ŞU GARİP KUANTUM-1

Yirminci yüzyıl fiziğinin en temel iki paradigmasından biri olan kuantum mekaniği, günlük yaşamımızdaki deneyimlerimize, içinde yaşadığımız büyük ölçekli dünyaya uyum sağlamış duyularımıza, bunlarla yapılan gözlemlere ve bunların üzerine kurulan klasik fiziğe, hatta mantığa ters gelen önerileriyle, 100 yıl sonra bile insanları şaşırtmaya devam ediyor. Öte yandan atomaltı ölçekteki ilişkileri son derece başarılı bir biçimde açıklayan kuantum mekaniğinin bu garip kuralları, yaşadığımız "normal" dünyamızda karşılaştığımız darboğazları aşmak için beklenmedik bir araç olmaya aday.
Bilim ve Teknik Dergisi, bu diziyle kuantum dünyasının garipliklerine ve bunların yaşamımıza getirdiği ve getireceği açılımlara ışık tutmayı amaçlıyor.

KUANTUM BİLGİSAYAR

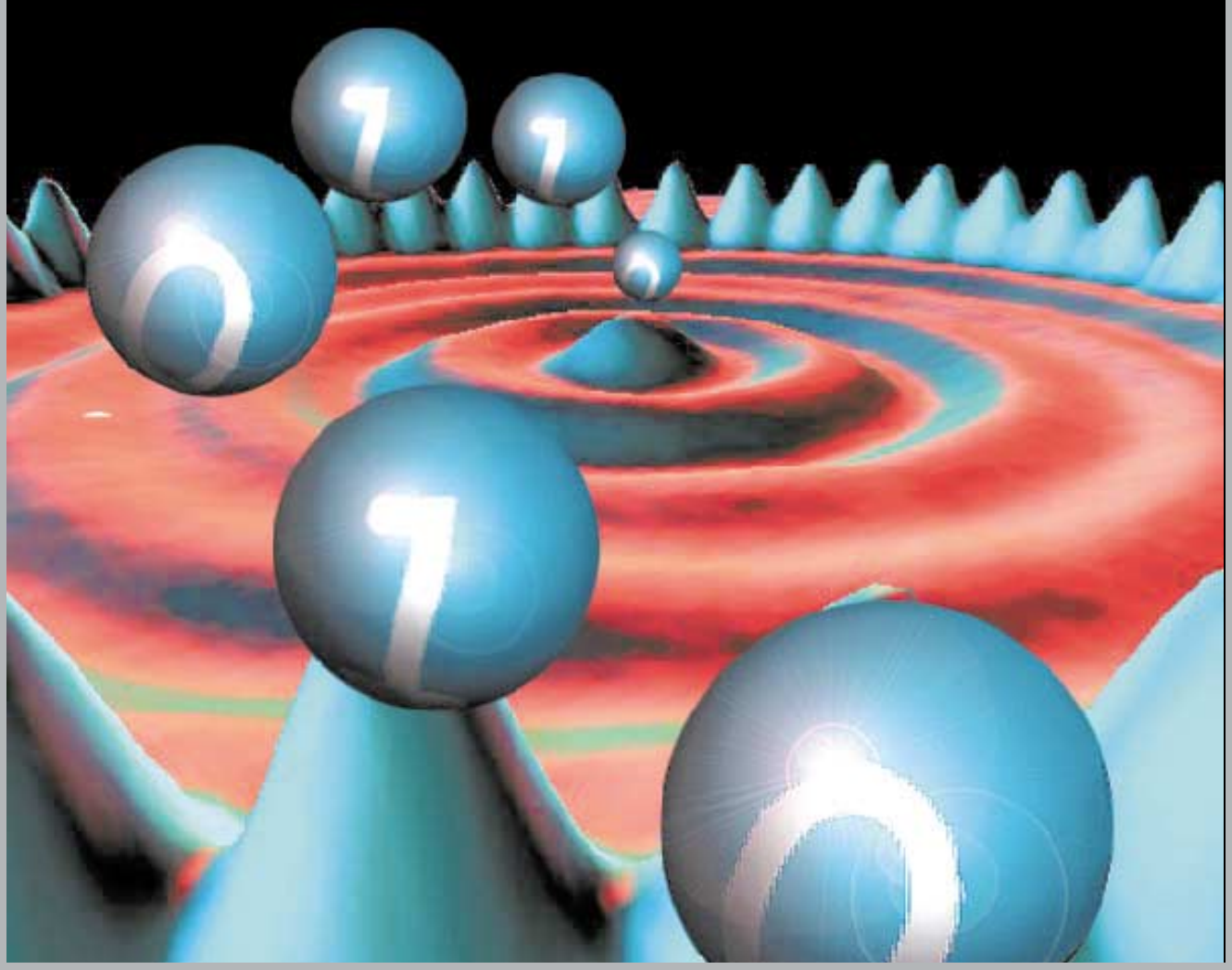
Bir teknolojik devrimin temelleri geçtiğimiz yirmi yıl içinde sessiz sakin bir şekilde atıldı. Henüz ortada çalışan bir modeli yok, yakın gelecekte de olacağı kuşkulu. Fakat, teknolojik gelişmenin hızı dikkate alındığında belki bir yirmi-otuz yıl sonra kuantum bilgisayarların piyasada satışa çıkacağından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

Kuantum bilgisayarlar, klasik akrabalarından farklı olarak, mikroskobik 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' hazırlanmak için kullanmayacaksınız.

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 soyadıyla 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 birisiyle 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 10500 tane sayıyı teker teker denememiz gerekiyor. İşinizin ne kadar zor olduğunu daha iyi anlatabilmek için, görünür evrendeki atom sayısının 1078 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

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.

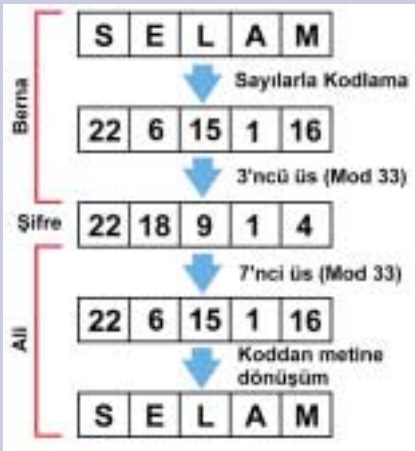
Euler, belli bir N sayısına göre modüler aritmetik yapıldığında, bu sayıyla ortak çarpanı olmayan başka bir sayının üslerinin birisinin 1 kalanını verdiğini biliyordu. Örneğin, N=14 durumunda, 3 sayısının üsleri 3, 9, 27, 81, 243, 729, 2187, ... şeklinde bir dizi oluşturur. Bu sayılar 14'e bölündüğünde 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, 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.

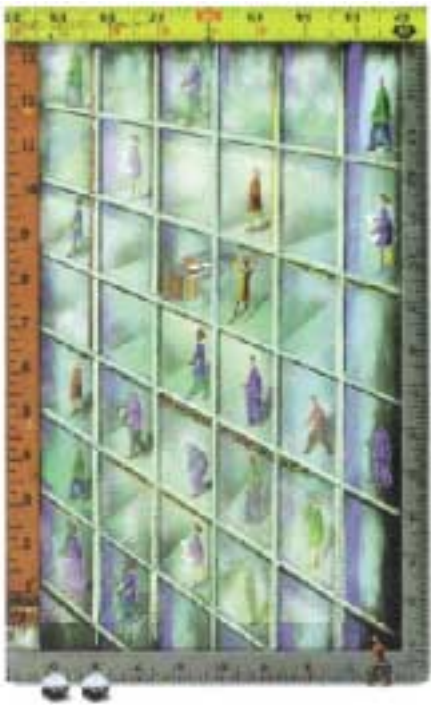
İnternet'teki uygulamalarda bu çok önemli. Örneğin kredi kartıyla alış veriş yaptığınızı düşünelim. Kredi kartı numaranızı elektronik-mağazaya iletmek istiyorsunuz, ama bunu yaparken de başka hiç bir kimsenin bu numarayı öğrenmesini istemiyorsunuz. Yukarıda açıkladığımız kriptosistemle bunu yapmak çok 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.

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 enigmanın, 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.

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...

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 bilim adamı 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 Makinesinin, diğer olası bütün makinelerin yapabileceği her şeyi yapabileceğini, hatta herhangi bir insanın ispatlayabileceği bütün teoremleri de ispatlayabileceğini göstermişti.

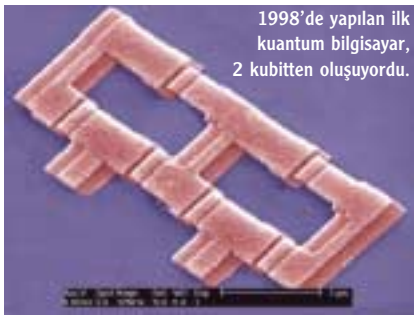
Eğer ileri teknolojilere yatırım yapmak isteyen bir iş adamı Turing'le karşılaşsaydı, mutlaka "matematiksel teorem ispatlayan bir makine ne işe yarar ki?" derdi. İşin ilginç tarafı, bilgisayarın toplumun her alanına damgasını vurduğu günümüzde bile, hala "teorem ispatlayan bir program" yok. Fakat, Turing'in 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. Hala, 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.


1998'de yapılan ilk kuantum bilgisayar, 2 kubitten oluşuyordu.

Kubit

Eğer bir bitlik bilgi taşımasını istediğiniz sisteminiz mikroskobik 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. 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.

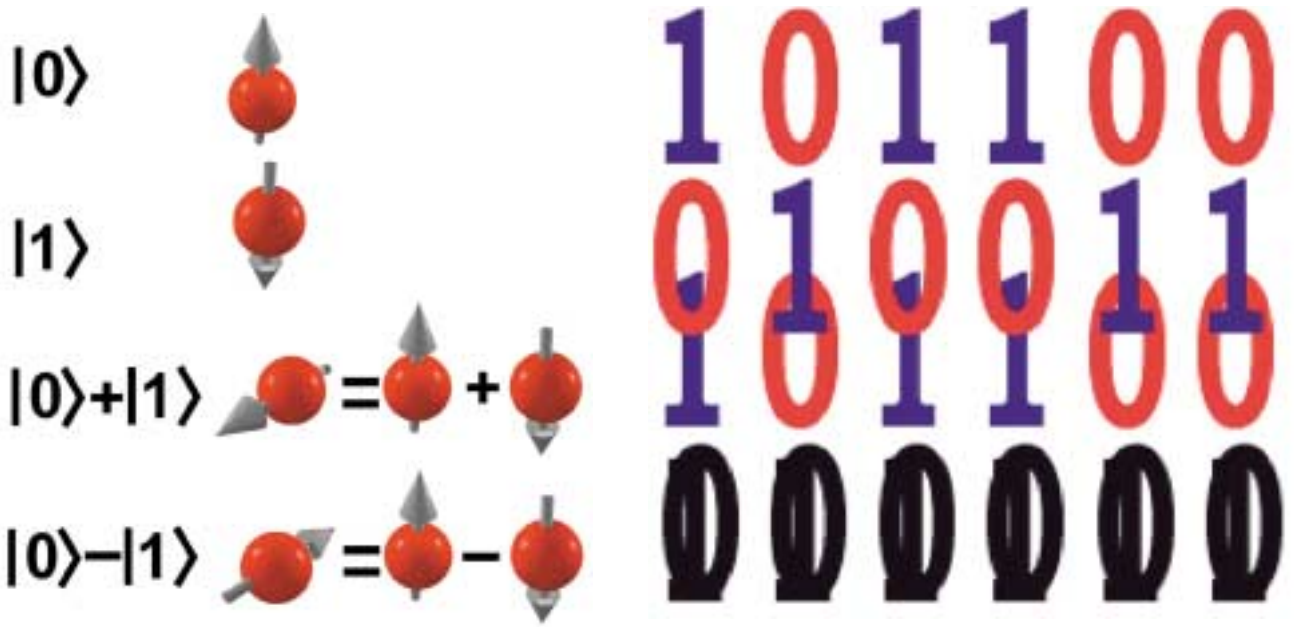
Fakat, kuantum fiziğinin garip yasaları bu spin doğrultusunu iki düzeyli olarak yorumlamamız gerektiğini söylüyor. Bunun bir nedeni spinin yönünü belirlemek için yapılan her ölçümün sadece iki olası değer veriyor olması. Ölçümü yaparken, öncelikle uzayda bir doğrultu seçiyorsunuz, ve ölçüm sonucu olarak 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, her-



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

hangi 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.

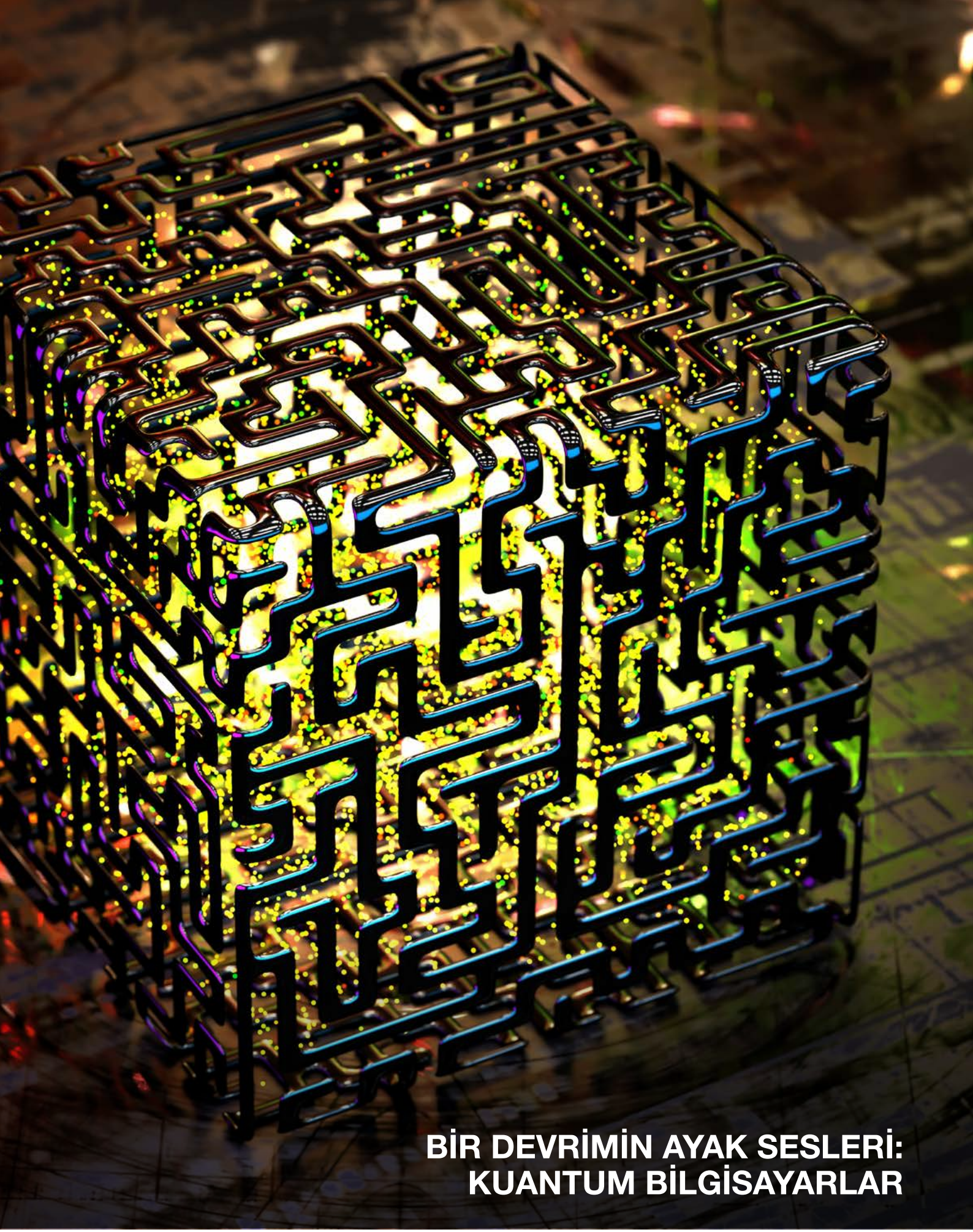
Kubitlerle Bilgi İşlem

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.



BİR DEVRİMİN AYAK SESLERİ: KUANTUM BİLGİSAYARLAR

1. GİRİŞ

Schrödinger'in kedisini bilirsiniz: Aynı anda hem ölü hem de diri olan kedi. Kuantum mekaniğinin kurucularından kabul edilen Avusturyalı fizikçi Erwin Schrödinger (1887-1961) fizik alanına önemli katkılarda bulunmuş ve 1933'te Schrödinger denklemi ile Nobel Fizik Ödülü almış bir bilim adamıdır. Schrödinger denklemi, bir kuantum sistemi hakkında bize her bilgiyi veren araç dalga fonksiyonu adında bir fonksiyondur. Ancak birçok kişi onu 1935 yılında ortaya attığı aslında bir paradoks olarak tanımlanan Schrödinger'in Kedisi düşünce deneyi ile tanır.

Kuantum fiziği tarihinin belki de en ünlü düşünce deneyidir bu. Schrödinger, paradoksunda, kuantum mekaniksel bir parçacığın iki farklı durumu aynı anda eşit olasılıkla taşıyabilme yeteneğini kullanıyor. "İki halin üst üste gelmesi" makro dünyaya yansıtıldığında, içinden çıkılmaz bir sorun ortaya çıkıyor.

Düşünce deneyinde, bozunup bozunmadığı dışarıdan bilinemeyecek, uyarılmış bir atom ile bir kedi aynı kutuya kapatılıyor. Atom bozunacak olursa bir tetikleme mekanizması aracılığıyla bir siyanür şişesini kıracak ve kediyi öldürecektir. Kuantum mekaniği kapsamında son derece sıradan olarak nitelendirilebilecek biçimde; atom, hem bozunmuş hem de bozunmamış sayılabiliyor. Bundan yola çıkarak, kendisi de atomlardan oluşan kediyi de hem canlı, hem de ölü sayabilir miyiz? Henüz kimse bu soruya herkesi tatmin edebilecek bir yanıt bulamadı[1].

2. GEREKSİZ KARAMSARLIKTAN AŞIRI İYİMSERLİĞE

Şimdi sizi Schrödinger'in bilim insanlarıyla tanıştıralım. Aynı anda hem şaşkın hem de sevinçli olan insanlarla.

Schrödinger'in meşhur deneyi, kuantum araştırmacılarının uzun zamandır üzerinde çalıştığı bir şeyi başarmanın eşiğine gelmesiyle tekrar gündeme geldi: Geleneksel bilgisayarların başaramayacağı işleri yapan kuantum bilgisayarlar.

Uzun yıllar boyunca kuantum bilgisayarın gerçekleştirilmesi mümkün olmayan bir bilim kurgu fantezisi olduğu itirazlarıyla mücadele eden bu isimler, engellerin ve itirazların üstesinden gelmek üzereler.

Ancak bu defa da itirazlar yerine abartılı övgülerle mücadele etmek durumuyla karşı karşıya kaldılar. Örneğin, 17 Şubat 2014 tarihinde *Time* dergisinde yayınlanan bir haberde, kuantum bilgisayarlar "insanlığın en karmaşık problemlerini çözebilen sonsuzluk makinesi" olarak tanımlandı. Sonrasında farklı yayın organlarındaki haberler de en az bunun kadar abartılıydı:

"Kuantum bilgisayarlar geleneksel bilgisayarların en hızlısının bile milyonlarca yılda yapabileceği hesaplamaları birkaç milisaniyede yapabilir. Kuantum bilgisayarlar, yıllardır çözülemeyen bilimsel ve ekonomik sorunları çözmenin yanında, yeni malzemeler ve ilaçlar oluşturma potansiyeline sahiptir."

Colorado Boulder Üniversitesi kuantum bilgisayar uzmanı Graeme Smith yaşadıkları çelişkiyi şu sözlerle anlatıyor: "Eskiden bu alanda çalışan insanlara, her şeyin mükemmel olacağını söyleyen iyimserler gözüyle bakılırdı. Şimdi ise abartılı yorumlar ve beklentiler karşısında, kuantum bilgisayarların kısa sürede tüm sorunlara çare olamayacağını anlatmak durumundayız[2]."

3. KUANTUM HÂKİMİYET BEKLENTİSİ

Yaşanan bu abartılı heyecanın nedeni, kuantum bilgisayar çalışmalarının bu yıl içerisinde önemli bir dönüm noktasına ulaşacağı beklentisi. Google ve IBM'deki uzmanların yıl içerisinde "kuantum hâkimiyetini" gözler

önüne serecek güçlü kuantum bilgisayarları tanıtması bekleniyor. Yani, kuantum bilgisayar sistemlerinin, mevcut bilgisayarların, mevcut hafıza ve işlemci güçleriyle çözmesi mümkün olmayan bir problemi çözmesi[3].

İnternet devi Google, kuantum bilgisayarların üstün işlem kapasitesini büyük veri analiz gücünü artırmak için kullanmak istiyor. Böylece sadece aradığımız kelimeleri değil, kurduğumuz cümleleri de anlayan akıllı web arama motorları geliştirecekler.

Ancak "kuantum bilgisayarların habercisi" bu başarı, medyadaki popüler söylemler ve iddialar kadar gösterişli olmayacak. Öncelikle, Google'ın üzerinde çalıştığı algoritma pratik bir fayda sağlamıyor. Bu, şu anlama geliyor: Henüz kuantum hâkimiyet kurulamamasının temel nedeni, günümüzdeki kuantum bilgisayarların sadece özel birkaç algoritmayı çalıştıracak şekilde tasarlanmış olması. Örneğin Google'ın kuantum bilgisayarı yazı-tura simülasyonu yapacak şekilde tasarlanmış. Normal bir bilgisayar iki sayı belirleyerek ve her seferinde bu sayılardan birini gelişigüzel bir şekilde seçerek yapar. 50 yazı-tura atışının simülasyonu için, iki sayıdan birini 50 kere gelişigüzel bir şekilde seçer.

Ancak paranın kuantum mekaniğinin kuralları çerçevesinde hareket eden parçacıklar gibi hareket etmesi durumunda işler biraz karışabilir. Böyle bir durumda, kuantum karışıklığı adı verilen ilke uyarınca, diğer tüm paralar hakkında bilgi sahibi olmadan bir paranın yazı mı yoksa tura mı geleceğini bilemeyiz. İşte bu kuantum karışıklığın simüle edilmesine, kuantum örnekleme adı veriliyor.

Normal bilgisayarlar bu işlemi 50 kere peş peşe seçim yaparak gerçekleştirir. Dolayısıyla 50 sayıyı da aynı anda seçmek, normal bir bilgisayarın yapabileceği bir şey değildir. Google ekibi, bunu başarmak, yani aynı anda 50 yazı-tura atmak için, 50 yazı-tura atışının olası tüm konfigürasyonlarının hafızaya alınması gerektiğini söylüyor.

Klasik bilgisayarların yapı taşları olan bitler, sadece her iki durumdan birini -yazı ya da tura- depolayabileceğine göre, olası tüm konfigürasyonları depolamak için yüzlerce terabaytlık depolama alanı gerekir.

İşte kuantum bilgisayarlar bu noktada devreye giriyor. Kuantum bilgisayarlarda kullanılan kubitler aynı anda iki halde birden olabilir. Bu da 50 yazı-tura atışının tüm konfigürasyonlarının her bir atış için bir kubit kullanılması yoluyla depolanmasını sağlayabilir. Google ekibi, bu özellikten dolayı kuantum örneklemenin kuantum bilgisayarlar açısından kolay olacağını savunuyor. Yani algoritmanın tek amacı, kuantum bilgisayarların normal bilgisayarların çözemeyeceği problemleri çözebileceğini kanıtlamak.

Google şu ana dek 9 kubitlik bir bilgisayarla 9 yazı-tura atışının simülasyonunu gerçekleştirebilmiş durumda. Kuantum bilgisayarların gerçek dünyada pratik olarak kullanılabilmesi için, 50 kubitlik bir bilgisayarla 50-yazı tura atışı simülasyonunun aynı başarıyla tekrarlanması gerekiyor. Ancak bu sayede geçmişte mümkün olmayan kuantum dinamiği araştırmaları yapılabilecek[4].

Gerçek dünyanın gerçek sorunlarını çözecek kuantum bilgisayarlar yapmak ise daha yıllarca sürecek araştırmalar gerektiriyor. Hatta Google ve IBM mühendislerine göre, bilgisayar dünyasının karmaşık sorunlarını çözebilecek bir "rüya makinesinin" ortaya çıkmasına daha on yıllar var. Üstelik o zaman bile kimse kuantum bilgisayarların geleneksel bilgisayarların yerini almasını beklemiyor. IBM araştırmacısı Jay Gambetta şöyle diyor: "Henüz başlangıç aşamasındayız. Klasik bilgisayarlardan daha karmaşık simülasyonlar yapabilecek bir aletimiz var ancak henüz bu simülasyonları hatasız bir şekilde gerçekleştirmek üzere kontrol edemiyoruz." IBM ekibini umutlandıran etken, kuantum bilgisayarların, kusurlarına rağmen işe yarayabilecek olması.

Thenextplatform.com sitesinin haberine göre, günümüz kuantum bilgisayarları, henüz geleneksel bilgisayarların 50 yıl önceki haline benziyor. Silikon temelli entegre devreler, "orta boyuta" 1968 yılında ulaşmıştı. Bu dönemde çipler üzerindeki Transistör sayısı ondan yüze ulaşmış, sonrasında da hızlı bir gelişim göstererek günümüzdeki on milyarlarca transistörün yolunu açmıştı.

Kuantum bilgisayarlar da şu anda çift haneli kubit dönemine ulaşmış durumda. 2017 yılında 20 kubitlik, 2018 yılında 50 kubitin üzerinde kuantum bilgisayarlarla tanıştık. Ancak hızlı bir ilerleme ve somut bir başarı için binlerce kubite ulaşmayı beklememiz gerekecek. Uzmanlara göre çift haneli kubitlerden üç haneli kubitlere ulaşmaya birkaç yıl var. Asıl hedef olan binlerce kubit ise 10, belki de 20 yıl uzakta[5].

Üstelik bırakın binlerce kubiti, kuantum hâkimiyet için ihtiyaç duyulan 50 kubitin de kusursuz çalışması gerekiyor. Ancak Quantum Circuits şirketinin kurucusu olan Yale profesörü Robert Schoelkopf'a göre, kuantum bilgisayarlar bu halleriyle kusursuz çalışmaktan uzak. Kubitlerin kuantum özelliklerini koruması şu an için oldukça zor[6].

Geleneksel bilgisayarların gelişimi hız kesmiş durumda. Bilgisayarlardaki olağanüstü gelişim adını Intel kurucu ortağı Gordon Moore'dan alan Moore Kanunu sayesinde mümkün olmuştu. Bu kanun, aynı paraya alınan işlemci gücünün 18 ayda bir iki katına çıktığını söylüyordu. Bu doğrultuda Transistörler 50 yıl boyunca giderek küçüldü ve ucuzladı. Ancak günümüzde Moore kanununun fiziksel sınırlarına ulaşmış durumdayız. Intel'e göre, Transistörler en fazla beş yıl daha küçülmeye devam edebilecek. Bu da, kimilerine göre, yeni yollar bulunmadığı sürece, bilgisayarların daha fazla güçlenemeyeceği anlamına gelecek[7].

Ancak kuantum bilgisayarları çalışır hale getirmek için gerekli yazılım ve donanımların gelişimi dikkate alındığında, kuantum bilgisayarların, geleneksel bilgisayarların rahatlıkla ve hızla yaptığı işlemleri daha yavaş yapması gibi bir ihtimal de söz konusu[8]. Örneğin YouTube videosu izleyecekseniz kuantum bilgisayar yerine klasik bilgisayar kullanın; çok daha hızlı çalışır. Ancak, evrenin büyük patlama ile nasıl oluştuğunu hesaplamak veya söylediklerinizi insan gibi anlayan akıllı bir web arama motoru geliştirmek istiyorsanız bir kuantum bilgisayar kullanabilirsiniz.

Uzun yıllar boyunca ABD Ulusal Standartlar ve Teknoloji Enstitüsünde kuantum bilgisayarlar üzerinde

çalışan, bir süre önce Microsoft'un araştırma birimine katılan Stephen Jordan "Kuantum bilgisayarların geleneksel bilgisayarların yerini alması beklenmesin" diyor. Jordan'a göre, kuantum bilgisayarlar, günümüz bilgisayarları tarafından gerçekleştirilmesi mümkün olmayan belirli görevlerde kullanılacak.

4. FİKİR BABASI RİCHARD FEYNMAN

Kuantum bilgisayar fikri, 1980'lere dayanır. 1981 yazında IBM ve Massachusetts Institute of Technology (MIT), MIT kampüsü yakınlarındaki Endicott House'da "Bilgisayar Fiziği Konusundaki İlk Konferans" adında, çığır açan bir etkinlik düzenledi. Etkinliğin ana konuşmacısı Nobel ödüllü ünlü fizikçi Richard Feynman'dı. Feynman, konuşmasında atomaltı parçacıkların karakteristiklerinden yararlanarak kuantum bilgisayarlar yapılabileceğini, kuantum hesaplamalarının, kuantum mekanikleriyle çalışan bilgisayarlarda çok daha rahat yapılabileceği fikrini ileri sürdü[9].

Bu yıldan itibaren kuantum bilgisayarların üretimi ve insanların günlük hayatlarında kuantum bilgisayarları kullanabileceği düşüncesi özellikle kuantum fiziğindeki ve teknolojideki yeni gelişmelerle daha da yaygınlaşmaya başladı.

Daha somut bir başlangıç noktası ise o dönem Bell Laboratuvarı'nda çalışan, sonraları MIT'de görev yapan Peter Shor'un çalışmalarıdır. Shor, kuantum bilgisayarlar için bir algoritma geliştirdi. Shor, geliştirdiği 6 kubitlik algoritmayla yüzlerce haneden oluşan sayıları çok kısa sürede çarpanlara ayırdı. Böylece artık çok küçük çaplı bir kuantum bilgisayarı geliştirilmişti[10].

Bu olaydan sonra 1998'de küçük hesaplamaları "eşfazlılığı kaybetmeksizin" birkaç nanosaniyede yapan 2 kubitlik bilgisayar geliştirildi. Bu gelişmeler, başta şifreleme çalışmaları yürüten istihbarat örgütleri olmak üzere birçok kesimin dikkatini çekti ve kuantum bilgisayar araştırmalarına yönelik yatırımlar arttı. Sonraki 20 yıl boyunca, kuantum bilgisayar araştırmalarına, çoğunluğu devletler tarafından, milyarlarca dolar harcandı. 2000'de 4 ve 7 kubitlik kuantum bilgisayarları da başarıyla yapıldı[11]. 2003 yılında DARPA dünyanın ilk kuantum ağını hayata geçirdi. Bu teknolojinin piyasaya sunulabilecek hale gelmeye başlamasıyla birlikte girişim sermayedarları da devreye girmeye başladı[12].

5. KUBİTLER BİTLERE KARŞI

Peki, bu kadar konuşulan kuantum bilgisayar nedir, nasıl çalışır?

Klasik bilgisayarlar bit adı verilen veri (data) birimleri kullanırlar. İşlemcideki moleküler boyuttaki yüzbinlerce transistör, devreden akım geçmesi ya da geçmemesine bağlı olarak, 0 ya da 1 sayılarından oluşan bit değerleri meydana getirir. Bu bitler anakart, ekran kartı ya da ses kartı gibi farklı donanım birimlerinde işlenerek bizlere yazı, görüntü, fotoğraf, video ya da ses çıktısı olarak

iletilir. Her ne kadar bilgisayarınızda aynı anda hem müzik dinleyip hem internette gezinip hem de Word'de metin yazıyor olsanız da bilgisayarınız, tüm bu işleri aynı anda değil, bir sıraya sokarak gerçekleştirir. Bunu oldukça süratli yapmış olduğu için de bizler bunu, aynı anda yapılıyormuş gibi algılarız. Aslına bakarsak bilgisayarda elde ettiğiniz her çıktı sırayla işlenmiş 0 ya da 1'lerden başka bir şey değildir.

Kuantum bilgisayarlarda durum çok farklıdır. Klasik bilgisayarlardaki bit dediğimiz birimlerin yerine kuantum bilgisayarlarda kubit denilen veri birimleri vardır. Bu kubitler sıradan bitlerin yapamadığı bir şeyi yaparlar: Kubitler, hem bitler gibi 0 ya da 1 değerleri alabilir hem ikisini de aynı anda barındırabilir. Kısaca bir kubit aynı anda hem 0 hem de 1 değerlerine sahip olabilir. Kavraması biraz zor olsa da bu durum, kuantum fiziği sayesinde öğrendiğimiz atomaltı parçacıkların karakteristik bir özelliğinin sonucudur. Zira yine kuantum fiziği sayesinde biliyoruz ki elektron gibi atomaltı parçacıklar gözlenmedikleri zamanlarda birer olasılık dalgası biçiminde davranış göstererek birden fazla farklı fiziksel durumda olabilirler[13].

Bunun avantajına gelince: 2 bitlik sıradan bir bilgisayarda ikilik sayı düzeni ile sadece 4 veri kombinasyonunu depolayabilirsiniz (00, 01, 10, 11). Bununla bir matematik problemi çözerseniz elde edeceğiniz sonuç bu dört kombinasyondan biri olacaktır. Buna karşın sıradan bir seri bilgisayar dört kombinasyonu tek tek deneyerek doğru sonuca varırken, 2 kubitlik bir kuantum çip bu kombinasyonların hepsini aynı anda hesaplayacaktır (örneğin 6 kubit: 26=64 bit veya 8 bayt demektir).

Elbette kubit sayısı 2'den 6'ya veya 49'a çıkarsa aynı anda çok daha fazla veri işleyebilir ve süperpozisyon özelliğiyle gerçekten paralel işlem yapan kuantum bilgisayarlar sayesinde en zor soruları en hızlı şekilde çözebiliriz[10].

Daha kolay anlaşılabilmesi için, gezici satış temsilcilerini ele alalım: Bir satış temsilcisi, belli bir grup şehri ziyaret etmek zorundadır ve her seferinde birinden diğerine yolculuk yaparken mümkün olan en kestirme yolu takip etmesi gerekmektedir. Şehirlerin sayıları arttıkça bu sıkıntı daha karmaşık bir hal almaktadır. Mesela 22 şehir arasında en uygun rotayı belirlemek, piyasada bulabileceğiniz Intel i7 işlemcili, 2,8 GHz işlemci hızına, 4 GM RAM'a sahip iyi bir bir laptop tarafından, saniyede 1 milyar deneme yapsa bile, 1000 yılını alırdı. Fakat Avustralya'daki Kuantum Bilgisayar ve İletişim Teknolojileri Merkezi (Centre for Quantum Computation and Communications Technology) direktörü Profesör Michelle Simmons'a göre, 30 kubitlik bir kuantum bilgisayar bu işlemi saniyeler içerisinde gerçekleştirebilir[14].

Simmons'a göre, gezici satış temsilcisi problemi, kuantum bilgisayarların pratik kullanım alanlarını gözler önüne sermesi açısından önem taşıyor. Örneğin bu problemin çözülmesiyle yakıt giderleri azalacak, dağıtım sistemleri optimize edilecek. Ancak bununla da kalmayacak. Avustralya'daki sektörlerin yüzde 40'ı kuantum bilgisayarlar sayesinde dönüşüme uğrayacak[15].

Kuantum bilgisayarlarının temel özelliği olan aynı anda birçok işlemi birden yapabilme yetisi, dalgaların (dolayısıyla da, dalgalar gibi davranan atom ve fotonların da) yapabildiği iki şeyden kaynaklanmaktadır. Bunlardan ilki, okyanus dalgalarında gözlemlenebilir.

Okyanusta hem büyük dalgalar hem de küçük dalgacıklar oluşur. Ancak rüzgârlı bir günde dalgalı bir denizi seyrederken herkesin bilebileceği gibi, büyük dalgaların üzerinde küçük dalgacıklar da görebilirsiniz. Tüm dalgalarda tanık olabileceğiniz bu özellik şu anlama geliyor: Eğer iki farklı dalga var olabiliyorsa, aynı şekilde, dalgaların bir kombinasyonu, yani süperpozisyonu da var olabilir. Süperpozisyon gerçeği, gündelik dünyada önemsiz bir şey gibi görünebilir. Ancak atomların dünyasında söz konusu kombinasyon olağanüstü sayılabilecek bir duruma örnektir; aynı anda hem camdan geçen hem de geri yansıyan bir fotonun varlığına. Diğer bir deyişle, foton camın iki tarafında aynı anda bulunabilmektedir.

Yapılan deneylerde, aynı anda iki yerde birden bulunan bir foton ya da atomu gözlemlemek gerçekten de mümkündür (daha doğru bir ifadeyle ortaya koyacak olursak, aynı anda iki yerde birden bulunan bir foton ya da atomun neden olduğu sonuçları gözlemlemek mümkündür). Bu durumun gündelik hayatımızdaki karşılığı, aynı anda hem İstanbul hem de Londra'da bulunabilmemizdir. Bu kadar da değil. Üst üste binecek dalgaların sayısının bir sınırı olmadığına göre, bir foton ya da atom aynı anda üç yerde de olabilir, bir milyon yerde de. İstanbul ve Londra örneğinden devam edecek olursak, aynı anda dünyanın tüm kentlerini geziyor olabilirsiniz.

Atomlar ve türevleri yalnızca aynı anda birçok yerde bulunabilmekle kalmaz, birçok işi de eş zamanlı bir şekilde gerçekleştirebilirler. Bunun gündelik yaşantımızdaki karşılığı ise, bir yandan evde temizlik yaparken, bir yandan da köpeği dolaştırmanız ve haftalık süpermarket alışverişinizi halletmenizdir. Kuantum bilgisayarlarının muazzam gücünün ardındaki giz budur. Atomların birçok işi bir arada yapabilme yetisini kullanan kuantum bilgisayarlar, aynı anda çok sayıda hesaplamayı yapabilmektedir. Geleneksel bilgisayarların belirli bir sıra içerisinde, teker teker ve uzun zamanda gerçekleştirdiği işlemler, kuantum bilgisayarlar açısından tek ve kısa bir işlem niteliğindedir[16].

6. NE GEREK VAR KUANTUM BİLGİSAYARA?

Normal bilgisayarlar yerine böyle bir teknolojiye geçilmesinin elbette bir nedeni var. Normal bilgisayarların sahip olduğu teknoloji artık limitlerine ulaştı, bunun nedeni bilgisayarların çalışma prensibinde yatıyor. Günümüzde bir bilgisayarın daha iyi olabilmesi için transistör sayısının daha fazla olması gerekir.

1971 yılında Intel tarafından üretilen ilk işlemci 2300 transistörden oluşuyordu. Şu anda Intel 5 milyar transistörden oluşan mikro işlemciler üretiyor.

"1971 yılında transistör kapı açıklığı 10 mikron civarındaydı (1 mikron, 1 metrenin milyonda biridir). 1980'de bu büyüklük 5 mikrona düştü. 1990 yılında 1 mikrona... 2000 yılında 0,1 mikrona, yani 100 nanometreye (1 nanometre, 1 metrenin 1 milyarda biridir). 2009 başında 50

nanometreye, sonunda 32 nanometreye... 2012'de 19 nanometre, 2014'te 10 nanometreye ve nihayetinde, 3 milyar dolarlık yatırım, 10 çığır açıcı araştırma sonucunda, 9 Temmuz 2015'te 7 nanometreye[17]..."

Ancak daha ne kadar ilerleyebiliriz? Transistörler, en nihayetinde fiziksel yapılardır. Dolayısıyla atomlardan oluşurlar. Bu da fiziksel sınırları olduğu anlamına gelir. Örneğin New South Wales, Purdue, Melbourne ve Sydney üniversiteleri araştırmacılarından oluşan uluslararası bir ekip tek bir fosfor atomundan oluşan, bugüne dek üretilen (ve iddialarına göre üretilebilecek) en küçük transistörü geliştirdi[18]. Daha küçük bir Transistör üretmek istediğimizde artık atomlardan söz edemeyiz. Bu noktada atomaltı parçacıkların dünyasına adım atmamız gerekir. Yani kuantum dünyasına[19]!

Bir diğer neden ise Moore yasasının geçerliliğini yitirmiş olması. *Electronics Magazine*'in 19 Nisan 1965 tarihli sayısında, daha sonra Intel şirketinin kurucu ortakları arasında yer alan mühendis Gordon Moore, yarı iletken teknolojisinde kaydedilmesi beklenen gelişmelere dair kehanet olarak nitelendirilebilecek saptamalarda bulunuyordu. Moore şöyle diyordu: "Minimum bileşen maliyetleri için karmaşıklık her yıl kabaca 2 prim oranı artmaktadır… Kısa vadede bu oranın bu şekilde devam etmesi beklenebilir – artması da mümkündür. Uzun vadedeki artış oranını bilemesek de, en az 10 yıl boyunca en azından sabit kalmayacağını düşündürecek bir neden yoktur. Bu da, 1975 itibarıyla, minimum maliyetli bir entegre devredeki bileşenlerin sayısının 65 bin olacağı anlamına gelir. Böyle büyük bir devrin tek bir plaka üzerine sığdırabileceğine ben inanıyorum."

Moore Yasası, "Her 18 ayda, bir tümleşik devre üzerine yerleştirilebilecek bileşen sayısı iki katına çıkarken, üretim maliyetleri aynı kalır, hatta düşme eğilimi gösterir" der. Basite indirgeyecek olursak, eğer paranızı saklarsanız 18 ay sonra bugün alacağımız bilgisayardan 2 kat daha güçlü (işlemci açısından) bir bilgisayar alabilirsiniz.

Ancak Stanford Üniversitesi Bilgisayar Bilimleri Bölüm Başkanı olan Nvidia Baş Bilimcisi ve Başkan Yardımcısı Bill Dally, 2010 yılında Moore Yasası'nın artık geçersiz olduğunu; işlemci hız artışlarının Moore Yasası'nı karşıladığını ama yasanın diğer parçası olan güç tüketimine yönelik ölçeklendirmenin sona erdiğini açıkladı. Dally'e göre Moore Yasası'nda yer alan CPU (Central Processing Unit - Merkezi İşlem Birimi) ölçeklendirmesine ilişkin öngörü artık (2010 itibariyle) geçerli değil. Dally şunları söylüyor: "Çok çekirdekli işlemci kullanmak, trene kanat takarak uçak yapmaya çalışmak gibi. Geleceğe yönelik ekonomik büyüme ve ticari yenilikler için paralel işlem teknolojilerinin yani Grafik İşlem Birimlerinin (GPU) ilerlemesi gerekiyor. İleri gidebilmek için kritik nokta, enerji verimli sistemler inşa etmek[20].

7. MÜHENDİSLERİN KÂBUSU

Ancak… Kuantum bilgisayarlar teorik olarak mümkün olsa da teknolojik zorlukları muazzam boyutlardadır. Böyle bir bilgisayar inşa etmek için gerekli olan mühendislik Mars'a insanlı uzay yolculuğundan daha zor sayılır. Birçok kuantum bilgisayarın gelişiminde rol oynayan Isaac Chuang'ın tabiriyle, "Fizikçilerin rüyası, mühendislerin kâbusu halini aldı[9]."

Kuantum bilgisayarların kubitleri kullanabilmeleri için atomaltı parçacık karakteristiklerine erişmeleri gerekir. Yani bir kuantum bilgisayar üretebilmek için kubitleri kullanabilecek yapıda bir donanım bulunmalıdır. Bunun için belli başlı teknikler mevcuttur. Bunların ilki süperiletken devrelerin kafes şeklinde örülmesi, kubitlerin bu kafeslerde saklanıp mutlak sıfır sıcaklığının hemen üzerinde bir sıcaklıkta sabit tutulmasıdır. Diğer bir teknik ise iyon atomları elektromanyetik alanlar içerisine sıkıştırarak kubitleri saklamaktır. "Sıkıştırılmış iyonları (yüklü atomlar) kullanarak küçük bir ölçekte kuantum hesaplama işlemi, her bir iyonun bir kuantum biti oluşturan bireysel iyonlara hizalamasıyla gerçekleştirilir. Bununla birlikte, büyük ölçekli bir kuantum bilgisayarında, milyarlarca kuantum biti kullanılacağı için, her iyon için bir tane olmak üzere milyarlarca tam hizalanmış lazer gerekir[21]."

Üstelik kuantum bilgisayarların, kubitlerin çevre şartlarına karşı çok hassas olması gibi bir sorunu vardır. Kubit'ler kırılgan bir yapıya sahiptir. Neredeyse eliniz değince bozulacak kadar hassastır. Bu yüzden de bilgi işlem sırasında büyük veri kaybı gerçekleşir. Kubitlerden bir kısmı, kuantum bilgisayar, verilen problemi çözmeden önce bozulur. Yakın zamana dek en gelişmiş kuantum bilgisayarların en fazla 10-20 kubite sahip olmasının ve en fazla basit aritmetik hesaplar yapabilecek kapasiteye ulaşmasının nedeni de bunu başarmanın güçlüğüdür.

Bu sorunu aşmanın yolu, müdahale durumunda hata yapabilecek olan kubitlerin yerini alacak "yedek" kubitlere sahip olmaktır ve mühendislerin hesaplarına göre, her bir kubitin en az 1000 yedeği olmalıdır. Dolayısıyla da düzgün bir şekilde çalışabilecek bir kuantum bilgisayardaki kubitlerin sayısı milyonları bulmalıdır.

Bu donanım sorunlarının yanı sıra yazılım sorunları da söz konusudur. Günümüzde mevcut yazılım dilleri bir verinin aynı anda sadece 1 adet belirli bit kombinasyonuna işlenebilmesini baz alır. Kuantum mekaniğinin belirsizlik temelli kubitlerini kullanabilecek bir yazılım dili ise henüz mevcut değildir.

8. FARKLI YAKLAŞIMLAR

IBM 2017'nin Kasım ayında 50 kubitlik bir kuantum bilgisayar ürettiğini açıkladı. California'da kurulan yeni bir girişim olan Rigetti Computing ve Intel ise 49 kubitlik bir çip geliştirdi. Yani henüz kat edilecek epey bir mesafe var. Üstelik bu çiplerin çok düşük sıcaklıklarda korunması gerekiyor. Bu da bilim kurgu filmlerinden çıkmışa benzeyen, büyük soğutma sistemleri anlamına geliyor.

Elektronların oda sıcaklığında gayet aktif ve enerjik olduğunu biliyoruz. Bu parçacıklar bugün odamızda biz görmesek bile her an hareket halinde. Bu durum tam bir kaos ortamı yaratır ve kubitlerin süperpozisyon durumunu bozar. Bunu engellemenin yolu kubitleri dış gürültülere karşı yalıtmaktır. Bu yalıtım ise kubitin ısınmasına

yol açacaktır. Bu nedenden dolayı kuantum bilgisayarlar oda sıcaklığında düzgün çalışamaz. Düzgün çalışması için kubitlerin düşük ısıda tutulması gerekir.

Ancak, kuantum bilgisayarların düzgün çalışması için soğutma tek başına yeterli değil. Sistemin bir de manyetik alanlardan, örneğin cep telefonu sinyallerinden izole edilmesi gerekir. Bu da vakumlama sayesinde gerçekleşir. Kuantum bilgisayarların bir oda kadar yer kaplamasının sebeplerinden biri manyetik alanların yol açtığı paraziti önlemek için kalın bir zırh kullanma gerekliliğidir.

Ancak bu da yeterli değil. "Bilgisayarlar çalışırken buodaların içinin yaklaşık 4 Kelvin düzeyinde (-270 Celsius derece) olması gerektiği söyleniyor. Yani uzay boşluğundan bile soğuk. Bu da yanlışlıkla içeride kalacak bir insanın, tıpkı uzay boşluğunda yaşanacağı gibi önce donupsonra patlamasına yol açacaktır[22]."

Bu sorunları aşmaya yönelik, tuzaklamış atomik iyon kubitlerin kullanıldığı, oda sıcaklığında çalışan farklı bir sistem de söz konusu. Duke Üniversitesinden fizik profesörü Jungsang Kim ve Maryland Üniversitesinden Christopher Monroe tarafından kurulan IonQ, bu yaklaşıma dayalı, iterbiyum iyonlarının kullanıldığı bir bilgisayar geliştirmek üzere çalışmalarına devam ediyor. Tuzaklanmış iyonlara yönelik uzun yıllardır devam eden laboratuvar çalışmalarının ürünü olan bu yöntemin çok daha iyi bir performans doğurabileceği savunuluyor. IonQ'nun mevcut yöntemlerden farkı, tuzaklanmış iyonların "doğal olarak kuantum halde" olması, 0 ve 1'lerin bir arada bulunduğu süperpozisyon özelliğine sahip olması.

IonQ CEO'su David Moehring, bu sistemin avantajını şöyle anlatıyor: "Bir kuantum bilgisayar yaparken, klasik bir sistemle başlayarak buna kuantum özellikler kazandırmaya çalışmak yerine, kuantum halde bir sistemle başlamak, donanımı bu sistem çevresinde kurmak büyük avantaj[23]."

"IonQ'nun geliştirdiği bilgisayar mıknatıslar, lazerleri ve elektron sayısı ile proton sayısının eşit olmamasından dolayı yüklü atom olarak adlandırılan iyonları bir araya getiriyor. İteberyum adı verilen belirli bir atomik sistemden elde edilen iyonlar, bir gerdanlıktaki inciler gibi, tek bir çizgi halinde tuzaklanıyor. Bu atomların her biri, bir kubiti oluşturuyor[23]." Bu yaklaşım sayesinde, süperiletken devrelere oranla 100.000 kat daha hızlı bağlantı hızı sağlanacak. Bu yöntem, masraflı soğutma sistemlerine duyulan ihtiyacı da ortadan kaldıracak. Bu anlamda da çevre dostu bir mimari ile karşı karşıyayız.

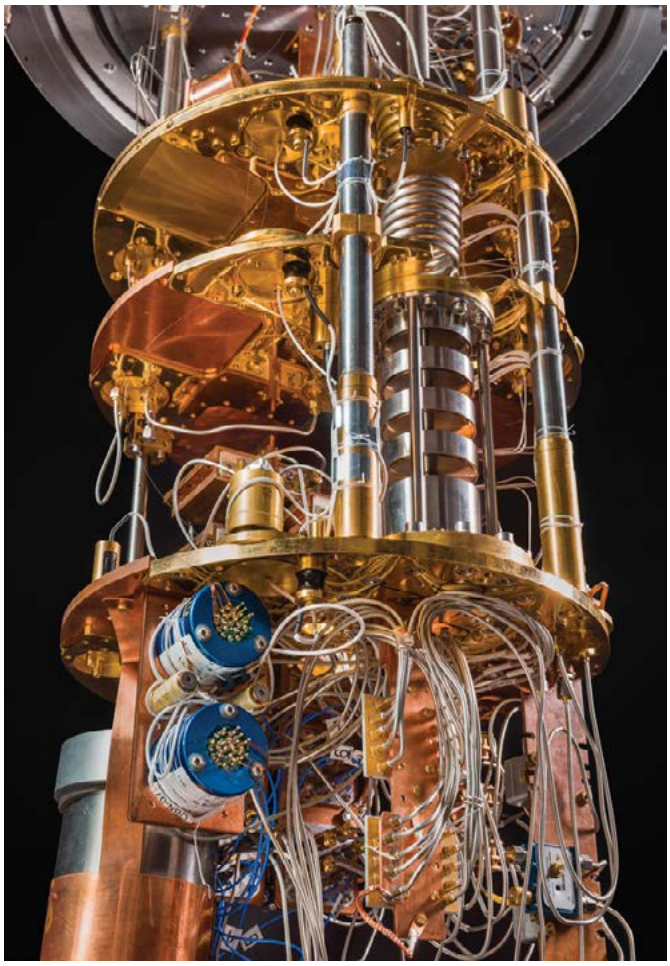
Microsoft ise topolojik kuantum bilgisayar olarak bilinen üçüncü bir strateji benimsemiş durumda. Strateji teorik olarak umut vadedici olsa da ortada henüz somut bir şey yok.

Bir de 2000 kubitlik yeni bir kuantum bilgisayar geliştirdiğini açıklayarak büyük sükse yapan Kanadalı D-Wave Systems şirketi var. Şirket, üç metre yüksekliğindeki yeni kuantum bilgisayarı D-Wave 2000Q'yu 15 milyon dolardan satışa çıkardığını duyurdu[24].

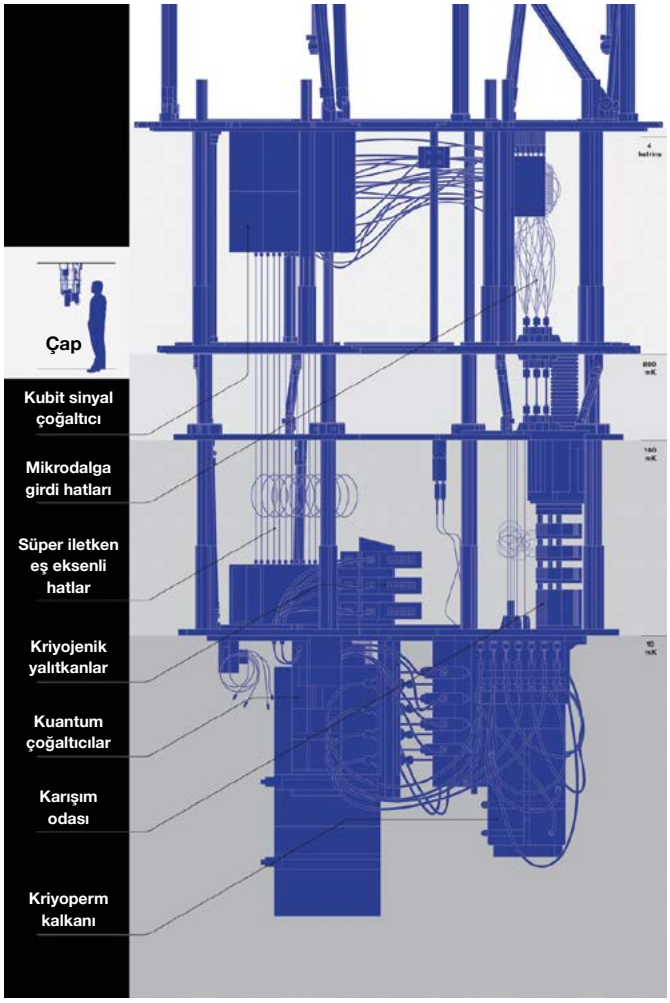
D-Wave'in kuantum bilgisayarları oda büyüklüğünde; çünkü diğer kuantum çiplerin tersine, kuantum halkalama denilen farklı bir teknoloji kullanıyor. Bu yüzden de başparmak tırnağı büyüklüğündeki bir çipin, 20 metreküplük oda büyüklüğünde dev bir soğutma dolabının içinde mutlak sıfıra kadar soğutulması gerekiyor.

D-Wave Google, NASA, Volkswagen gibi kuruluşlara kuantum bilgisayar sattı. Örneğin Volkswagen daha iyi elektrik araç pilleri oluşturmak için kuantum bilgisayarlar ve yapay zekâ kullanacak bir ekip oluşturuyor. NASA da Google'la işbirliği içerisinde kuantum yapay zekâ laboratuvarı kurma çalışmalarını sürdürüyor[25]. Ancak sistem bilim çevrelerinde kuşkuyla karşılanıyor. D-Wave, belirli algoritmaları sıradan bilgisayardan hızlı çözse de, daha karmaşık bir algoritma kullandığınızda bu üstünlük ortadan kalkıyor. Bu nedenle sistemin kuantum hıza ulaşacağına dair ciddi şüpheler bulunuyor.

Texas Üniversitesinden Scott Aaronson ve UC Davis'ten Greg Kuperberg, D-Wave'de kuantum hızlanmaya tanık olmadıklarını, bu yüzden de sıradan laptop gücündeki bir bilgisayara 15 milyon dolar vermenin yersiz olduğunu söylüyor. Ayrıca D-Wave'in kendini kanıtlamak için yayınladığı kuantum bilgisayar testlerinin de yanıltıcı olduğunu belirtiyorlar. "Buna göre D-Wave sadece kendi çip tasarımıyla hızlı çözülecek problemlerle



Fotoğraf: Christopher Payne/Esto
Fütüristik bilgisayar: IBM'in yeni kuantum bilgisayarları bilim kurgu filmlerinden fırlamışa benziyor. Bu karmaşık cihazların gerçekten yararlı olup olmadıklarını ise zamanla göreceğiz.



Soğukkanlı bilgisayar[28]: IBM'in yeni kuantum bilgisayarının, tıpkı Google'ınki gibi, çalışması için neredeyse sıfır dereceye kadar soğutulması gerekiyor. Bu soğutma işlemi, yukarıda görülen seyrelti buzdolabı aracılığıyla gerçekleştiriliyor.

test yaptı ve ortaya 'Klasik bilgisayardan 100 milyon kat hızlı kuantum bilgisayar yaptık' iddiası çıktı[26]."

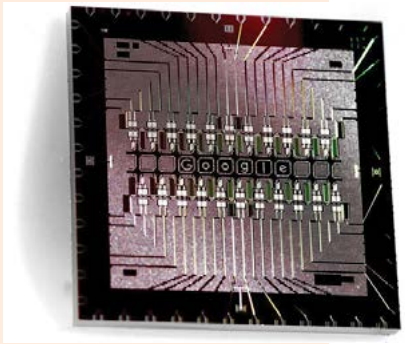
Bu arada Çin'in de kuantum bilgisayar araştırmalarına milyarlarca dolar yatırdığını ve rakiplerinden 24 bin kat hızlı bir kuantum makine yaptığını açıkladığını söylemekte yarar var[27].

9. GİDİLECEK ÇOK YOL VAR

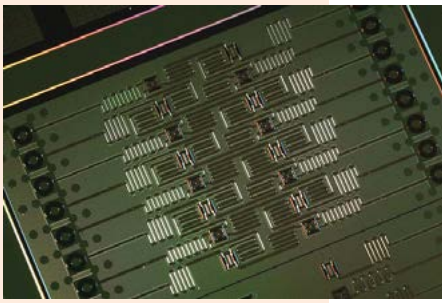
Özetle, şu an için Google-IBM-Rigetti yaklaşımı kuantum bilgisayar yarışında bir adım önde görünüyor. Yine de bu şirketlerin bir masaüstü kuantum bilgisayar geliştirmek için daha çok çalışmaları gerekiyor. Maryland kuantum bilgisayar şirketi IonQ'nun kurucu ortağı Chris Monroe'nun dediği gibi, "Basit bir çip üretmekle tam kapsamlı masaüstü kuantum bilgisayar üretmek arasında çok fark var."

Bir diğer sıkıntı da Moore Yasası'nın kuantum bilgisayarlar açısından geçerli olmaması. Yani ne zaman yeterli kubit gücüne ulaşılacağının bilinmemesi. Kuantum bilgisayarların karmaşık yapısından dolayı, geleneksel

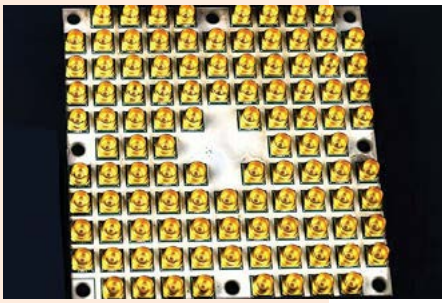
KUANTUM BİLGİSAYAR YARIŞININ BEŞ OYUNCUSU[28]



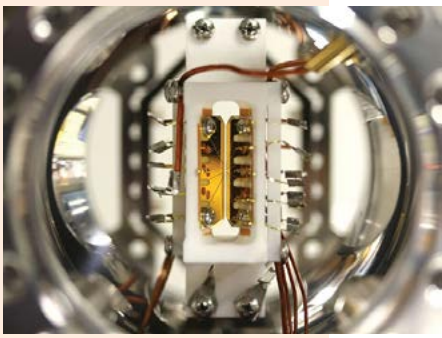
1. Google: Google, yukarıdaki gibi, 22 kubitlik unsurların iki sıra halinde dizildiği süperiletken işlemciler kullanıyor.



2. IBM: Bu 16 kubitlik süperiletken işlemci, IBM'in kuantum bilgisayarların incelenmesine olanak vermek amacıyla herkesin kullanımına açtığı platformuna güç veriyor.



3. Intel: Intel, Şubat ayında Langle Lake adını verdiği, 49 kubitlik süperiletken kuantum bilgisayar çipini ürettiğini açıkladı.



4. IONQ: IONQ, 2016 yılında cihaz içinde hapsedilen iteberyum iyonlarını lazerlerle kontrol ederek, çalışır haldeki 5 kubitlik bilgisayarının tanıtımını gerçekleştirdi.

5. Rigetti: California, Berkeley'deki yeni bir girişim olan Rigetti, bir süre önce 19 kubitlik süperiletken işlemci çipleri üretmeye başladı.

bilgisayarlarda olduğu gibi "işlemci gücü iki yılda iki katına çıkar" benzeri bir öngörüde bulunmak mümkün değil. Yani görünüşe göre yakın zamanda en fazla birkaç yüz kubitlik kuantum bilgisayarlarla yetinmek durumunda kalacağız.

Sonuçta kuantum bilgisayarlar geliyor demenin ötesine geçtik. Artık buradalar. Kuantum üstünlük sınırı denilen 50 kubit beklenenden çok daha erken karşımızda. Henüz pratik kullanım alanları ortaya çıkmasa da bunun yalnızca bir zaman meselesi olduğu açık. Yani, büyük bir sürpriz olmazsa yavaş ve aşamalı bir gelişme mümkün. California Üniversitesinden Fizik Profesörü Wim van Dam durumu şu sözlerle ortaya koyuyor: "Kuantum bilgisayarların yakın zamanda gerçek sorunların çözümünde kullanılacağını, bu sektörden para kazanılacağını sanmıyorum. Bunun için çok daha büyük sistemlere ihtiyacımız var." Bu nedenle de mühendisler bilgisayarların gücünü artırmak yerine, mütevazı makinelerle çalışacak algoritmalar geliştirmeye odaklanmış durumda.

10. KUANTUM BİLGİSAYARLAR HEM GÜVENLİ HEM RİSKLİ

D-Wave'in ilk müşterisi Temporal Defense Systems adlı bir siber güvenlik firmasıydı ve amacı da kuantum bilgisayarla internetteki şifreleri incelemekti.

"Daha önce de belirtilen kuantum bitlerin özelliği gereği, kuantum çipler şifreleme ve büyük veri analizi gibi konularda normal bilgisayardan daha hızlı çalışıyor. Yani bu bilgisayarlar, normal/klasik bilgisayarlardaki 0 ile 1 mantık değerlerine değil; kuantum fiziğinde yer alan 'dolanıklılık özelliği'nin bir getirisiyle 0,14 gibi ara değerlere de sahip olabiliyor[26]."

Örneğin, Singapur Ulusal Üniversitesi araştırmasına göre, kuantum bilgisayarlar, Shor algoritması adı verilen algoritmayı kullanarak dijital para birimlerinin özel anahtarlarını 2027 yılının başlarında kırabilecek kapasiteye erişebilir. Bitcoin gibi dijital para birimlerinin şifreleme sistemini kırmak bugünkü mevcut bilgisayarlar kullanılarak imkânsız olsa da kuantum bilgisayarlarının teknolojisi daha da ilerledikçe Bitcoin'in şifreleme sistemini kırma imkânının doğabileceği öne sürülüyor[29].

Yani, normal bilgisayarların yıllarca uğraşarak çözemeyeceği şifreleri birkaç saniyede çözebilen kuantum bilgisayarlar, aynı zamanda korsanlara da hızlı bir silah sunmuş olacak. Neyse ki korsanlar yakın gelecekte bu bilgisayarlara kolay kolay sahip olamayacak. Hem fiyatları hem de zorlu kullanım koşulları korsanların kuantum bilgisayarların sunduğu olanaklara erişmesini zorlaştıracak. Bununla birlikte; Çin, Rusya gibi organize siber saldırılar düzenleyen ülkelerin, kuantum bilgisayarları da casusluk amacıyla kullanması pek şaşırtıcı olmayacak[30].

Tabii kuantum bilgisayarlar geliştikçe, kötüye kullanımlarını önlemeye yönelik önlemler de gelişiyor. Güvenlik şirketi FireEye'ın araştırmasının da ortaya koyduğu gibi, kripto para birimlerini daha güvenli hale getirmeye, kuantuma karşı dirençli muhasebe defterleri geliştirmeye yönelik çeşitli çalışmalar devam ediyor[31].

Gemalto'nun Ürün Stratejisi Direktörü Joe Pindar bu konuda iyimser isimler arasında bulunuyor: "Kuantum bilgisayarların çok sayıda olasılığı aynı anda hesaplamasının en ilginç yanı ve bu bilgisayarların ilk prototiplerinin İsviçre bankaları ve devletler tarafından kullanılmasının nedeni, "tek seferlik bloknotlar" üreterek siber güvenliği artırmaları. Bu şifrelerin kırılması teorik olarak mümkün değil. Aslına bakarsanız bu yeni teknoloji ilhamını 100 yıl öncesinden, Birinci Dünya Savaşı'ndan alıyor. Her bir şifrenin sadece tek bir mesaj için ve sadece bir kereliğine kullanılması o dönemde şifrelerin kırılmasını engellemişti. Bugün de bizi saldırılardan koruyabilecek[31]."

11. İŞ DÜNYASINA YANSIMALARI

Kuantum teknolojilerinin geleceği ve iş dünyasına olası yansımalarıyla ilgili STM Genel Müdürü Dr. Davut Yılmaz, *Bloomberg Businessweek Türkiye* dergisinde yayınlanan yazısında bilim ve teknoloji alanındaki baş döndürücü gelişmelerin, kuantum teknolojisini fizikçilerin tartıştığı bir konsept olmaktan çıkarıp, iş dünyasının yakından takip ettiği bir alan haline getirdiğine dikkat çekti[32]. "Bir yandan IBM, Microsoft, Google, Lockheed Martin, Airbus, Raytheon gibi dünya devleri bu alana uzun vadeli yatırımlar yaparken, diğer yandan J.P.Morgan, Honda, Hitachi, Daimler, Samsung gibi şirketler de bu yatırımların çıktısının ilk kullanıcıları olmak için işbirliği anlaşmaları yapıyor. Bunların yanında gelişmeleri yakından takip eden ya da bu alanda çalışmaya başlayan startup'ları markaja alan pek çok şirket bulunuyor. 2018'in ilk beş trendinden biri olan kuantum teknolojisi, pek çok alanı derinden etkileyecek" diyen Dr. Yılmaz bu teknolojileri şöyle sıralıyor:

Bilişim ve İletişim Teknolojileri: Bir çipin üzerine yerleştirebilecek transistör sayısının her 18 ayda bir iki katına çıkacağını ve bu sayede işlem kapasitesinin artacağını savunan meşhur Moore Yasası artık yolun sonuna geldi ve bu sorunu aşacak en önemli çözüm kuantum teknolojisi olarak karşımıza çıkıyor. Kendine has karakteristiğiyle kuantum teknolojisi, çok yüksek işlem hızlarının yanı sıra, bilişim ve iletişim sektörü için güvenli haberleşme ve kırılamayan şifreler de vadediyor.

Yapay Zekâ Teknolojileri: Kuantum teknolojisinin özellikle makine öğrenmesine katalizör etkisi yapması, bu yolda çok hızlı bir şekilde ilerleyeceğimizi gösteriyor.

Sağlık: Kuantum teknolojisinin karmaşık olayları mikro seviyede simüle edebilme ve sensör teknolojisine getirdiği çok güçlü kabiliyetler, sağlık ve biyoteknoloji alanlarını doğrudan etkileyecek. Bu da yeni ilaçlar, sağlık cihazları ve tedavi yöntemleri anlamına geliyor.

Malzeme: Kuantum simülasyonlar sayesinde yeni malzemeler tasarlanması, modern teknolojinin en büyük sorunlarından biri olan batarya başta olmak üzere, pek çok derde deva olacak.

Savunma: Kuantum teknolojisi, uzaydaki uydulardan derin sulardaki denizaltılara, sahadaki radarlardan kullanılan silahlara kadar pek çok alanda gelişimi sağlayacak.

12. SONUÇ

Sonuç olarak, kuantum bilgisayarların geleceği umut verici olsa da, bu alanda henüz ilk adımlar atılmış durumda. Kuantum bilgisayarların somut faydalarını görebilmek için aşılması gereken birçok engel söz konusu. Dünyanın dört bir yanındaki araştırmacılar gerçek anlamda sağlam ve başarılı ilk kuantum bilgisayarı üretmek için bir yarış halinde.

IBM'in 7 kubitlik sistemiyle yaptığı berilyum hidrür simülasyonu bize kuantum bilgisayarların yalnızca yazılım alanında değil kuantum kimya gibi inanılmaz potansiyeller barındıran alanlarda da aktif olarak kullanılmaya başlandığını gösteriyor. D-Wave'in hâlihazırda savunma devi Lockheed Martin'le ve NASA'yla yaptığı çalışmalar ise havacılık ve uzay sektöründe kuantum bilgisayarların şimdiden kullanıldığına işaret ediyor[33].

Kısacası kuantum bilgisayarlar güvenlik, havacılık/uzay, kimya, ilaç, yapay zekâ ve daha kim bilir nice sektörde büyük değişimlere yol açacak bir teknoloji ve zannedilenin aksine 2050'lerde değil 2020'lerde aktif olarak kullanımına başlanacak gibi duruyor.

Ancak bu konuda da beklentileri çok yüksek tutmamak gerekiyor. Çünkü kuantum bilgisayarları üstün kılan özellikler, aynı zamanda bu bilgisayarların üretimini olağanüstü derecede güçleştiriyor. Yani, olağanüstü keşifler doğurabilecek yeni bir çağın eşiğinde bulunuyoruz. Ancak henüz yolun başındayız. Kuantum bilgisayarlar, şu an için geleneksel bilgisayarların 100 yıl önceki haline benziyor ve daha yapılacak çok şey bulunuyor.

KAYNAKÇA

[1] Sibel Çağlar, "Nedir Bu Schrödinger'in Kedisi?", *Matematiksel*, 21 Ocak 2017, https://www.matematiksel.org/nedir-schrodingerin-kedisi/.

[2] Lee Gomes, "Quantum Computers Strive to Break Out of the Lab", *IEEE Spectrum*, 22 March 2018, https://spectrum.ieee.org/computing/hardware/quantum-computers-strive-to-break-out-of-the-lab.

[3] Philip Ball, "The Era of Quantum Computing Is Here. Outlook: Cloudy", *Quanta Magazine*, 24 January 2018, https://www.quantamagazine.org/the-era-of-quantum-computing-is-here-outlook-cloudy-20180124/.

[4] Mark Kim, "Google quantum computer test shows breakthrough is within reach", *New Scientist*, 28 September 2017, https://www.newscientist.com/article/2148989-google-quantum-computer-test-shows-breakthrough-is-within-reach/.

[5] Paul Teich, "Quantum Computing Enters 2018 Like It Is 1968", *Next Platform*, 10 January 2018, https://www.nextplatform.com/2018/01/10/quantum-computing-enters-2018-like-1968/.

[6] Henry Joseph-Grant, "IBM Now Have A 50 Qubıt Quantum Computer, But Are Still Trying to Figure Out What to Do with It", *Irish Tech News*, 24 February 2018, https://irishtechnews.ie/ibm-now-have-a-50-qubit-quantum-computer-but-are-still-trying-to-figure-out-what-to-do-with-it/.

[7] Tom Simonite, "Moore's Law Is Dead. Now What?", *MIT Technology Review*, 13 May 2016, https://www.technologyreview.com/s/601441/moores-law-is-dead-now-what/.

[8] Kozan Demircan, "Kuantum Bilgisayar Klasik Bilgisayara Karşı >> D-Wave'in Kuantum Bilgisayarı Ne Kadar Hızlı Ve Ne Kadar Akıllı?", *Khosann (Kozan Demircan)*, 21 Şubat 2014, https://khosann.com/kuantum-bilgisayar-klasik-bilgisayara-karsi-d-wavein-kuantum-bilgisayari-ne-kadar-hizli-ve-ne-kadar-akilli/.

[9] Will Knight, "Serious quantum computers are finally here. What are we going to do with them?", *MIT Technology Review*, 21 February 2018, https://www.technologyreview.com/s/610250/serious-quantum-computers-are-finally-here-what-are-we-going-to-do-with-them/.

[10] "Quantum computing 101", Institute For Quantum Computing, University of Waterloo, https://uwaterloo.ca/institute-for-quantum-computing/quantum-computing-101.

[11] "Kuantum Bilgisayarı Nedir?", *Fizik Makaleleri*, http://www.fizikmakaleleri.com/2013/02/kuantum-bilgisayar.html.

[12] Bernard Marr, "20 Mind-Boggling Facts About Quantum Computing Everyone Should Read", *Forbes*, 23 February 2018, https://www.forbes.com/sites/bernard-marr/2018/02/23/20-mind-boggling-facts-about-quantum-computing-everyone-should-read/#8dadd625edb7.

[13] "What is quantum computing?", *IBM*, https://www.research.ibm.com/ibm-q/learn/what-is-quantum-computing/.

[14] Elif Edin Dinç, "Kuantum Bilgisayarlar Yapay Zekadan Daha Büyük Bir Tehlike Olabilir!", *Bilimoloji*, 09 Şubat 2018, http://bilimoloji.com/kuantum-bilgisayarlar-yapay-zekadan-daha-buyuk-bir-tehlike-olabilir/.

[15] Asha McLean, "Australia's ambitious plan to win the quantum race", *ZD Net*, 03 July 2017, https://www.zdnet.com/article/australias-ambitious-plan-to-win-the-quantum-race/.

[16] "Kuantum Bilgisayarlarına Hazır mıyız?", *Kobitek*, http://kobitek.com/kuantum-bilgisayarlarina-hazir-miyiz.

[17] Çağrı Mert Bakırcı, "Kuantum Bilişim: Kuantum Bilgisayarlar Nedir, Ne İşe Yarar, Nasıl Üretilecek?", *Evrim Ağacı*¸15 Temmuz 2015, https://evrimagaci.org/kuantum-bilisim-kuantum-bilgisayarlar-nedir-ne-ise-yarar-nasil-uretilecek-3768.

[18] "One and done: Single-atom transistor is end of Moore's Law; may be beginning of quantum computing", Purdue University, 19 February 2012, https://www.purdue.edu/newsroom/research/2012/120219KlimeckAtom.html.

[19] Andrew Anthony, "Has the age of quantum computing arrived?", *Guardian*, 22 May 2016, https://www.theguardian.com/technology/2016/may/22/age-of-quantum-computing-d-wave.

[20] Fırat Demirel, "Moore Yasası", http://firatdemirel.com/moore-yasasi/; 14 Ağustos 2018

[21] "Radikal Olarak Basitleştirilmiş Pratik Kuantum Bilgisayarların İnşası", *NTBoxMag*, 13 Aralık 2016, http://www.ntboxmag.com/2016/12/13/radikal-olarak-basitlestirilmis-pratik-kuantum-bilgisayarlarin-insasi/.

[22] Zeki Seskir, "Kuantum Bilgisayar İçin Hangi Yan Sanayiler Gerekiyor", *Düzensiz*, 15 Ocak 2018, https://duzensiz.org/kuantum-bilgisayar-yan-sanayi-75aafe80b829.

[23] Sara Castellanos, "Venture Firms Back Startup with Novel Twist on Quantum Computing", *Wall Street Journal Blog*, 26 July 2017, https://blogs.wsj.com/cio/2017/07/26/startups-trapped-ions-could-lead-to-better-quantum-performance/.

[24] James Temperton, “Got a spare $15 million? Why not buy your very own D-Wave quantum computer”, Wired, 17 Ağustos 2018, https://www.wired.co.uk/article/d-wave-2000q-quantum-computer

[25] Marc Lallanilla, “Why Are Google & NASA Getting a Quantum Computer?”, *Live Science*, 16 May 2013, https://www.livescience.com/32080-google-nasa-quantum-computer-d-wave.html.

[26] Kozan Demircan, “Google Kuantum Bilgisayar Yarışında Yeni Çiple Öne Geçti”, Khosann (Kozan Demircan), 10 Mayıs 2017, https://khosann.com/google-kuantum-bilgisayar-yarisinda-yeni-ciple-one-gecti/.

[27] “World’s First Quantum Computer Made By China — 24,000 Times Faster Than International Counterparts”, *Fossbytes*, 04 May 2017, https://fossbytes.com/worlds-first-quantum-computer-made-by-china/.

[28] “Quantum Computers Strive to Break Out of the Lab”, IEEE Spectrum, 22 Mart 2018, https://spectrum.ieee.org/computing/hardware/quantum-computers-strive-to-break-out-of-the-lab

[29] C. Edward Kelso, “Bitcoin’s Encryption Could be Broken by 2027, Claim Singapore Quantum Experts”, *Bitcoin.com*, 10 November 2017, https://news.bitcoin.com/bitcoins-encryption-could-be-broken-by-2027-claim-singapore-quantum-experts/.

[30] Will Hurd, “Quantum Computing Is The Next Big Security Risk”, *Wired*, 12 July 2017, https://www.wired.com/story/quantum-computing-is-the-next-big-security-risk/.

[31] Adrian Bridgwater, “Five ways quantum computing will change cybersecurity forever”, *Racounter*, 17 December 2017, https://www.raconteur.net/risk-management/five-ways-quantum-computing-will-change-cybersecurity-forever.

[32] Davut Yılmaz, “Kuantum Çağı’na Hazır mısınız?”, *Bloomberg Businessweek Türkiye*, 10 Haziran 2018, ss. 4-5.

[33] Quentin Hardy, “A Strange Computer Promises Great Speed”, *New York Times*, 21 March 2013, https://www.nytimes.com/2013/03/22/technology/testing-a-new-class-of-speedy-computer.html.