındaki uyumun bozulmasını önlemek için bunları pahalı yalıtım cihazları içine hapsedmeyi öneriyorlar. Johns Hopkins Üniversitesinden James Franson ise, önceleri herkesin dudak büktüğü, şimdiye ilgiyle izlediği bir yöntem deniyor. Kuantum hesap yönteminin zorluklarından biri uygun malzeme. Çünkü kullanacağımız malzeme, bir kere yabancı etkileri duymayacak. Ayrıca hesaplama işleminin gerçekleşmesi için kullanılan malzemelerin birbirleriyle etkileşmesi gerekli. Işık, bu amaç için hem uygun, hem de değil. Uygun; çünkü dış etkilere daha az açık. Ayrıca optik kablolar içinden geçebiliyor. Uygun değil; çünkü etkileşmesi zayıf. Kütleli ve elektrik yüksüz fotonlar birbirleriyle nadiren etkileşiyorlar. Bu nedenle iki ayrı yönden gelen ışık demetleri birbirlerinin içinden rahatlıkla geçip gidiyor. Franson, işte ışığın bu özelliğini değiştirmeye çalışıyor. Eğer başarılı olursa kuantum mantık kapıları son derece ucuzlayacak. Bu mantık kapıları hesaplama için gerekli. Bir işlem için bir kubit, birçok mantık kapısından geçmek zorunda. Bunlar kuantum dünyasının



paralel evrenleri olarak düşünülebilir. Bu evrenlerden birinde işlem, sanki bit "0" değerindeymiş gibi, ötekindeyse "1"miş gibi gerçekleşir. Çok kubitli bir bilgisayar, "paralel evrenlerde" çok sayıda hesap yapabilir. Olası hesaplamaların sayısı, kubitlerin kuvvet katlarına orantılı olarak artar.

Az önce kubitlerin, dış etkilerden korunması gerektiğini söylemiştik. Oysa mantık kapılarından geçerken etkilenmemek bir hayli güç. Örneğin bir elektron, bir kapıdan geçerken çoklu kuantum durumunda ancak bir nanosaniyeden (saniyenin milyarda birinden) daha az süreyle kalabiliyor. Fotonlara daha dayanıklı. Vakum içinde fotonu rahatsız edecek herhangi bir şey yok. Fotonu bir şeffaf optik kablo içine koysanız bile içinde bulunduğu çoklu durumu en az bir milisaniye (saniyenin binde biri) süresince koruyabiliyor. Yani elektrondan bir milyon kere daha uzun. Bu da kuantum hesaplar için yeterli zaman bırakıyor. Fotonu uygun bir araç kılan bir özelliği de, kutuplanmasının bir "anahtar" olarak kullanılabilmesi. Yani düsey kutuplanma "0", yatay kutuplanmaysa "1" olarak işlev görebiliyor. Franson işte bu kutuplanmayı sağlamaya uğraşiyor.



Fotonlar kolay etkileşmedikleri için işi kolay değil. Çoğu kez ışık demetleri birbirinin içinden geçip gidiyor. Ancak Franson, Kerr Etkisi denen bir olgudan yararlanıyor. Bazı kristalimsi maddeler içinde kuvvetli bir foton, daha zayıf olanın kutuplanmasını değiştirebiliyor. Caltech'li araştırmacının yaklaşımı Kerr Etkisi ayesinde iki fotonu bir ortam içinde çarpıştırarak kutuplanmalarını değiştirmek. Ancak fotonlar arasında çarpışmalar gene de tek tük oluyor. Franson'un aradığıysa, belli bir düzene göre gerçekleşen

çarpışmalar: Birbirinden biraz farklı A ve B dalga boylarında iki foton, ortam içinden geçerken, ortamın içindeki bir atom, A dalga boylu fotonu soğuracak ve B dalga boylu bir başka foton yayımlayacak. Biraz ötede bir başka foton, B dalga boylu fotonu soğurarak bir A fotonu yayımlayacak. Kuantum mekaniği, bu tür foton değiş-tokuşunun küçük bir kutuplanma farkına yol açmasını öngörüyor. Ama bu değişim normal olarak ölçülemeyecek kadar küçük gerçekleşiyor. Gelgelelim, araştırmacı, kuantum belirsizliklerinden yardım alıyor. Ortamdaki atom denizi içinde, hangi atom çiftinin sisteme giren iki fotonu soğurduklarını saptamak olanaksız. "Bu durumda elinizde, birbirinden ayırt edemeyeceğiniz bir olasılıklar toplamı kalıyor" diyor Franson. Kuantum kurallarına göre her olası değiş-tokuş, toplam etkiye katkıda bulunuyor. Etki, medyumdaki atom sayısının karesiyle orantılı olarak büyüyor. Ve çok az miktarda madde içinde bile muazzam sayıda atom bulunduğundan, ikinci fotona verilen eksen bükülmesi, işe yarayacak kadar büyüyor.

Franson, sodyum buharı kullanarak denediği bir kuantum mantık kapısında gerçekleştirdiği foton çarpışmalarında üç derece kadar bir kutuplanma kayması elde edebilmiş. Bu, henüz yeterli değil; Çünkü kubit zincirinin oluşması için 90 derecelik bir açıyla bükülmüş kutuplanma gerekiyor. Gene de yöntem, bilim dünyasında ilgi uyandıracak kadar önemli. Öyle ki, "Jim Franson işi tamamlarsa Nobel'i götürür" deniyor.

Raif Gürdilek

Kaynaklar:

Aharonov, D., *Quantum Computation*, Hebrew University, 15 Aralık 1998
 Buchahah, M., *Qubits Go Out For a Spin*, New Scientist, 2 Ocak 1999
 Freedman, D. H., *The Great Quantum Number Cruncher*, Discover, Ocak 1999
 Taylor, R., *Jim's Bright Idea*, New Scientist, 6 Haziran 1998