Kuantum Bilgisayarlar

Muhammet Ali ŞEN
Bilgisayar Mühendisliği
Yıldız Teknik Üniversitesi
İstanbul, Türkiye
l1120701@std.yildiz.edu.tr

***Abstract*—Bu çalışmada kuantum mekaniği kapsamında günümüzde geliştirilme aşamasında olan kuantum bilgisayarlar ele alınmıştır. Kuantum fiziğinin en büyük deneylerinden olan çift yarık deneyi ile kuantum fiziğine yön veren bilim adamlarının ardından kuantum hesaplamalarının yapılması için geliştirilmesi planlanan kuantum bilgisayarların ne olduğu, kısaca çalışma stratejisi ve kuantum bilgisayarlar ile gelecekte bizlerin neyi beklediği açıklanmaya çalışılmıştır. Kuantum bilgisayarları için tasarlanan algoritmaların neler olduğu ve bu algoritmaların klasik bilgisayar bilimlerinin temeli olan hesaplama teorilerinde ne gibi etki oluşturduğu, kuantum hesaplamanın ne olduğuna da değinilerek kuantum dünyasının literatüründeki belli başlı kavramların neler olduğu yüzeysel olarak açıklanmaya çalışılmıştır.**

***Index Terms*—Kuantum, Bilgisayar, algoritma, kuantum bilgisayar, hesaplama teorileri, kuantum fiziği, kuantum mekaniği, çift yarık deneyi,**

I. Giriş

Kuantum bilgisayarlarının temeli kuantum mekaniğine dayanır. Kuantum mekaniği 20. yüzyılın başlarında, içinde bulunduğumuz evreni bir süreklilik olarak tanımlayan klasik mekaniğin yetersiz kaldığı durumlarda alternatif açıklamalar üretmek üzere geliştirildi. Örneğin 20. yüzyılın başlarına gelindiğinde klasik mekanik artık ışığın, enerjinin ve atomların yapısını açıklamakta yetersiz kalıyordu. Temelleri tam olarak 1925-1935 yılları arasında Werner Heisenberg, Erwin Schrödinger, Max Born, Pascual Jordan, Wolfgang Pauli, Niels Bohr, Paul Dirac, Friedrich Hund ve John von Neumann gibi bir avuç İngiliz, Alman ve Avusturyalı bilim insanı tarafından atılan kuantum fiziği, sonraki yıllarda başka bilim insanlarının katkısıyla daha da geliştirilerek günümüzün modern teknolojisinin oluşumuna çok önemli katkılarda bulunmuştur. Kuantum mekaniği sayesinde bugün herkesin yakından bildiği lazer, elektron mikroskopu, röntgen cihazı ve atom saati gibi teknolojik araçlar geliştirilmiş ve yarı iletken maddelerin yine kuantum mekaniği sayesinde incelenebilmesiyle günümüzün modern elektroniğinin temelini oluşturan yarıiletkenlik özelliğine sahip modern diyot ve transistörler icat edilerek, en sonunda bugün hepimizin kullandığı bilgisayarlar geliştirilmiştir. Nükleer silahların geliştirilmesinde de hayli önemli bir rolü olan kuantum mekaniğinin günümüzdeki en önemli uygulama alanlarından biri, kuantum bilgisayarları olarak da adlandırılan yeni nesil bir bilgisayarın geliştirilmesidir. [9].

Kuantum bilgisayarları klasik bilgisayarlardan ayıran temel özellik bilginin depolandığı ve işlendiği birimlerdir. Klasik bilgisayarlardaki bitlerin aksine kuantum bilgisayarlardaki kübitler, sadece “0” ve “1” durumlarında değil, bu durumların bir süperpozisyonunda da (yani her iki durumda birden) bulunabilir. Kübitler üzerinde yapılan bir işlem her iki durumu da aynı anda etkiler. Bir kuantum bilgisayarı N tane kübite sahipse, bu kübitler, kuantum mekaniği ilkeleriyle uyumlu bir biçimde, 2N farklı durumun süperpozisyonunda bulunabilir. Dolayısıyla N tane kübite sahip bir kuantum bilgisayarı, tek bir seferde 2N tane işlemi paralel biçimde gerçekleştirebilir. Kuantum bilgisayarları klasik bilgisayarlar karşısında güçlü kılan işte bu özellikleridir. [9] Davranışları kuantum mekaniği ilkeleri ile açıklanan sistemler üzerinde yapılan ölçümlerin sonuçları olasılığa dayalıdır. Bu yüzden kuantum bilgisayarlar için yazılan algoritmalar, doğru sonuçları kesin olarak vermez. Ancak işlemler ve ölçümler tekrarlandıkça elde edilen sonuçlardan biri eninde sonunda doğru olacaktır. Sonuçların olasılığa dayalı olması kuantum bilgisayarlarla yapılan hesapları tabii ki yavaşlatır. Ancak süperpozisyonun sağladığı hesaplama gücüyle karşılaştırıldığında bu durum önemsizdir. [9].

II. Çift Yarık Deneyi

Çift Yarık Deneyi olarak da bilinen Young Deneyi, fotonlar gibi parçacıkların hem dalga, hem parçacık olarak davrandığını ortaya çıkarması bakımından bilim için büyük öneme sahip olan bir deneydir. Dahası, bu deneyden sonra, sadece ışığın değil, elektronların da dalga özelliklerine sahip oldukları kanıtlanmıştır. Ancak deney, aynı zamanda sıra dışı bazı kuantum özellikleri de ortaya çıkararak, bilim insanları ve bilimseverler arasında oldukça popüler bir konuma gelmiştir. Orijinal çift yarık deneyini yapan Thomas Young, tek ışık kaynağı olarak, iğne deliğinden geçen Güneş ışığını kullanmıştır. Günümüze kadar bu deneyin sayısız versiyonu üretilmiş, konunun birçok yeni açısı keşfedilmiştir. [8]

Eğer bir fiziksel niceliği parçacık olarak tanımlamak istersek, durgun kütlesinin sıfırdan farklı olması gerekir. Dalga ise temel anlamda enerjinin yayılma ve taşınmasına yol açan titreşim hareketidir. Maddenin boyutu küçültülerek atomik yapısına inildiğinde karşımıza çıkan atom altı parçacıkların, ki bunlara kuantum düzeyindeki parçacıklar da denilmektedir, davranışları salt parçacık veya salt dalga gibi klasik konseptlere uymamaktadır. [8]

Maddenin doğası ile ilgili ikilik fikri ilk olarak 17. yüzyıldaki ışık ve maddenin doğası tartışmalarına dayanır (HuygensNewton). 1803'de ise fizikçi Thomas Young tarafından gerçekleştirilen "Çift Yarık", diğer bir adıyla "Çift Delik" deneyi, maddenin doğasında yer alan bu ikiliği ortaya koymak için yapılan başlangıç çalışmalarından biridir. Young, deney düzeneğinde tek ışık kaynağı olarak, iğne deliğinden geçen güneş ışığını kullanmıştır. İğne deliğinden yayılan ışık, üzerinde birbirine yakın iki iğne deliği bulunan ve deliklerin ilk kaynağa uzaklıkları eşit olacak şekilde yerleştirilen saydam olmayan bir engele düşürülür. Birinci iğne deliğinden herhangi bir anda çıkan ışık, diğer iki iğne deliğinden aynı anda geçeceği için, iki iğne deliğinden çıkan ışık o anda aynı fazda olur ve ekranda girişim saçakları (deseni) gözlemlenir. Young'ın çift yarık deneyinde sadece ışık üzerine denemeler yapılmıştır. Ta ki, 1961'de Clauss Jönsson bunu o zamana kadar parçacık tanımına uyan elektronlarla deneyene kadar. [10].

Yeni deneyin tam olarak anlaşılabilmesi için parçacıkların nasıl davrandıklarının görülmesi gerekmektedir. Bir elektron tabancasından (Eski tip televizyonlardaki katot ışın tüpü de diyebiliriz.) gönderilen elektronlar sadece tek bir yarıktan geçirilirse gözlem plakasında çarpma sonucu oluşan noktalar en sonunda düz bir çizgi oluşturur. Diğer bir deyişle, yarıktan geçebilen elektronlar tek bir doğrultuda ilerler. Benzer şekilde yarığa ışık gönderildiğinde plakada yine düz bir çizgi görülür. Bu çizgi ışığın en yoğun olduğu bölgedir. [10]

Yarık sayısı ikiye çıkartıldığı zaman ışığın dalga özelliğinden dolayı, bir girişim deseni oluşturduğu Young'ın deneyinde gösterilmişti. Bu durumda çift yarığa elektron gönderildiğinde, düz bir doğrultuda sadece iki yarığın birinden geçebilecekleri için iki sütundan oluşan bir görüntü elde edilmeliydi. Fakat elde edilen bir girişim deseniydi. Nasıl oluyor da madde parçacıkları tıpkı dalgalar gibi bir girişim deseni oluşturuyordu? İlk akla gelen elektronların toplu halde gönderildiğinde birbirlerine çarpıp doğrultu değiştirdikleriydi. Ancak elektronlar çift yarığa tek tek gönderildiğinde de sonuç değişmemişti. Dönemin bilim insanları elektronların nasıl bir hareket yaptığını gözlemlemek için sisteme bir dedektör eklediklerinde ise elektronlar bu kez parçacık gibi davranıp doğrultu değiştirmeyerek iki sütun oluşturdular. Deney yakından gözlendiğinde bir şeyler değişmişti. [8]

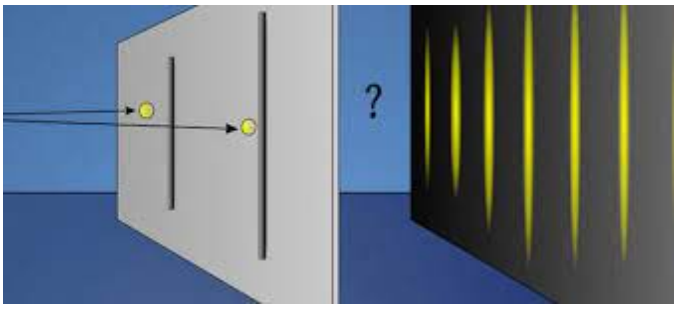

Fig. 1. Çift Yarık Deneyi

Tüm bu elde edilen sonuçların yorumlanması gerekiyordu. Bu nedenle fizikçi Niels Bohr tarafından oluşturulan konsey Kopenhag Yorumu adı verilen kuantum mekaniğinin görüş ve ilkeler dizisini yayınladı. Deneyin sonuçları buna göre şöyle maddelenebilir:

1) Makroskopik sistemler klasik fizik kuralları, mikroskopik sistemler ise kuantum mekaniğinin ilkeleri ile değerlendirilmelidir. Yani aynı deneyi elektrondan çok çok daha büyük parçacıklar olan bilyeler ile yaparsak ekranda göreceğimiz girişim deseni değil iki adet çarma sütunudur.
2) Bir mikroskopik sistemin konum ve momentum gibi durumlarını içeren bir dalga fonksiyonu vardır. Mikroskopik bir sistem olan elektrona da bir dalga fonksiyonu eşlik etmektedir hatta kendisi bir potansiyeller dalgasıdır.
3) Dalga fonksiyonunun normalizasyonu sistemin belli bir noktada değil, bölgede olduğunu söyler. Yani elektron parçacık olarak tabancadan çıkıyor ancak aynı zamanda bir potansiyeller dalgası olduğu için yarıklara ulaştığında her ikisinden de aynı anda geçerek kendisi ile girişiyor ve ekranda girişim deseni oluşturuyor.
4) Gözlemler dalga fonksiyonunu çökertir. Bir niceliği gözlemek üzerine ışık tutmak anlamına gelir ve elektron, foton ile etkileşebilecek kadar küçüktür. Bu etkileşim sonucu dalga fonksiyonu özelliğini kaybeder ve sadece parçacık özelliği gösterir.

Sadece tek bir deneyden dahi, böylesine büyüleyici sonuçların elde edilebilmesi, madde nedir sorusunun cevabının "hem dalga-hem parçacık" olduğunu göstermektedir. Görebildiğimiz makro evren yani biz ve çevremiz, matematiksel ve fiziksel olarak daha genel bir küme olan mikro evrenin özel bir durumuyuz. Sadece maddesel dalga boyumuz çok küçük olduğu için tamamen ihmal edilebilir bir dalga özelliğimizin yanında, tamamen parçacık özelliği gösteriyoruz. [10]

III. Kuantum Hesaplama

Günümüzde bilgisayar teknolojisi, insan beyni dışında, bizlere, hesaplama yeteneği kazandırmıştır. Bilgisayarlar, bir insandan çok daha hızlı bir şekilde hesaplama yapabildikleri gibi, bir insanın aynı anda aklında tutabileceğinden daha fazla bilgiyi depolayabilmekte ve bunlara hızlı bir şekilde erişilebilmesine olanak sağlamaktadırlar. İlkel bilgisayarlar mekanik bir mimariye sahipti. Bunlar daha sonra röleler, vakum tüpleri, transistorlar ve nihayet entegre devrelerle değiştirildiler. Her geçen gün bütünleştirilmiş devrelerdeki eleman sayısı artmakta, gelişen litografi teknikleri sayesinde bu devrelerdeki transistor boyları küçülmektedir. Intel Pentium 4 işlemcilerinde 42 milyon adet transistor bulunmaktadır. Bu sayı iki yıla yakın bir periyotta katlanarak artmaktadır. Intel bir on yıl daha bu şekilde gelişimin devam edeceğini tahmin etmektedir. [6] Bu gelişim yakın bir gelecekte mikroelektronik elemanların birkaç atomdan oluşan modelleri karşımıza çıkaracaktır. Bu boyutta, atomik ölçekte, fiziğin klasik kuralları değil, Quantum fiziğinin kuralları geçerli olmaktadır.

Mikroelektronik devre elemanları arasındaki sınırlardan elektronlar atlama yaparak mikroişlemcilerin, görevlerini yerine getiremez hale gelmelerine sebep olacaktır. Ancak bu aşamaya gelinmeden önce klasik bilgisayar mantığında çalışacak ancak Quantum fiziğinin kullanılacağı bilgisayarlar inşa edilebilecektir (Nanoteknoloji). Ancak bu tür bilgisayarlar Quantum algoritmaları yerine klasik bilgisayarlarda işletilebilen algoritmaları kullanacaklardır. Quantum sistemleri gerçek "Quantum Bilgisayarları" inşa edilebildiğinde asıl avantajı sağlayacaktır. Quantum teknolojisi çok daha fazla bitin aynı anda işlenmesine olanak tanıyacak, bilgi işleme teknolojisini temelinden değiştirecektir. [6].

IV. Kuantum Bilgisayarlar

Fig. 2. Kuantum Bilgisayar [12]

Quantum bilgisayarlarını klasik eşleniklerinden ayıran farklılığı vurgulamak için önce bit kavramına eğilmek gerekir. Fiziksel bakış açısından bir bit mantıksal iki durumdan birini (Evet-Hayır, Doğru-Yanlış veya basitçe 0-1) ifade etmek için hazırlanabilen bir fiziksel sistemdir. Örneğin günümüzün sayısal bilgisayarlarında bir kondansatörün levhaları arasındaki gerilim bir bitlik bilgiye karşılık gelir; yüklü bir kondansatör, bit değeri "1"e karşılık gelirken yüklü olmayan bir kondansatör ise mantıksal "0"a karşılık gelmektedir. Bir bitlik bilgi ayrıca ışığın farklı iki polarizasyonu veya bir atomun iki elektronik durumu kullanılarak da kodlanabilir. Ancak, bir atom fiziksel sistem olarak seçilirse atomun iki ayrık elektronik durumu dışında, atom, iki ayrık durumun bağdaşık (Coherent) bir üst konumunda da (Superposition) bulunabilir. Bu atomun hem "1" ve hem de "0" durumunda olması demektir. Bu durumun başka bir fiziksel sistemde karşılığı yoktur; bu durum tümüyle Quantum fiziğine has bir fenomendir. [9] Üç fiziksel bitten oluşan bir yazmacı ele alalım. Bu tür bir klasik yazmaç, bir anda, bu üç bitin karşılık gelebileceği sekiz sayıdan birini depolayabilir (000, 001, 010, ..., 111). Ancak üç qubit'ten oluşan bir Quantum yazmacı herhangi bir anda bir Quantum üst pozisyonunda bu sekiz sayının tümünü depolayabilir. [3].

Bir qubit aynı anda hem "0" ve hem de "1" değerlerini alabildiğinden bu şaşırtıcı bir sonuç değildir. Eğer bu yazmacı oluşturan qubit sayısı artırılırsa, depolama kapasitesi de üstsel olarak artacaktır. Örneğin dört qubit 16, beş tanesi ise 32 farklı sayıyı depolayabilecektir. Genel olarak L adet qubit 2L adet sayıyı aynı anda depolayabilir. Bir yazmaç değişik sayıların üst konumunda hazırlandıktan sonra üzerinde işlem gerçekleştirilebilir. Örneğin, eğer qubit'ler atomlar ise, uygun bir şekilde ayarlanmış lazer darbeleri atomların elektronik durumlarını etkileyecek ve kodlanmış sayıların başlangıçtaki üst konumlarını başka üst konumlara kaydıracaktır. Her sayının bu tür bir kayma ile etkilenmesi tek parça bir Quantum donanımı ile geniş hacimli bir paralel işleme yeteneği sağlayacaktır. Bu başka bir değişle L adet qubit'in bağdaşık üst konumlarında kodlanmış 2L adet girdi sayısı üzerinde tek adımda aynı matematiksel işlemi gerçekleştirilebilmesi demektir. Aynı işlemin klasik bir bilgisayarda gerçekleştirilebilmesi için aynı matematiksel işlemin tek işlemci ile 2L kez veya 2L adet farklı işlemci üzerinde paralel olarak işletilmesi gerekir. Özetle bir Quantum bilgisayarı zaman ve bellek gibi kaynakların kullanımında müthiş bir tasarruf sağlamaktadır. [5].

Kuantum bilgisayarı fikri ilk olarak 1980'lerde Nobel ödüllü fizikçi Richard Feynman tarafından klasik bir bilgisayarda çözülmesi çok uzun süren kuantum mekaniğinin karmaşık denklemlerini simüle etmek için ortaya atılmıştır. [9]

Kuantum bilgisayarları aslında bir bilgisayardan çok güçlü kuantum algoritmalarını sıradan bir işlemciden çok daha hızlı çalıştırabilen süper hesap makineleridir. Bunu fotonlar, elektronlar ve atomlar gibi temel parçacıkların ve aynı zamanda süper iletken devreler gibi daha büyük sistemlerin davranışından sorumlu olan kuantum mekaniği ilkelerini kullanarak yaparlar. Kuantum mekaniği, doğal dünyanın birçok yönünü klasik fiziğin yaptığından daha iyi açıklamakta ve klasik fiziğin ürettiği neredeyse tüm teorileri barındırmaktadır. [4]

Kuantum bilgisayarların ardındaki fizik, matematik ve bilgisayar biliminin büyüleyici karışımı oldukça karmaşıktır. Kuantum hesaplama (Quantum computing), kubit (qubit) olarak da bilinen kuantum bitlerini kullanır ve atom altı parçacıkların birden fazla durumda var olma yeteneğinden yararlanır. Kubitlerin bakımı inanılmaz derecede zordur, çünkü kubitler oldukça hassastır, ortamdaki en ufak bir değişikliğe tepki verirler ve kodlanmış verileri kaybedebilirler. [4]

Bu bileşenler, bir anlamda birçok potansiyel değeri aynı anda almalarına izin veren "süperpozisyon" adı verilen bir kuantum fiziği durumuna getirilebilir. Değerleri belirsiz olsa da daha klasik bir duruma indirgenmeden önce bir süperpozisyondayken bu kübitler üzerinde güvenilir hesaplamalar ve dönüşümler gerçekleştirilebilir, bu da hesaplamaları

etkili bir şekilde paralel hale getirir. [4]

Kuantum bilgisayarlar yeni nesil süper bilgisayarlardan tamamen farklı bir şey olarak karşımıza çıkar. Geleneksel bilgisayarlar 1 veya 0 olan transistörleri kullanır, bilgileri yalnızca 1 veya 0 değerine sahip bitlerde kodlayabilirler ve bu da yeteneklerini ciddi şekilde sınırlar. Daha fazla transistör bağlamak, gücü yalnızca doğrusal olarak artırır. Kuantum bilgisayarlarda ise yalnızca 0 veya 1 olabilen standart bir bilgisayar bitinin aksine, bir kübit bunlardan biri olabilir veya hem 0 hem de 1'in bir süperpozisyonu olabilir. Birbirine bağlanan kübitlerin sayısı, kuantum hesaplama gücünü katlanarak artırır. [4]

Kuantum bilgisayarlar için önemli bir sorun, bir kuantum hesaplamasının sonuçlarını doğru okumanın çok yüksek bir hata oranına meyilli olmasıdır. Bunun nedeni bir kuantum bilgisayar ile yakındaki elektrik alanları ve sıcak nesneler gibi çevresi arasında istenmeyen etkileşim anlamına gelen uyumsuzluktur. [4]

A. Kuantum Üstünlük

Kuantum üstünlüğü (quantum supremacy) bir kuantum bilgisayarın hızının klasik bilgisayarlarınkinden çok daha YÜKSEK olduğunu ima eder. Kuantum bilgisayarların klasik bilgisayarların yapamadığı şeyleri yapabildiği anlamına gelen kuantum üstünlüğü, basit bir avantaj değildir.

Peter Shor 1994'te bir kuantum bilgisayarın internetteki işlemleri koruyan şifrelemenin çoğunu kırabileceğini keşfetti. Shor'un algoritmasının, pratikte kuantum üstünlüğünü kanıtlamak için uygun olmamasının sebebi bu algoritmanın büyük bir sayıyı çarpanlara ayırmak için milyonlarca kübite ihtiyaç duymasıdır. Son teknoloji kuantum bilgisayarların yaklaşık 100 kübiti bulunur. Ve bunlar da hataya açıktır. [9]

Buna rağmen kuantum üstünlüğünü kanıtlamanın çetin bir rekabet alanı haline geldiğini söyleyebiliriz. 2019'da Google, 53 kübitlik kuantum bilgisayarı Sycamore'un, günümüzün en güçlü süper bilgisayarlarının binlerce yılda tamamlayacağı bir görevi birkaç dakika içinde çözdüğünü duyurmuştu. Bunun üzerine kuantum bilgisayarların geliştirilmesinde büyük bir rakip olan IBM, hemen itiraz etmiş ve klasik süper bilgisayarların aynı görevi 2,5 günde zaten yapabileceğini savunmuştu. [11]

Sonrasında 2021'de Çinli bir ekibin iddiasıyla Çin bir kez daha ne kadar güçlü bir rakip olduğunu kanıtladı: Ekip kuantum bilgisayarı "Zuchongzhi"nin normalde çözümü sekiz yıl sürecek olan bir sorunu bir saatte çözdüğünü iddia etti. [12]

B. Algoritmalar

Kuantum bilgisayar düşüncesi, ilk olarak 1982 yılında Richard Feynman tarafından ortaya atılmıştı. Aradan geçen kırk seneye yakın zamanda kuantum bilgisayarları için çok sayıda algoritma geliştirildi. Bu algoritmaların bazıları siber güvenlikle doğrudan alakalı matematik problemleriyle ilgili. Dolayısıyla günümüzde siber güvenliği sağlamak için kullanılan bazı yöntemlerin bu algoritmalar karşısında savunmasız kalacağı biliniyor. Bugüne kadar geliştirilmiş kuantum bilgisayarların hiçbiri bu algoritmaları uygulayarak modern kriptografik yöntemlerle hazırlanmış şifreli metinlerin çözülmesini sağlayacak kapasitede değil. Ancak birkaç sene içinde olmasa bile 30-40 yıl sonra siber güvenliği gerçek anlamda tehdit edecek kuantum bilgisayarların geliştirileceği düşünülüyor. En bilindik algoritmlar şu şekilde olarak:

1) Peter Shor 1994 yılında kuantum bilgisayarla çiftasal sayıların çarpanlarının hesaplanmasına imkân veren Shor Algoritmasını geliştirmiştir. Günümüzde laboratuvarlarda sadece bilimsel amaçlı deneyler için geliştirilen kuantum bilgisayarlarının test edilmesi için özellikle iki kuantum algoritması ön plana çıkıyor: Shor algoritması ve Grover algoritması. 1994'te Amerikalı matematikçi Peter W. Shor tarafından geliştirilen bu algoritma kuantum bilgisayarlarında çok büyük sayıları kolaylıkla faktörlerine ayırabiliyor. Shor algoritmasının bu özelliği kriptoloji açısından çok büyük önem taşıyor, zira günümüzdeki şifreleme mekanizmaları çok büyük sayıların klasik bilgisayarlar tarafından kabul edilir bir zaman dilimi içerisinde faktörlerine ayrılmasının mümkün olmadığı varsayımına dayanarak çalışıyor. Laboratuvar ortamları için geliştirilmiş ve çok az sayıda kubite sahip kuantum bilgisayarlarının bile en büyük sayıları, çok çok kısa sürede faktörlerine ayırabilmesi bugüne kadar bildiğimiz klasik kriptoloji biliminin temellerini şimdiden sarsarak kuantum kriptoloji adlı yeni bir bilim dalının yolunu açıyor.
2) 1996 yılında Lov Grover, kuantum hesaplamalarının gelişimiyle birlikte, sıralanmamış bir veri tabanı üzerinde arama yapmak üzere geliştirilmiş Grover algoritmasını geliştirmiştir. Hint asıllı Amerikalı bilgisayar bilimci Lov Grover tarafından geliştirilen Grover algoritması (GSA) çok büyük veri tabanlarında aranan bir bilginin, gerekli sorgulamanın çok detaylı bir şekilde formüle edilmesine gerek kalmadan fakat yine de hızlı bir şekilde bulunmasını sağlıyor. GSA da diğer birçok kuantum algoritması gibi olasılık kuramı tabanlı çalışan bir algoritma, dolayısıyla doğru cevabı bulabilmesi için veriler üzerinde çoğu zaman sadece bir kez değil, birçok defa çalıştırılması gerekiyor. Bu şekilde aynı verileri birçok defa işleyen algoritma, en sonunda doğru olma olasılığı en yüksek cevabı buluyor.
3) 1985'te David Deutsch tarafından geliştirilen Deutsch algoritması bilim tarihindeki ilk kuantum algoritması. Sadece tek bir kubit üzerinde işlem yapabilen Deutsch algoritması, günümüzde de klasik algoritmaların sınırlarına dayandığı yerde kuantum algoritmalarının olağanüstü bir işlem hızıyla sonuca ulaşabildiğini kanıtlaması açısından hayli önemli bir yere sahip. 1992'de yine David Deutsch ve Richard Josza tarafından genelleştirilerek sınırsız sayıda (n tane) kubit üzerinde işlem yapabilecek şekilde tekrar formüle edilen ve Deutsch-Jozsa algoritması adını alan Deutsch algoritması, daha sonraki yıllarda geliştirilen Shor ve Grover algoritmaları için gerçek bir ilham kaynağı olmuştur. [7]

verilebilir.

C. Kuantum Bilgisayarlar Ne işe Yarar ?

Kuantum bilgisayarlarının süperpozisyon ilkesinin beraberinde getirdiği süper paralel işlem yapma yeteneğinden ve programlanmalarının hayli zor olmasından dolayı ilk aşamada sadece günümüzün klasik bilgisayarları ve süper bilgisayarlarının yardımıyla çözülemeyen veya son derece uzun sürede çözülebilen özel problemlerin çözümünde kullanılması planlanıyor. Gelecekte kuantum bilgisayarlarının başlıca uygulama alanları şunlar olacak: [9]

1) Çok büyük sayıların olağanüstü hızlı bir şekilde faktörlerine ayrılarak, günümüzde hiçbir şekilde kırılamayacağı düşünülen şifreleme mekanizmalarının sadece saniyeler içinde kırılması
2) Kuantum sistemlerini atom düzeyinde simüle ederek, bu simülasyonlar sonucunda gerçeğe yakın sonuçlar elde edilmesi ve özellikle tıp, ilaç sektörü gibi alanlarda bugüne kadar erişilemeyen bilgilere erişilmesi
3) Olağanüstü derecede kapsamlı veri tabanlarının çok hızlı bir şekilde sorgulanması

Gelişmeler artık dijital sistemlerin günlerinin sayılı olduğunu gösteriyor, fakat kuantum bilgisayarlarının tam anlamıyla hayata geçirilebilmesi için bilim insanlarının önünde daha uzun bir yol olduğu da açık, çünkü kuantum bilgisayarları klasik mekanik kanunlarına göre değil, insanlığın henüz tam bir fikir sahibi olmadığı kuantum mekaniği yasalarına göre çalışıyor. Bu nedenle ilk aşamada bu yasalarla uyumlu çalışacak kuantum mikroişlemcilerin, kuantum belleklerin, kuantum algoritmalarının ve hatta yeni kuantum programlama dillerinin geliştirilmesi gerekiyor. İlk kuantum bilgisayarlarının üretimine odaklanmış firmaların mühendisleri ve bu konuda araştırma yapan diğer bilim insanları önümüzdeki 15-20 yıl içinde ilk kuantum bilgisayarının prototipinin gerçekleştirilmiş ve üretime hazır olacağını belirtiyor. [3]

Kuantum bilişim, güvenli bilgi paylaşımı (hack'lenemez internet ağı) da dahil olmak üzere çeşitli uygulamalara sahiptir; kanser ve diğer sağlık sorunlarıyla mücadele etmenin yanı sıra yeni ilaçlar geliştirmekten ulusal güvenliğe kadar pek çok alanda büyük etkilerinin olacağı öngörülmektedir. [9]

Deloitte'un 2021 raporu, kuantum hesaplama yaklaşımlarıyla dönüştürülebilecek düzinelerce uygulamayı listelemiştir; akışkan simülasyonu, kriptografi, kredi taahhüt, finansal risk analizi, tedarik zinciri optimizasyonu ve tahmini, arıza analizi, dolandırıcılık tespiti, hava tahmini, yarı iletken çip tasarımı, ürün portföyü optimizasyonu...

Kuantum bilgisayarlar, radarların füzeleri ve uçakları tespit etme yeteneklerinin geliştirilmesine yardımcı olabilir. Büyük veri analizi veya simülasyonları için kullanılabilir. Kimyasal sensörler kullanarak suyu temiz tutmaya yarayabilir.

Kuantum hesaplama, daha iyi tahminler ve kararlar almak için genellikle çok büyük miktarda verinin işlenmesini içeren yapay zekada potansiyel olarak yeni fırsatlara yol açabilir. [2]

Hesaplama hızı, uzun zamandır finansal piyasalarda bir avantaj kaynağı olmuştur. Kuantum algoritmaları, önemli bir dizi finansal hesaplama için hızı artırabilir.

V. Özet

Ticari ya da bireysel kullanıma yönelik bir kuantum bilgisayar henüz geliştirilmemiş olsa da uzmanlar, kuantum sistemlerinin önümüzdeki yıllarda ilaç geliştirme, finans, makine öğrenimi gibi pek çok sektöre değer sağlayabileceğini ifade etmektedir.

Google, IBM, Microsoft gibi teknoloji devlerinin peşinde koştuğu kuantum bilgisayarlar; birçok alandan bilim insanlarının birlikte çalışması için muazzam bir fırsattır. Kuantum Bilgisayar Nedir? sorusunun yanıtları gerçek dünyada kuantum bilgisayarlara giden yolun uzun olacağını ancak yol boyunca birçok heyecan verici keşfin insanlığı beklediğini işaret etmektedir.

Kaynakça

[1] M. E. Ocak, "Kuantum Bilgisayarlar Çağında Kriptografi", Bilim ve Teknik, Şubat 2020, https://bilimteknik.tubitak.gov.tr/system/files/makale/44-51_kuantum.pdf.

[2] Seth Lloyd Peter W. Shor'un "Kuantum Hesaplamaya Giriş" dersi, E. T.: 2006. http://web.mit.edu/2.111/www/.

[3] John Preskill'in "Kuantum Hesaplama" dersi, Erişim Tarihi: 2006.http://www.theory.caltech.edu/~preskill/ph229/.

[4] Centre for Quantum Computation, E. T.: 2006.http://www.qubit.org/

[5] Bennet C. H. ve Brassard G., "Quantum Cryptography: Public Key Distribution and Coin Tossing", Proc. Int'l Conf. Computers, Systems Signal Process., CS Press, s.175–179, 1984.

[6] Kaplan, Y. "Quantum Computing", https://www.yasinkaplan.com/tr/docs/QC.pdf

[7] Ege, B. "Kuantum Mekaniğinden Kuantum Bilgisayarlarına", http://bortecin.com/kuantum_bilgisayarlari.pdf

[8] Haliki, E.,"Maddenin Dalga Parçacık İkiliği: Çift Yarık Deneyi ve Varyasyonları", 2018,https://rasyonalist.org/yazi/maddenin-dalga-parcacik-ikiligi-cift-yarik-deneyi-ve-varyasyonlari/

[9] https://www.youtube.com/watch?v=Jj5ix0NOFLo

[10] https://www.youtube.com/watch?v=JILLwsGdRGg

[11] Giles M., "IBM's new 53-qubit quantum computer is the most powerful machine you can use",2018 https://www.technologyreview.com/2019/09/18/132956/ibms-new-53-qubit-quantum-computer-is-the-most-powerful-machine-you-can-use/

[12] Ölmez Y., "Çin, Zuchongzhi İşlemcisiyle Kuantum Avantajını Tekrardan Gösterdi ",2021 https://kuantumturkiye.org/cin-zuchongzhi-islemcisiyle-kuantum-avantajini-tekrardan-gosterdi/