

# Quantum Computing Hakkında Araştırma Çalışması

Merve Doğan  
Bilişim Sistemleri Mühendisliği  
Kocaeli Üniversitesi

Umuttepe Kampüsü, 41380, Kocaeli-Türkiye  
[191307011@kocaeli.edu.tr](mailto:191307011@kocaeli.edu.tr)

**Özet-** Kuantum hesaplama; bilimde, hayat kurtaracak ilaçlarda, hastalıkların erken teşhis tanı teknikleri için makine öğrenmesinde, daha etkili cihazlar kurmayı sağlayacak malzeme yapımında, daha iyi bir emeklilik yaşamı için finansal stratejiler oluşturma gibi birçok sosyoteknik alanda yeni atılımları teşvik edebilir. Kuantum işlemcilerin yapı taşı olan kübitler, kuantum bilgisayarların programlanmasına olanak tanıyan tekli ve çoklu kuantum mantık kapıları, kübitlerde süperpozisyon durumu, kuantum dolanıklığı ve kuantum dolanıklığının programlanması incelenmiştir. Kuantum algoritmalarına, toplama işlemi ve Grover Algoritması örnek olarak verilmiş; detaylı açıklamaları ile birlikte simülasyon ve gerçek kuantum bilgisayarda çalıştırılmış ve elde edilen sonuçlar incelenmiştir. Bütün bilgi-işlem sistemleri, temel depolama ve veri işleme yeteneğine dayanırlar. Klasik bilgi teorisi, bilgisayar bilimi ve kuantum fiziğinden fikirleri bir araya getirir. Evrensel kuantum bilgisayarı (QC), Church-Turing ilkesine ve bir ağ hesaplama modeline dayalı olarak açıklanmaktadır. Bu gözden geçirme, yalnızca kuantum hesaplamayı değil, kuantum bilgi teorisinin tüm konusunu özetlemeyi amaçlamaktadır. Bilgi, bir nedenden sonuca doğru yayılması gereken en genel şey olarak tanımlanabilir. Bu nedenle fizik biliminde temelde önemli bir role sahiptir.

**Anahtar Kelimeler** -Kuantum hesaplama ,QC ,kuantum fizik ,Church-Turing ,tarihi, Kuantum bilgisayar, Kuantum dolanıklığı, Grover algoritması

**Abstract-** Quantum computing; It can spur new breakthroughs in science, life-saving drugs, machine learning for early detection of diseases, making materials to build more effective devices, and creating financial strategies for a better retirement life. Qubits, which are the building blocks of quantum processors, single and multiple quantum logic gates that allow programming of quantum computers, superposition state in qubits, quantum entanglement and programming of quantum

entanglement are examined. As examples of quantum algorithms, addition operation and Grover's Algorithm are given; It was run on simulation and real quantum computer with detailed explanations and the results were examined. All computing systems rely on basic storage and data processing capability. It brings together ideas from classical information theory, computer science, and quantum physics. The universal quantum computer (QC) is explained based on the Church-Turing principle and a network computing model. This review aims to summarize the entire topic of quantum information theory, not just quantum computing. Knowledge can be defined as the most general thing that needs to be propagated from a cause to an effect. Therefore, it has a fundamentally important role in physical science.

**Keywords-** Quantum computing, QC, quantum physics, Church-Turing, history, Quantum computer, Quantum entanglement, Grover's algorithm

## I.GİRİŞ

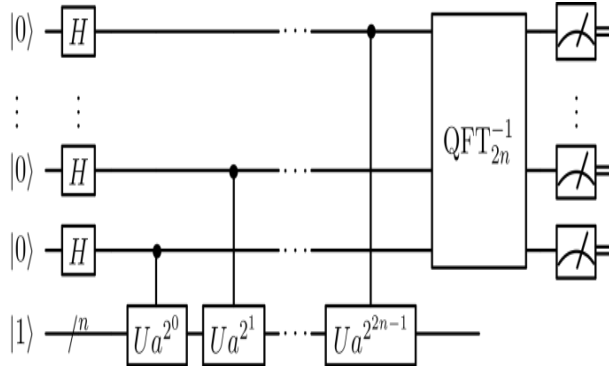
Bilgisayar dünyasında yıllar boyunca bir konu üzerine hep tartışmalar, ve olaylar döndü. Belli bir büyüklük ve karmaşıklık seviyesinin üzerindeki problemler söz konusu olduğunda, Dünya bunlarla başa çıkacak yeteri hesaplama gücünden yoksun. Bu sorunlardan bazılarını çözmek için yeni bir hesaplama türüne ihtiyacımız var. Bugün günümüz bilgi sistemlerinde bütün hepsi 0 ve 1'lerden oluşan mantık ilkesine dayanır. İzlediğimiz dizi, yazdığımız kitaplar, oynadığımız oyun, yayınlanan filmler ve daha fazlası. [GÜNDOĞAN,2021] Kuantum bilgisayarlar ise kuantum mekaniğinde sunulan matematiksel modeli kullanarak günümüzde hali hazırda kullanılmakta olan klasik bilgisayarlardan çok daha hızlı bir şekilde hesaplama yapılabilmesine olanak tanımaktadır.[1] Makalenin düzeni şu şekilde olacaktır: II. bölümde Kuantum hesaplamanın ne işe yarayacağından, faydalarından ve Shover ve Grover algoritmasından bahsedilecektir. III. bölümde kuantum hesaplamanın tarihinden ve temelleri anlatılacak. IV. bölüm de Kuantum faz eşleştirme, faz düşürme ve faz hızlarından bahsedilecek. V. bölümde IBM Kuantumu anlatılacak. VI. bölüm de kuantum bilgisayarlarına değinilecek. VII. bölüm de Kuantum dolanıklığından bahsedilecektir.Son olarak VIII. bölümde sonuçlar

## II.KUANTUM HESAPLAMA NE İŞE YARAR

Kuantum hesaplamanın birçok alanda sayısız faydası olacaktır. Bununla beraber kuantum mekaniğinin çalışma şeklini ve kuantum bilgisayarların geliştirilme sürecinde nasıl kontrol edilip kullanılacağını anlatmak da epey farklı bir zorluk. Kuantum bilgisayarların tek amacı kriptografik yapıları bozulmaya uğratmak veya şifreleri çözmek değildir. Kuantum bilgisayarlar yardımıyla aynı zamanda günümüzdekinden çok daha güçlü şifreleme altyapıları da oluşturulabilir. Bir kuantum sisteminde başkaları tarafından izlenip izlenmediğimizi anlamak amacıyla dolaşıklık özelliğinden faydalanabiliriz. Böylece kuantum işlemciler tasarlanana kadar yan teknoloji aktarımıyla daha farklı alanlarda bilimsel anlamda başarılar elde edilebiliyor. Kuantum bilgisayarlar şu an ki bilgisayarlardan farklı olarak yeni algoritmalar kullanmaktadır. Bilim adamları tarafından geliştirilen iki adet algoritma vardır. Bunlar Shover ve Grover algoritmalarıdır.

#### A. Shover Algoritması

Shor algoritmasının çözdüğü ana problem verilen bir tamsayının bütün asal çarpanlarını bulmakla ilgilidir. Hesaplamanın karmaşıklığından ötürü pek çok kriptografik yapının merkezinde yer alır. Kuantum için bu algoritma en iyi versiyondan bile hızlı işleme imkanı tanır. Gerçek dünyada bu algoritmanın kuantumla kullanılması durumunda birçok güvendiğimiz kriptografik teknolojinin bozulması ve kırılması kaçınılmaz olur.

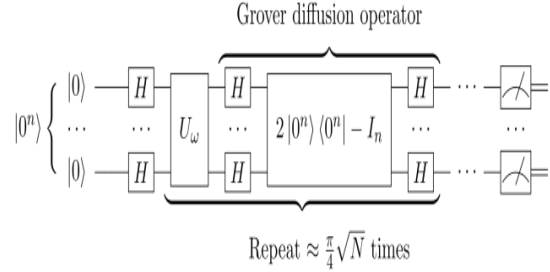


Şekil 1. Shover algoritması

#### B. Grover Algoritması

Grover algoritması, klasik bilgisayarlarımızın şu anki algoritmalarından çok daha fazla hızlı bir yapıdadır. Çoğu klasik algoritmanın verileri araması sırasında nesneleri teker teker tespit edebilmesi gerekiyorken, Grover'in algoritması sayesinde eldeki bütün nesnelerin karekökü gözlemlenerek arama işlemi yapılır. Birçok algoritmanın temeli

arama ve buna göre veriyi işleme üzerine olduğundan, bu algoritma bilimsel hesaplamalar açısından da oldukça önem arz eder. Birçok problemin, aşılmaz denilen zorluğun aşılmasını sağlar. [2]



Şekil 2. Grover algoritması

### III. KUANTUM HESAPLAMANNIN TARİHİ GELİŞİMİ

Kuantum bilgisayar fikri ilk olarak 1970 ler ve 1980 lerin başında fizikçi ve bilgisayar bilimcileri tarafından ortaya atıldı. Bu bilimcilerden bazıları IBM'in Thomas J. Watson Araştırma Merkezinden Charles H. Bennett, Illinois'te ki Argonne Ulusal Araştırma Laboratuvarı'ndan Paul A. Benioff, Oxford Üniversitesinden David Deutsch ve daha sonraları Kaliforniya Teknoloji Enstitüsünden Richard P. Feynman'dır. Bu fikirler bilim adamlarının bilgisayarların hesaplama kapasitesindeki sınırların fark edilmesiyle başladı. Moore kuralı olarak bilinen teoriye göre bilgisayar devreleri zamanla gittikçe küçülmektedir ve sonucunda da bir kaç atomdan oluşan boyutlara kadar küçülecektir.

1982 de, Feynman, kuantum fiziğinin nasıl hesaplamada kullanılabileceğini gösteren teorik bir model tasarladı.

1985'te Deutsch, Feynman'ın önermelerini kullanarak ilk kuantum bilgisayar fikrini ortaya atmış ve bu bilgisayarla tüm fizik olaylarının modellenmesinin mümkün olduğuna dair bir makale yazmıştır. Bu aynı zamanda, kuantum bilgisayarının klasik bilgisayarın yapabileceği her şeyi yapabileceğini söylemektedir.[3]

#### A. Kuantum Hesaplamanın Temeli

Bütün bilgi-işlem sistemleri, temel depolama ve veri işleme yeteneğine dayanırlar. Mevcut bilgisayarlar, veriyi 0 ve 1 şeklindeki ikili durumlarda depolayan tekil bitleri işlerler. Kuantum bilgisayarlar ise veri

işlemek için kuantal fenomenlerden yararlanırlar. Bunu kuantum bit ve kubitleri ile yaparlar.[4]

#### IV.KUANTUM FAZ EŞLEŞTİRME,FAZ DÜŞÜRME VE FAZ HIZLARI

Uzun bir süre boyunca, QC araştırması, dünyadaki sadece birkaç seçkin akademik seçkinin lüksü oldu, ta ki Shor'un [5] ünlü asal çarpanlara ayırma algoritmasını icat ettiği 1994 yılına kadar. Shor, bir QC'nin klasik bir bilgisayardan çok daha iyisini yapabileceğini somut bir örnekle gösterdi. Daha da önemlisi, büyük bir sayıyı çarpanlarına ayırmanın zorluğu, günümüzde yaygın olarak kullanılan Rivest–Shamir–Adleman (RSA) açık anahtarlı şifreleme şemasının temelidir. Shor'un algoritması sayesinde, Kuantum bilgisayarlar birdenbire gerçek bir olası tehdit haline geldi ve bu algoritma, Kuantum Bilgisayarlara dünya çapında ilgi uyandırdı. Shor'un algoritması yalnızca belirli bir soruna uygulanabilir.[6]

Grover'in algoritması, dijital şifreleme şeması (DES) şifreleme şeması optimizasyonunun deşifre edilmesi gibi birçok uygulamaya sahiptir.

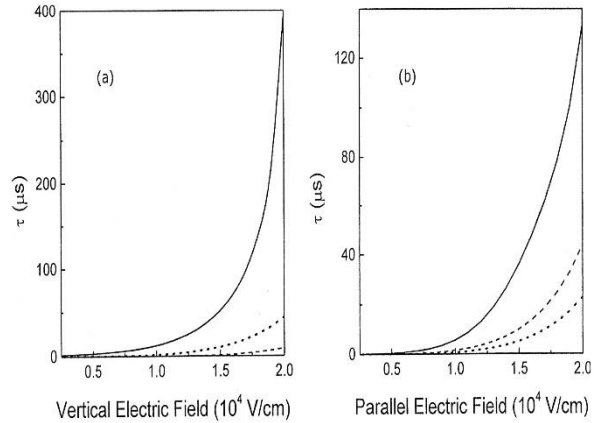
Standart Grover algoritması, klasik arama algoritmalarına göre ikinci dereceden hızlanma sağlar. Bu algoritmanın bir sorunu vardır: işaretli durumu bulma olasılığı hiçbir zaman tam olarak 1 olmayabilir. Bu zorluğun üstesinden gelmek için, arama adımının yapılabilmesi için faz ters çevirmelerini daha küçük açılarla dönüştürerek değiştirilerek standart Grover algoritmasını genelleştirmek gerekir. daha küçük Yalnızca işaretli durumun yalnızca daha küçük bir faz dönüşünü kullanan genelleştirilmiş algoritmanın yanlış olduğunu ortaya çıkardı[7]. Ayrıca, her iki faz ters çevirmesi de değiştirilirse, o zaman iki fazlı dönüşler bir faz eşleştirme gereksinimini [8] karşılamalıdır.

##### A.Qubit'te Faz Düşürme Hızı

Son zamanlarda yapılan bir çalışmada, statik bir elektrik alanının bir QD'de faz azaltma oranını etkili bir şekilde azaltabileceğini veya dekoherans süresini uzatabileceğini açıklayarak ikinci noktaya odaklandık. Modelimizde  $|0\rangle$  ve  $|1\rangle$  arasında büyük bir enerji farkı varsaydık, böylece akustik ve optik fonon saçılmalarını ihmal edebiliriz. Yalnızca vakum dalgalanmasından gelen baskın uyumsuzluğu hesaba kattık. InAs'ın kendi kendine bir araya getirdiği QD'lerin bir silindir olduğunu varsaydık. Katı hal kubit için kullanılan GaAs'a

gömülü bir InAs tek elektronlu QD'nin faz değiştirme oranını inceledik. InAs ve GaAs malzemelerinin etkili kütleleri sırasıyla  $0,023 m_0$  ve  $0,067 m_0$  ve GaAs ve InAs'ın bant boşlukları  $1,518$  eV ( $1 \text{ eV} = 1,602 \times 10^{-19} \text{ J}$ ) ve sırasıyla  $0,418$  eV. İletim bandı kaymasının, bant aralığı farkının %70'i olduğu varsayılmıştır. Malzeme dielektrik sabiti  $\epsilon_r, 12.250$ 'a [9] eşittir.

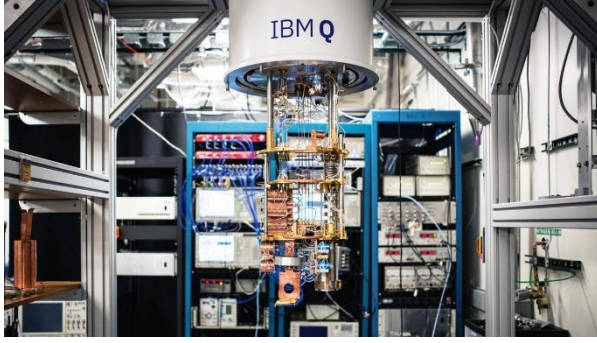
Şekil 3 a ve b, aynı yarıçap (5 nm) ve 3 farklı yükseklik için sırasıyla dikey ve paralel statik elektrik alanının bir fonksiyonu olarak uyumsuzluk sürelerini gösterir: 4 nm (düz çizgiler), 5 nm (noktalı çizgiler) ve 6 nm (kesikli çizgiler). Bu şekilden, elektrik alanının şiddeti  $5 \text{ kV/cm}$ 'nin altına düşene kadar eşevresizlik süresinin hassas bir şekilde elektrik alana bağlı olmadığı görülebilir. Elektrik alan  $5 \text{ kV/cm}$ 'nin üzerine çıktıkça eşevresizlik süresi çok hızlı artar. 5 nm yarıçaplı ve 4 nm yüksekliğe sahip QD için  $20 \text{ kV/cm}$  statik elektrik alanı altında eşevresizlik süresi milisaniyeler mertebesine ulaşabilir. [Li-Uzun,Bai,Feng,Zheng,2001]



Şekil.3 Dikey ve Paralel Elektirik Alanları

#### V.IBM KUANTUM

IBM bilim insanları, IBM Cloud aracılığıyla sağlanan ve masaüstü veya mobil aygıtlar tarafından ulaşılabilen türünün ilk örneği olan bir kuantum bilgi işlem platformu olan IBM Quantum Experience'ı oluşturmaya başladı. Bu çalışma ile; kullanıcıların IBM'in kuantum işlemcisi üzerinde deneyler yapmasına, bireysel kubitler ile beraber çalışmasına ve kuantum hesaplamanın mükemmel olasılıklarının öğretici ve simülasyonlarını keşfetmesine olanak sağladılar.



Resim.1. IBM Kuantum

#### A. IBM Quantum bilgisayarın piyasaya sürülmesi:

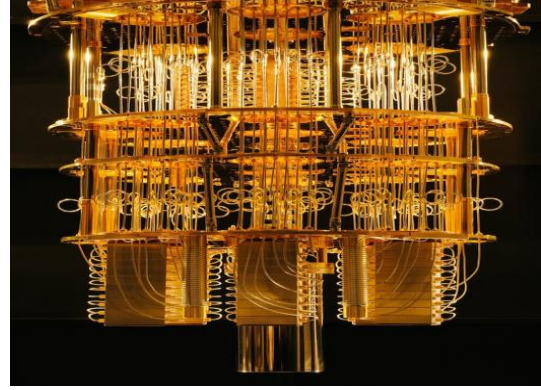
Kuantum hesaplama sistemleri oluşturmak için ilk endüstri girişimi 2017 yılında açıklandı. IBM Quantum sistemleri, şu anda yapısı gereği klasik ve normal bilgi işlemin üstesinden gelemeyeceği kadar karışık, zor ve deneysel sorunların üstesinden gelmek için tasarlanmayı hedefledi. IBM hedeflerinden birisi de bu çalışmanın kuantum hesaplamanın uygulanabilirliğini ve endüstrilerdeki faydasını göstermektir. Kuantum bilgisayarları daha güvenilir ve kararlı hale getirmek için IBM Quantum, ticari kullanım amaçlı dünyanın ilk entegre kuantum bilgi işlem sistemini oluşturdu. Bu sistem yani IBM Q Sistem 1, evrensel yaklaşık süper iletken kuantum bilgisayarların ilk defa araştırma laboratuvarının sınırları dışında çalışmasına olanak sağladı.[10]

### VI.KUANTUM BİLGİSAYARLAR

Kuantum bilgisayarlar, verileri depolamak ve hesaplamalar yapmak için kuantum fiziğinin özelliklerini kullanan makinelerdir. Bu, en iyi süper bilgisayarlarımızdan bile çok daha iyi performans gösterebilecekleri belirli görevler için son derece avantajlı olabilir. Bununla birlikte, klasik bilgisayarların hala kuantum bilgisayarlardan daha iyi performans göstereceği birçok durum olabilir. Dolayısıyla geleceğin bilgisayarları bu iki türün bir kombinasyonu olacak.

Şimdilik kuantum bilgisayarlar oldukça hassas: ısı, elektromanyetik alanlar ve hava molekülleriyle çarpışmalar bir kubitin kuantum özelliklerini kaybetmesine neden olabiliyor. Kuantum decoherence olarak bilinen bu süreç, sistemin

çökmesine neden oluyor ve ne kadar çok parçacık varsa olay o kadar hızlı gerçekleşiyor.[11]



Resim.2 Quantum Bilgisayarın sistem içinden bir görüntü

Artık bilgisayarlarımızı birbirine bağlamak gereksinmesine ihtiyaç duyuyoruz. Aslında uzun yıllar kuantum bilgisayarlara, atomaltı dünyanın karmaşık hesaplarını yapacak garip bir araç olarak bakıldı. Ancak, 1994 yılında AT&T araştırmacısı Peter Shor, kendi olağan dünyamızın zorlu bir matematik sorununun da, kuantum bilgisayarlarınca çözülebileceğini öne sürmüştü. Gelelim, şifre kırıcı kuantum bilgisayarlara, Bu 21. yüzyıl için bile zorlu bir hedeftir. Şimdilik, bir kubitlik "bilgisayarlar" başarı sayılıyor. Bunların bile boyutları bir hayli büyük. Önemli bazı problemleri klasik bilgisayarlardan ancak biraz daha hızlı çözebilecek kuantum bilgisayarların bile, en az 50 kubit içermesi gerekmektedir. Haber alma örgütlerin ise biraz daha beklmeleri gerekecek. İstedikleri türden hesapları yapabilecek kuantum bilgisayarların, bir hangar büyüklüğünde olacağı hesaplanıyor.[12]

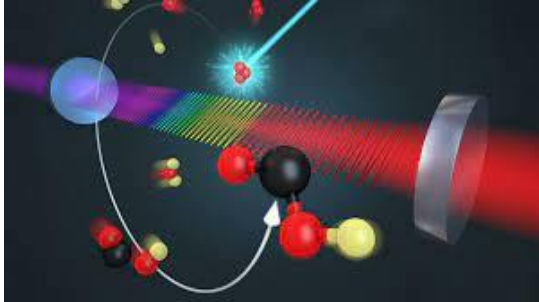
### VII.KUANTUM DOLANIKLIĞI

Niels Bohr'un dillendirip desteklemesiyle fizik dünyasını karıştırdığı kuantum mekaniği, Einstein'ın EPR fikri ile ortaya koyduğu zorluklar yıllar boyu bilim insanlarının kafasında soru işareti olarak kalmaya devam etti.

Kuzey İrlandalı fizikçi John Bell, EPR paradoksu hakkında araştırma yapmaya başladı. Zaten CERN'de günlük olarak yaptığı iş sürekli parçacık fiziğiyle aktif olarak uğraşmaktadır. 1964 yılında Bell, Einstein'ın ve Bohr'un söylediklerinin aslında farklı şeyler olduğunu kanıtladığı "On the Einstein-Podolsky-Rosen Paradox" isimli yazısını yayınladı. Fakat oldukça az dergide yayınlandı ve diğer fizikçilerle konusu bile açılmadı.

1972 yılında tesadüfen olarak bir başka fizikçi John Clauser makaleyi okudu ve fazlasıyla etkilendi. Bunu destekleyecek deneysel kanıtlar oluşturmayı planladı ve üstünde çalışmaya başladı. Berkeley’de bilim insanı olan Stuart Freedman ile beraber çalışarak bir lazer ışığını kuantum teorisine göre dolaşması gereken çift fotonlu kalsiyum atomuna yönltiltiler. Fotonları ise filtrenin arkasında bulunan bir dedektör yardımıyla ölçüp fotonların filtreden geçip geçemediğini ve birbiriyle alakalı olup olmadığını baktılar. Garip bir şekilde fotonlar arasındaki bağlantı deneysel sonuçlarla eşleşiyordu. Bohr’un fikrinin haklı olduğu böylece anlaşılmıştı.

Önyargıdan veya o dönemdeki atmosferden olsa gerek bilim dünyasında pek çok kişi bu deneye itibar etmedi. Bazı fizikçiler filtrelerin rastgele olduğu takdirde deney sırasındaki ölçümleri etkileyebileceğini düşündü, ta ki 2017 yılına kadar. “Cosmic Bell Test” adı verilen bir test yapıldı. Viyana Üniversitesi fizikçileri 1974’teki deneye benzer şekilde bir yapı tasarladılar. Bu yapıda ise filtreleri kontrol etmek amacıyla 8 milyar yıl kadar eski iki kuasarın ışığı kullanıldı. Sonuç yine aynı oldu. Uzaktaki parçacıkların aslında birbirine dolanmış olduğu görüldü.



Resim.3 Kuantum dolanıklığı görseli

Günümüzde kuantum bilgisayarların gelişiminin altında yatan şey bu aslında. Halihazırda kullanmış olduğumuz bilgi işlem teknolojilerinde bilgilerin kodlanması bitlerle gerçekleştiriliyor. İşlemcide hesaplanan her şey birer bit’ten ibaret. Kuantum bilgisayarlarla geliştirilen yapılar ise (kuantum biti veya kübit olarak adlandırılır) birbiriyle iç içe bulunuyor, bir kübitin değiştirilmesi sistemdeki kübit yapısının tamamen değişmesine neden oluyor.

Kuantum bilgisayarlar geliştirirken bu karmaşık yapıya dikkat edilmesi, bilginin depolanabilmesi ve değişime uğrayan bilginin anlamlandırılabilmesi bakımından oldukça önem arz ediyor.[13]

Kuantum mekaniğine göre süperpozisyonda dolanık hale getirilmiş iki parçacık, birbirlerinden ne kadar uzakta olursa olsunlar ölçümlendikleri zaman

birbirlerinin durumlarından haberdarlarmışçasına sonuç verirler [14]. Örneğin Dünya’da dolanık hale getirilmiş iki parçacıktan birinin Mars’a götürülmesi durumunda, Dünya’daki parçacık durumunda gözlemlenirse aynı anda Mars’taki parçacık da 0 durumunda gözlemlenmelidir. Aynı mantık çerçevesinde Dünya’daki parçacık 1 durumunda ise bu sefer Mars’taki parçacık da 1 durumunda gözlemlenmelidir.[15]

## VIII.SONUÇLAR

Kuantum hesaplama hakkında çalışmalar her zaman yapılmakla beraber tam olarak biteceği zaman belli değildir. Teknoloji ve zaman ilerledikçe bilim insanları keşfedilmemiş gelecek hakkında daha fazla araştırma yapmaktadır. Kuantum hesaplama ile beraber kuantum bilgisayarlar, kuantum fizik ve çeşitli algoritmalar hakkında da araştırmalar yapılmıştır ve çeşitli makaleler yazılmıştır. Kuantum hesaplama ile insan hayatına etkileri gözden kaçırılmayacak kadar önemli bir yere sahip olmaya başlayacaktır. Makale yazmak için yaptığım araştırmalar sayesinde kuantum hesaplamının özelliklerini, içeriklerini, geçmişten şimdiye kadar yapılan araştırma ve tezler hakkında bilgi sahibi oldum.

## KAYNAKÇA

Andrew Steane 1998 *Rep. Prog. fizik* **61** 117

[12]Gücü, H. G. Kuantum Bilgisayarlar.

[1,15]Mavi, A. Kuantum Hesaplamaya Teorik ve Uygulamalı Giriş

[2,11,13,14]<https://www.technopat.net/>[Son Erişim 2-5 Aralık 2022]

[3]West, J., & Grv, O. B. M. F. A. KUANTUM BİLGİSAYARI.

[4,10]<https://sophosakademi.org/>[Son Erişim 11 Aralık 2022]

[5,6,]<https://doi.org/10.1073/pnas.191373698>{[Son Erişim 16 Aralık 2022]}

[7,]JGL Long, WL Zhang, YS Li, L Niu *Theor Phys* **32** , 335–338 (1999).

[8,]GL Long, YS Li, WL Zhang, L Niu *Phys Lett A* **262** , 27–34 (1999).

[9,]SS Li, JB Xia *Phys Rev B* **58** , 3561–3564 (1998).

<https://iopscience.iop.org/> [ Son Erişim 5 Aralık 2022]

<https://www.matematiksel.org/> [ Son Erişim 1-7 Aralık 2022]