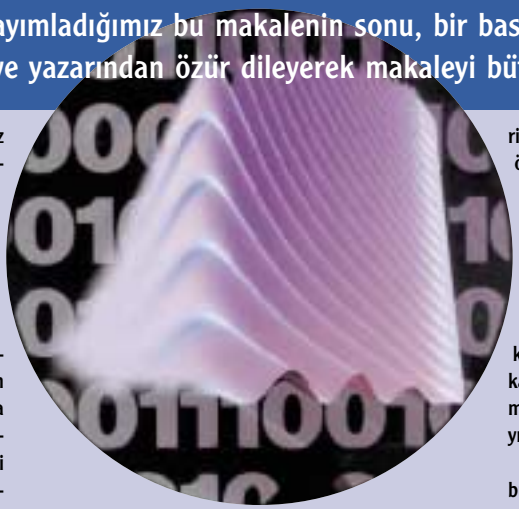
KUANTUM BİLGİSAYAR

Daha önce Nisan sayımızda yayımladığımız bu makalenin sonu, bir basım hatası sonucu birkaç satır eksik çıktı. Okurlarımızdan ve yazarından özür dileyerek makaleyi bütünüyle tekrar yayımlıyoruz.



Bir teknolojik devrimin temelleri geçtiğimiz yirmi yıl içinde sessiz sakin bir şekilde atıldı. Henüz ortada çalışan bir modeli yok, yakın gelecekte de olacağı kuşkulu. Fakat, teknolojik gelişmenin hızı dikkate alındığında, belki bir yirmi-otuz yıl sonra kuantum bilgisayarların piyasada satışa çıkacağından şüphe duymamak gerekir.

Kuantum bilgisayarlar, klasik akrabalarından farklı olarak, mikroskopik dünyaya hükmeden kuantum yasalarına dayalı olarak çalışacaklar. Son yıllarda yapılan kuramsal araştırmalar, çalışma mekanizmasındaki bu değişikliğin sonucunda kuantum bilgisayarların bir takım zor problemleri daha kolay çözebileceğini gösteriyor. Henüz hangi problemlerin çözülebileceği tam olarak bilinmiyor, ama bilinenler, bu bilgisayarların işlem gücü hakkında heyecanlanmamıza yetiyor.

Fakat bu, kuantum bilgisayarların piyasaya çıktığı gün, bugün kullandığımız klasik bilgisayarların çöpe atılmaya başlanacağı anlamına da gelmiyor. Kuantum bilgisayarlar çok farklı şekilde çalışıyor olacaklar. Örneğin, kelime işlemci programlarda sıklıkla kullandığımız "Kopyala-Yapıştır" fonksiyonunun bu bilgisayarlarda olmayacağını söylersek ne demek istediğimiz kısmen anlaşılabilir sanırım. Doğanın gizemli yasaları, böyle bir fonksiyonun kuantum bilgisayarlarda kullanılmasına izin vermiyor. Kısaca söylemek gerekirse, bu bilgisayarları 'kuantum oyunlar' oynayıp, 'kuantum ödevler' hazırlamak için kullanamayacaksınız.

Kuantum İletişim

"Peki bunlar ne işe yarayacak?" diye soruyorsunuzdur. "Hiç olmazsa İnternet'te bu bilgisayarlarla sörf edemez miyiz?" Bu son soruya kısmen olumlu cevap vermek mümkün: Kuantum yasalarının verdiği olanaklarla istediğiniz kişiyle gizli bir haberleşme yapabilir, üçüncü bir kişinin konuşmalarınızı dinlemesine kesin bir şekilde engel olabilirsiniz. Değişik bir kaç yöntemin geliştirildiği bu uygulama alanına "kuantum kriptografi" deniyor.

Kriptografi, matematiğin askeri kullanımları ağır basan çok eski bir alanı. Kuantum kriptografinin önemli deneylerinden birinin Beyaz Saray ile Pentagon arasında yapıldığını söylersek herhalde konunun önemi daha iyi anlaşılabilir. Fakat, kriptografinin geniş sivil uygulamaları da var. Örneğin, İnternet'te kredi kartıyla alış verişte kart numaranızın iletilmesi, bu tip sivil uygulamalardan en çok bilineni. Özellikle son 30 yılda bu konuda önemli gelişmeler yaşandı.

Geliştirenlerin soyadlarıyla anılan Rivest, Shamir ve Adleman (RSA) şifreleme sistemi, sivil uygulamalar için kullanılan yöntemlerden biri. Şu anda İnternet'te sıkça kullanılan Pretty Good Privacy (PGP) paketi bu yönteme dayanıyor. Eğer bir-risiyle gizli bir haberleşme yapmak istiyorsanız, öncelikle kısa bir ön haberleşme yapıyorsunuz. Bu ön görüşmede kullanacağınız protokolü ve anahtarı belirledikten sonra, mesajınızı RSA ile şifreleyerek gönderiyorsunuz. Doğal olarak, meraklı bir üçüncü kişi, ön görüşmenizi ve şifreli mesajınızı ele geçirebilir (kriptografinin en temel problemi: Mesaj yanlış ele geçebilir). Fakat meraklı, mesajınızın içeriğini öğrenmeye kalktığında karşısında çözülmesi oldukça zor bir matematik problemi bulacaktır: Büyük bir tam sayının çarpanlarına ayrılması.

Küçük bir sayının (örneğin 15) çarpanlarını bulmak çocuk oyuncağıdır. Fakat, problemi çözmek için kullandığınız yöntemi dikkatle analiz ettiğinizde, problemin zorluğunun katlanarak arttığını görebilirsiniz. Örneğin, bir milyona yakın 6 rakamlı bir sayının çarpanlarını bulmak istiyorsunuz diyelim. Çarpanlardan en azından birinin 3 rakamlı olması gerektiğinden yola çıkarak, 2'den 999'a kadar bütün sayıları (ya da asal sayıları) denemeniz gerekiyor. Kısacası 1000'e yakın bölme işlemi yapmayı göze almanız gerek. Eğer sayı bir trilyona yakın 12 rakamlı bir sayı ise, bu defa 2'den başlayarak yaklaşık bir milyona kadar sayıları denemeniz gerekiyor. Burada dikkat edilmesi gereken en önemli nokta, problemde verdiğiniz sayının rakamlarını 6 artırdığınızda, yapmanız gereken işlem sayısının bin kat artması.

Şimdi de, iki tane 500 rakamlı asal sayının çarpımından elde edilen 1000 rakamlı bir sayının verildiğini, ve sizden bunun çarpanlarını bulmanızın istendiğini düşünün. Yukarıdaki yöntemle, yaklaşık 10^{500} tane sayıyı teker teker denememiz gerekiyor. İşinizin ne kadar zor olduğunu daha iyi

RSA Nasıl Çalışır?

1979 yılında Ron Rivest, Adi Shamir ve Leonard Adleman'ın geliştirdiği şifreleme sistemi RSA, gücünü büyük sayıların çarpanlarına ayrılması problemindeki inanılmaz zorluktan alıyor. Sistemin temeli, ünlü matematikçi Euler'in modüler aritmetikte bulduğu çok eski bir bağlantıya dayanıyor.

Euler, belli bir N sayısına göre modüler aritmetik yapıldığında, bu sayıyla ortak çarpanı olmayan başka bir sayının üslerinin birisinin 1 kalanını verdiğini biliyordu. Örneğin, N=14 durumunda, 3 sayısının üsleri 3, 9, 27, 81, 243, 729, 2187, ... şeklinde bir dizi oluşturur. Bu sayılar 14'e bölündüğünde sırasıyla 3, 9, 13, 11, 5, 1, 3, ... kalanlarını verir. Aynı şey 5 sayısıyla yapıldığında kalanlar 5, 11, 13, 9, 3, 1, 5, ... şeklinde başka bir dizi oluşturur. Her iki durumda, sayının 6'ncı üssü 14'e bölündüğünde kalanın 1 olduğuna dikkat ediniz. Doğal olarak, 7'nci üs sayının kendisini veriyor. Euler, hangi üssün 1 kalanı verdiğini herhangi bir N sayısı için bulmuştu. Eğer N sayısının p ve q gibi iki asal çarpanı varsa, bu üs, m=(p-1)(q-1) şeklinde hesaplanıyor (N=14 için m=6). Olayın en güzel yönü, hangi sayıyı kullanırsanız kullanın, bir sonraki üssün sayının kendisini vermesi. Yani, N=14 durumunda, hangi sayıyla işlem yaparsanız yapın, 7'nci üs 14'e bölündüğünde aynı kalanı veriyor. Matematiksel olarak ifade etmek gerekirse, (Mod 14).

RSA sistemi, bu güçlü matematiksel sonucu kullanıyor. Örneğin Ali'nin, Berna'yla gizli bir şekilde haberleşmek istediğini düşünelim. Öncelikle, iletilecek mesajın sayılarla kodlanması gerekiyor. A=1, B=2, ..., Z=29 gibi bir kodlama bu iş için yeterli olacaktır. Eğer, güzel yazım kurallarına dikkat ediyorsanız, küçük harfler, boşluklar, noktalama işaretleri için de uygun bir kod seçebilirsiniz. Bu kodlama sistemine göre, örneğin "SELAM" mesajı "22, 6, 15, 1, 16" şeklinde kodlanacaktır. Bundan sonraki iş, bu kodları matematiksel bir işlemden geçirerek şifreli mesajın kodlarını elde etmek olacaktır.

Bu amaçla Ali iki tane p ve q asal sayısı seçerek bunları çarpar. Örneğin, p=3 ve q=11 ise, çarpım N=33 olacaktır. Bundan sonra, m=(p-1)(q-1) sayısını hesaplayarak, m ile ortak çarpanı olmayan rasgele bir a sayısı seçer (örneğin a=3). En sonunda a ve N sayılarını Berna'ya ileterek "Mesajındaki her sayının a=3'üncü üssünü al ve bunların N=33 ile bölündüğünde verdikleri kalanı bana ilet" der. İşin en garip yanı, Ali'nin bu (a,N) sayı çiftini başkalarının da duyabileceği şekilde bildirebilmesi. Bu nedenle bu sayı çiftine 'açık anahtar' (Public Key) adı veriliyor. Eğer N sayısı yeterince büyükse, bu iki sayının bilinmesi şifreleme sistemi için bir sorun yaratmıyor. Buna karşın, Ali'nin çok gizli tuttuğu büyük sırrı olan (p,q) sayı çiftine de 'özel anahtar' (Private Key) deniyor. Sistemin en önemli özelliği, özel anahtardan yola çıkılarak açık anahtarın rahatlıkla hesaplanması, ama tersinin mümkün olmaması. Açık anahtarı bilen hiç kimse, Ali'nin gizli kalmasına özen gösterdiği kapalı anahtarı hesaplayamaz; tabii, eğer büyük sayıları çarpanlarına ayırmanın kolay bir yolunu bilmiyorsa.

Berna "SELAM" mesajını göndermek istiyorsa, mesajındaki her sayının küpünü hesaplayarak [(Mod 33), (Mod 33), ...] şifreli mesajını "22,

anlatabilmek için, görünür evrendeki atom sayısının 10^{78} civarında olduğunu ekleyelim. Basit bir hesap yaparsanız, evrende bu problemi makul bir sürede çözme yeteneğine sahip paralel işlemcili bilgisayarı üretebilecek kadar bile madde olmadığını görürsünüz. Gerçi çarpanlara ayırma problemini çözen daha hızlı matematiksel yöntemler var; ama bunlardan en iyisiyle bile bugünkü teknoloji 250 rakamlı bir sayıda pes ediyor.

Bu problemin en önemli özelliği, tersinin, yani çarpma işleminin rahatlıkla yapılabilmesi. Kağıt üzerinde yapılamasa bile, iki tane 500 rakamlı sayının çarpımı herhangi bir bilgisayarla kısa sürede bulunabilir. İşte, RSA şifreleme sistemi, gücünü bu problemin zorluğundan alıyor. Herhangi birisi rahatlıkla iki asal sayı bulup, meraklı dinleyiciye çözmesi imkansız bir problem sunabilir. Ne yazık ki, RSA'nın en temel zayıflığı da bu noktada yatıyor. Hiç kimse bu problemin gerçekten kolay bir çözümü olup olmadığını bilmiyor. Kim bilir, belki bir gün bir matematikçi oldukça hızlı bir çarpanlara ayırma yöntemi geliştirecek ve o güne kadar gönderilmiş tüm mesajları okuyabilecek. Belki de bugün bizi izleyen uzaylılar (oradalar değil mi?) böyle bir yöntemi zaten biliyorlar ve gönderdiğimiz tüm mesajları okumaktalar. RSA sistemi bize bu anlamda hiç bir garanti veremiyor.

Bütün klasik kriptografi teknikleri de aynı zayıflığı paylaşıyorlar. Eğer şifreli mesajlarınızın dinlenme olasılığı varsa (ki tüm uygulamalarda bu olasılık her zaman vardır), dinleyicilerin o şifreyi kıracak yeterli bilgi ve teknolojiye sahip olma olasılığı da vardır. Bugünkü teknoloji yeterli olmasa bile, gelecekteki olacaktır. İkinci Dünya Savaşı sırasında Almanların çok güvendikleri şifreleme sistemi Enigma'nın, tahmin etmedikleri bir teknolojik gelişmeyle, bilgisayarla kırıldığını hatırlamakta fayda var. Almanların yenilgisinde bilgisayar çok önemli bir yer tutuyor.

İşte kuantum kriptografi bu noktada önemli bir yenilik getiriyor. Geliştirilen yöntemler, üçüncü bir kişinin bir haberleşmeyi dinleme olasılığını tamamen ortadan kaldırıyor. Üstelik ortada bir güvence de var: Doğa yasaları! Yani konuşmanızı ne uzaylılar dinleyebilir, ne de gelecekte ileri teknoloji ve bilgiye sahip olacak kişiler. Doğa bir şekilde bize güvenli haberleşmemiz için bir kapı açıyor. Bu yöntemleri daha iyi anlatabilmemiz için bu konuyu gelecek sayıya bırakıyoruz.

Kuantum Bilgisayarları Ne İşe Yarar?

Kuantum bilgisayarların hesap gücünü bize gerçek anlamda gösteren, AT&T Bell araştırma laboratuarlarında çalışan Peter Shor'dur. Shor, 1994 yılında yayımladığı bir makalede kuantum mekaniğinin temel özelliklerini kullanarak çalışan bir bilgisayarın büyük sayıların çarpanlarını çok hızlı bir şekilde bulabileceğini gösterdi. Problemi çözme hızı konusunda yapılan kaba hesaplar, klasik bilgisayarların imkansız gördüğü 250 rakamlı bir sayının çarpanlarının bulunması işleminin iki gün gibi bir süre içinde yapılabileceğini gösteriyor. Herkesi heyecanlandıran şey, kriptosistemler bağlamında bir çok kişiyi meşgul etmiş bir problemin çözümünün "hiç bir zaman" gibi bir süreden "iki gün" gibi daha kısa bir süreye indirgenmesi. Stanford Üniversitesi'nden bir grup, Shor'un algoritmasını kullanarak 15 sayısının çarpanlarını bulmayı başardı. Bunu bulmakta ne var demeyin. Yöntemin tahmin edildiği gibi çalışıyor olması, gelecekte daha büyük sayıları çarpanlarına ayırabilecek gerçek kuantum bilgisayarların yapılabileceğini söylüyor.

Kuantum bilgisayarların daha iyi çözebildiği bir başka problem, sıralanmamış bir listede arama yapmak. Bir kelimenin anlamını bulmak için sözlüğe baktınız ve sözlükteki kelimelerin harf sırasında sıralanmadığını gördünüz! Ne yaparsınız? Yapabileceğiniz tek şey aradığınızı buluncaya kadar teker teker bütün kelimelere bakmak. Bir milyon elemanı olan bir listede, aradığınızı her hangi bir yerde bulabileceğiniz için ortalama 500,000 karşılaştırma yapmanız gerekiyor. Bundan daha iyisini yapabilmenizin imkanı yok. Fakat yine AT&T Bell laboratuarlarından Lov Grover, 1997 yılında geliştirdiği algoritma yardımıyla kuantum bilgisayarların bu işi yaklaşık 1,000 kadar adımda çözebileceğini gösterdi.

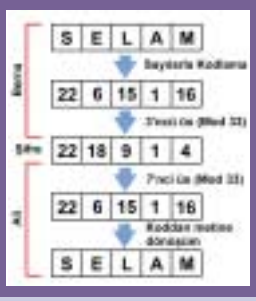
Sıralanmamış bir listede arama yapma problemi, ne yazık ki, büyük teknolojik uygulamaları olan bir şey değil. Nasıl sıralı sözlüklerden istediğiniz kelimeyi rahatlıkla bulabiliyorsanız, modern veri tabanı sistemleri, sıralı listeler ve indeksler oluşturarak aramayı çok kısa sürede tamamlıyor. İnternet'teki arama motorlarını kullananlar, bu yöntemlerin ne kadar gelişmiş olduğunu daha iyi anlayabilirler. Grover'in algoritmasının önemi, klasik anlamda 'umutsuz' olarak niteleyebileceğimiz bir problem üzerinde ilerleme sağlaması. Aynı şey Shor'un çarpanlara ayırma yöntemi için de geçerli. Bunlar dışında bir kaç tane daha problem için algoritma biliniyor; ama bunlar çoğumuzun ilgisini çekebilecek türden şeyler değil.

Peki öyleyse bu bilgisayarlar ne işe yarayacak? Günümüzdeki kuramsal araştırmaların çoğu bu soru üzerinde yoğunlaşıyor. Yukarıda saydığımız iki algoritma bu bilgisayarların işlem hızının çok önemli bir göstergesi. Öyleyse, daha henüz bilmediğimiz günümüzün önemli bazı problemlerini çözebilen çok sayıda algoritma olmalı. Umut vaat eden uygulama alanlarından biri, kuantum yasalarının önemli olduğu fiziksel sistemlerin (örneğin bir molekülün) kuantum bilgisayarlarla simulasyonu. Ünlü bilimadamı Richard Feynman, 80'lerin başlarında, klasik bilgisayarların kuantum yasalarına göre işleyen sistemlerin simulasyonunda karşılaştığı zorluktan yola çıkarak, bir kuantum bilgisayarın bu işi daha iyi yapabileceğini iddia etmişti. Bu tip bir simulasyonunsa çok önemli teknolojik uygulamaları olacağı kuşkusuz.

Kuantum bilgisayarlar konusundaki araştırmaların bugünkü durumu, ilginç bir şekilde klasik bilgisayarların 1930'lardaki durumuna benziyor. Bilgisayar biliminin kurucusu olarak görülen ünlü matematikçi Alan Turing, bu sıralarda "hesaplama" kavramı üzerinde çalışmalar yapıyordu. Turing, daha çok matematiksel bir teoremi ispatlayan mekanik bir makine düşünüyordu. Bu noktadan hareket ederek kendisine yüklenen bir programla çalışan ve 'Evrensel Turing Makinesi' olarak adlandırılan bir makine tasarlamıştı. Turing'in gösterdiği önemli şeylerden biri, Evrensel Turing Makinesi'nin, diğer olası bütün makinelerin yapabileceği her şeyi yapabilme, hatta herhangi bir insanın ispatlayabileceği bütün teoremleri de ispatlayabilme yeteneğiydi.

18, 9, 1, 4" olarak oluşturur ve bunu Ali'ye gönderir. Ali, şifreli mesajı çözmek için, öncelikle Euler'in formülünden m=(p-1)(q-1)=20 sayısını hesaplar. Sonra da, a=3 ile çarpıldığında m=20 ile 1 kalanını veren bir b sayısı bulur. Burada, b=7 seçildiğinde, ab çarpımı 21 verdiği için işlem kolay. Büyük sayılarda da bu çok zor bir işlem değil. Ali'nin orijinal metni görmesi için yapması gereken tek şey, şifreli mesajdaki her sayının b=7'nci üssünü almak ve N=33'e göre kalanını bulmak.

Eğer Ali, Berna'ya bir mesaj göndermek istiyorsa, bu kez Berna kendine özgü yeni anahtarlar oluşturacak ve yeni açık anahtarı Ali'ye gönderecek. Ali de mesajını, Berna'nın açık anahtarıyla şifreleyip gönderecek. Kısacası, Ali'ye mesajlar Ali'nin sistemiyle; Berna'ya mesajlar Berna'nın sistemiyle hazırlanıp gönderiliyor.



Doğal olarak, bu haliyle sistem o kadar da güvenilir değil. Şifreli mesajda her harfin belli bir sayıyla değiştirildiği bu tip sistemlerde, basit bir istatistiksel analizle orijinal mesajı bulmak mümkün. Bunu engellemek için orijinal mesaj daha büyük sayılardan oluşturulmalı. Örneğin SELAM mesajını "22, 6, 15, 1, 16" şeklinde beş sayıyla kodlamak yerine, 2206150116 gibi tek bir sayıyla kodlamak güvenliği artıracaktır. Tabii, bu durumda modüler aritmetiğin yapıldığı N sayısının da mesajdan daha büyük seçilmesi gerekiyor.

Bu şifreleme sistemindeki en garip nokta, Berna'nın mesajını kodlaması için bilmesi gerekenlerin herkes tarafından bilinmesinde bir sakınca olmaması. Eski kriptografik sistemlerde bu büyük bir sorun oluşturuyordu. Göndereceğiniz şifreli mesaj çoğu durumda herkes tarafından dinlenebilir (mesajınızı radyo dalgalarıyla ya da cep telefonlarıyla gönderiyorsanız bu çok doğal). Bu nedenle, şifreleme için kullandığınız anahtarın güvenli bir şekilde saklanması gerekir. Eğer kullandığınız anahtar bir şekilde ele geçmişse (metin analiziyle ya da casuslar sayesinde) haberleşmeyi devam ettirebilmek için yeni bir anahtar belirlemeniz gerekir. Fakat bu yeni anahtarı haberleştiğiniz kişiye nasıl ulaştıracaksınız? RSA sistemi bu sorunu tamamen çözüyor: Açık anahtarı normal yolla gönder; kimin dinlediği önemli değil. Üstelik bu tip bir haberleşmeyi daha önce hiç karşılaşmadığınız biriyle de yapabiliyorsunuz.

İnternet'teki uygulamalarda bu çok önemli. Örneğin, kredi kartıyla alış veriş yaptığınızı düşünelim. Kredi kartı numaranızı elektronik-mağazaya iletmek istiyorsunuz, ama bunu yaparken de başka hiç bir kimsenin bu numarayı öğrenmesini istemiyorsunuz. Yukarıda açıkladığımız kriptosistemle bunu yapmak çok kolay. Mağaza size kendi açık anahtarını iletiyor. Siz de bunu kullanarak kart numaranızı şifreli bir şekilde mağazaya bildiriyorsunuz. Üstelik, mağazanın her müşteri için yeni bir anahtar belirlemesine gerek yok. Her müşteri, aynı açık anahtarla numarasını gönderebilir, ve bunları ancak özel anahtarı elinde bulunduran mağaza okuyabilir.

Eğer ileri teknolojilere yatırım yapmak isteyen bir iş adamı Turing'le karşılaşsaydı, mutlaka "matematiksel teorem ispatlayan bir makine ne işe yarar ki?" derdi. İşin ilginç tarafı, bilgisayarın toplumun her alanına damgasını vurduğu günümüzde bile, hala "teorem ispatlayan bir program" yok. Fakat, Turing'in temel matematiksel sorular üzerine attığı temeller, bilgisayar kavramının gelişmesinde önemli bir aşama.

Bu nedenle, kuantum bilgisayarlar konusunda bugün yapılan çalışmaları, Turing'in çalışmalarına benzetmemiz gerekir. Hâlâ, cevap bekleyen temel sorular var. Bunlar cevaplandıktan uzun bir süre sonra, kuantum bilgisayarların hayatımızın her köşesine nüfuz edeceği günlerin geleceği kuşkusuz.

Bit

Kuantum bilgisayarlar hakkında yapılan çalışmaların bir bölümü 'bilgi' kavramı çevresinde yoğunlaşıyor. Bilgi, kolaylıkla tanımlayabileceğimiz bir şey değil: Bir sorunun cevabı olabilir (evet/hayır); ya da bir önermenin doğruluğu (doğru/yanlış); bir sayı ya da kredi kartı numarası da olabilir. Değişik fiziksel şekillerde de var olabilir: Havadaki ses titreşimleri, sabit disk üzerindeki manyetik alan ya da bellekteki bir voltaj farkı gibi. Fakat hepsinin ortak bir takım özellikleri var. Örneğin, o bilgiyi saklamak için ne kadar kaynak kullanmak gerektiği gibi.

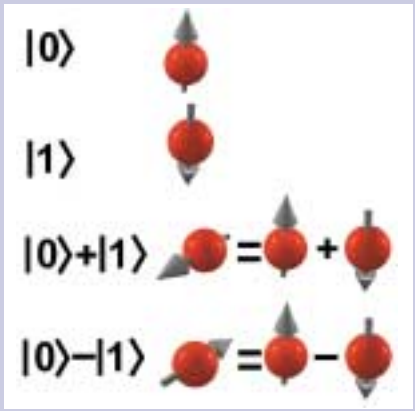
Klasik bilgisayarlarda en küçük bilgi birimine 'bit' deniyor. Bir bitlik bilgi taşıyabilen bir sistem iki farklı konumundan sadece birisini alabilir. Bilgisayar bilimciler bunları '0' ve '1' olarak gösteriyor. Bir bilginin miktarı, o bilgiyi saklamak için kaç bitlik bir kaynak ayırmak gerektiğiyle ölçülüyor. Örneğin, sadece 'evet' ve 'hayır' olabilen bir cevabı bir bitle kodlamak mümkün, ama eğer 'belki' cevabı da olasıysa, en az iki bit kullanmak zorundasınız. Yeteri kadar bit ile istediğiniz bilgiyi kodlayabilirsiniz. Örneğin, bin rakamlı herhangi bir sayıyı, yaklaşık 3,300 bit kullanarak gösterebilirsiniz. İlginç olan bir nokta, dünyamızda herhangi bir şeye karşılık gelemeyecek derecede büyük böyle bir sayının, çok az (3,300 bitlik) bir kaynak ayrılarak gösterilebilmesi.

Kubit

Eğer bir bitlik bilgi taşımasını istediğiniz sisteminiz mikroskopik ölçekteyse, o zaman kuantum fiziğinin yasaları saklamayı umduğunuz bilginin garip formlara bürünmesine neden oluyor. Çünkü, sisteminiz '0' ve '1' olarak yorumladığınız iki olası durumda bulunabileceği gibi, bu iki durumun üst üste gelmesiyle oluşan, ancak egzotik olarak niteleyebileceğimiz, sonsuz sayıda değişik durumlara da girebiliyor. Kuantum yasalarına uyan, iki düzeyli tüm sistemlerin bir 'kubit' bilgi taşıdığını söylüyoruz.

Bir kubitlik bilgi taşıyabilen çok sayıda sistem var: Bir fotonun polarizasyonu, bir elektronun ya da atom çekirdeğinin spini, bir atomun enerji seviyeleri, kısacası kuantum yasalarına uyan ve değişik durumlara girebilen her şey böyle bir bilgiyi taşıyabilir. Bitlerde olduğu gibi, kubitlerde de bilginin hangi fiziksel ortamda saklandığı önemli değil. Gerekli olduğu durumlarda bu bilgi bir ortamdan diğerine aktarılabilir.

Örneğin, iki düzeyli bir sistem olarak, bir elektronun spini böyle bir bilgiyi taşıyabilir. Her elektronu küçük bir mıknatıs olarak düşünebiliriz.



Bir elektronun bütün spin durumları iki temel durumun üst üste gelmesi olarak düşünülebilir.

Bu mıknatısın güney kutbunun gösterdiği yöne spinin yönü diyoruz. Doğal olarak, bu yön yukarı, aşağı, sağ, sol, ön, arka ve bunların dışındaki herhangi bir yeri gösteriyor olabilir. Bu nedenle de elektron spini sonsuz değişik durumda bulunabilir.

Fakat, kuantum fiziğinin garip yasaları, bu spin doğrultusunu iki düzeyli olarak yorumlamamız gerektiğini söylüyor. Bunun bir nedeni spinin yönünü belirlemek için yapılan her ölçümün sadece iki olası değer veriyor olması. Ölçümü yaparken, öncelikle uzayda bir doğrultu seçiyorsunuz, ve ölçüm sonucu olarak spinin ya bu doğrultu boyunca ya da tam tersi yönde olduğunu buluyorsunuz. Kuantum fiziğine göre, diğer tüm olası spin doğrultuları, deneyde bulunabilen bu iki özel durumun üst üste gelmesiyle oluşuyor.

Örneğin, yukarı-aşağı doğrultuda bir ölçüm yaptığınızı düşünelim. Yukarı yönelmiş bir spin '0' olarak, aşağı yönelmiş olan da '1' olarak düşünülebilir. Bu ikisi dışındaki durumlarda spin, hem '0' hem de '1' durumlarının her ikisinde de aynı anda bulunabilir. Böyle bir spin için, yukarı-aşağı doğrultuda yapacağınız her ölçüm belli bir olasılıkla ya '0' verecektir ya da '1'. Örneğin, eğer spin sağa ya da sola doğru yönelmişse, ölçüm sonucunda % 50 olasılıkla '0' ve yine % 50 olasılıkla '1' değerini bulursunuz.

Bir kubit sonsuz farklı olası değer taşıyabilmesine karşın, bu bilgiyi öğrenmek için bir ölçüm yapmalısınız ve ölçüm de size ancak iki olası değer verebilir: '0' ya da '1'. Kuantum algoritmaları tasarlarken önünüze çıkan en büyük engel işte bu. Üstelik, ölçümü yaptığınızda mecburen kubitteki bilgiyi tamamen yok ediyorsunuz. Eğer ölçüm size '0' değerini vermişse, o andan sonra sisteminiz '0' değerini taşımaya başlıyor; ölçümden önceki değeri ne olursa olsun. Bu da size, aynı kubit üzerinde ikinci bir ölçüm yapma şansı tanımıyor.

Kopyalamak Yasaktır!

Bir kubitten sadece bir bitlik bilgi okunabilmesi kuralının üstesinden gelmek için şöyle bir yöntem deneyebilirsiniz. O kubitteki bilginin, herhangi bir ölçüm yapmamaya dikkat ederek, binlerce kopyasını çıkarırsınız (kelime işlemcilerdeki Kopyala-Yapıştır fonksiyonu gibi). Bundan sonra her bir kopya üzerinde farklı ölçümler alırsınız. Bu binlerce ölçüm sonucunun istatistiksel analizinden, orijinal kubitteki bilgi hakkında (örneğin olasılıklar) istediğiniz şeyi öğrenebilirsiniz. Ne yazık ki, matematiksel olarak bir kubitteki bilginin kopyasını çıkarmanın mümkün olmadığı ispatlanabiliyor ve bu sonuç "Kopyalamak Yasaktır" (no cloning theorem) olarak biliniyor. Doğal olarak, aynı sonuç çok sayıda kubitten oluşan herhangi bir sistem için de geçerli. Kopyalama yasağı teoremi sanki bir kubitten ancak bir bitlik bilgi çıkarılabilmesi kuralını güçlendirmek için var.

Her ne kadar kuantum bilgisayarlarda kopyala-yapıştır fonksiyonu olamasa da, kes-yapıştır fonksiyonu mümkün. Yani bir kubitteki bilgiyi başka bir kubite aktarabiliyorsunuz ama bunun kaçınılmaz sonucu olarak, eski kubitteki bilgiyi değiştiriyorsunuz.

Kubitlerle Bilgi İşlem

Çok sayıda kubitle çok daha fazla bilgi taşınabilir ve bunlardan o kadar fazla bilgi okunabilir. Kuantum bilgisayarların ana işlevi, belleğindeki kubitlerdeki bu bilgileri uygun işlemlere sokmak olacak. Tek bir kubitteki bilgiyi değiştirmek genellikle zor değil. Örneğin, bir elektronun spini, uygun bir manyetik alan yardımıyla değişik yönlere döndürülebilir. Bunun dışında, iki elektronun etkileşmesi, spinlerinin de değişmesine neden olacaktır. Tıpkı, klasik bilgisayarlardaki gibi, bir kaç temel operasyonla, kubitler üzerinde yapabileceğiniz tüm olası dönüşümleri gerçekleştirebilirsiniz. Kuantum bilgisayarlar erişilecek amaca uygun olarak, hangi kubitlerin nasıl değişmesi gerektiğini kontrol edecek.

Kuantum bilgisayarın çalışmasının sonunda, bu bilgileri okumak için bir ölçüm yapılması gerekiyor ve yukarıda da değindiğimiz gibi, böyle bir ölçüm bellekteki orijinal bilginin silinmesine ve bize olası sonuçlardan sadece birisinin iletilmesine neden oluyor. Buna karşın, bazı özel tasarlanmış algoritmalarda bu olası sonuçlardan bazıları bize bulmak istediğimiz bilgiyi yüksek olasılıkla veriyor. Eğer, istediğimiz bilgiyi elde edememişsek, bilgisayarı yeniden çalıştırmak ve ölçümü tekrarlamak zorundayız. Algoritma yeterince iyiyse, az sayıda yeniden çalıştırma sonucunda istenilen sonuç elde ediliyor.

Kubitlerin taşıdığı bilginin en büyük özelliğinin, bunların aynı anda değişik bilgiler saklaması olduğunu söylemiştik. Örneğin, sağa doğru yönelmiş bir elektron spini, eşit olasılıkla hem '0' hem de '1' değerini taşıyor. Eğer bellekte 3,300 tane sağa doğru yönelmiş elektron spini varsa bu, yine eşit olasılıkla, bine kadar rakamı olan bütün sayıların aynı anda bellekte olması demek! Halbuki aynı miktarda klasik bit bu sayılardan sadece birini saklayabilir. Bu kadar çok fazla sayının, bu kadar küçük bir fiziksel kaynağa sığması kuantum bilgisayarların en güçlü yanı. Üstelik, toplama, çarpma, modüler aritmetik ve benzeri bir çok işlemi bu sayılar üzerinde tek bir işlemle yapmak mümkün. Kısacası, tek işlemle belli bir uzunlukta olan bütün sayıları çarpıp bütün olası çarpım sonuçlarını bulabilirsiniz. Bu olaya kuantum paralelliği deniyor.

Peter Shor'un büyük sayıları çarpanlara ayırmak için önerdiği algoritma da bu paralelliği kullanıyor. Doğal olarak, kubitlerde aynı anda bulunan bilgiler ne kadar fazlaysa, bunların içinde sizin elde etmeyi umduğunuz bilgiyi çekip çıkarmak da o oranda zor. Bu nedenle kuantum algoritmaların, istenen sonucun bulunma olasılığını artıracak şekilde zekice tasarlanması gerekiyor. Ve yine bu nedenle bilinen algoritmaların ve çözülebilecek ilginç problemlerin sayısı çok az.

Doç. Dr. Sadi Turgut
ODTÜ Fizik Bölümü

Kaynaklar
Lines, M. E., Bir Sayı Tut, TÜBİTAK Popüle Bilim Kitapları, Ankara 1998
http://www.qubit.org/
http://www.rsasecurity.com/rsalabs/faq/
http://www.turing.org.uk/turing/