Tekin Dereli

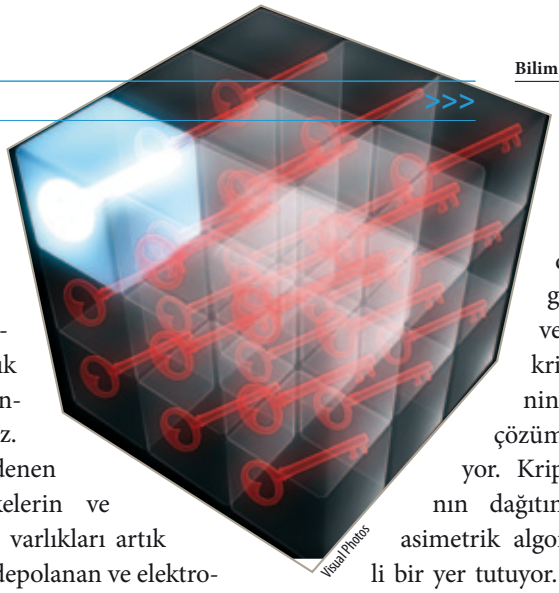
Prof. Dr., Fizik Bölümü
Koç Üniversitesi

İletişimde Mutlak Güvenlik İçin Kuantum Kriptografi

Kuantum kriptografi konusu alışılmadık kuantum teknolojilerine iyi bir örnektir. Bir foton çiftinin dolaşık bir kuantum durumunda hazırlandığını düşünelim. Bu dolaşık çifti özel optik lifler üzerinden uzayda birbirlerinden -aralarındaki mesafe çok uzun olacak şekilde- ayırır ve bizde kalan fotonun kutuplanma yönünü ölçerek belirlersek, eş-anlı olarak iyice uzakta olan ötekinin kutuplanma yönünü de belirlemiş oluruz. Bu çok hassas deney ilk kez 1997'de yapılabildi. Bugün artık piyasada, dolaşık foton çiftleri üstüne kurgulu "kuantum teleportasyon" yöntemiyle, birkaç yüz kilometrelik mesafe aralıklarında bile yüzde yüz güvenlikli kuantum anahtar dağıtımı yapılıyor.

Prof. Dr. Tekin Dereli Koç Üniversitesi Fizik Bölümü öğretim üyesidir. Yüksek lisans ve doktora derecelerini ODTÜ Fizik Bölümü'nde aldıktan sonra ABD ve Avrupa'nın tanınmış üniversitelerinde araştırmacı ve misafir profesör olarak bulunmuştur.
Uzun yıllardır üniversitelerimizde ileri düzeyde dersler vermekte ve doktora öğrencileri yetiştirmektedir. Kuantum mekaniği, kuantumlu ayar alanları ve genelleştirilmiş gravitasyon teorileri üstüne yayımlanmış 100'den fazla makalesi bulunmaktadır. 1996 TÜBİTAK Bilim Ödülü'nü kazanmıştır. Halen TÜBA Konseyi üyesidir. Prof. Dr. Tekin Dereli 1993-2000 yılları arasında TÜBİTAK *Bilim ve Teknik* dergisinde Yayın Kurulu üyesi olarak görevliydi.

Tarihsel gelişimine bakarsak kuantum mekaniği, gazların ışıma ve soğurma spektrumlarının neden her atomun kendisine özgü kesikli çizgilerden oluştuğunu açıklamaya çalışırken keşfedilmiştir. 1900 yılı Aralık ayında Alman fizikçi Max Planck'ın enerji kuantumları varsayımıyla başlayan kuantum serüvenindeki en önemli aşamalardan birisi, Albert Einstein'ın "foton" adı verilen ışık kuantumları yardımıyla fotoelektrik etkiyi açıklayabilmesi olmuştur. Einstein 1921 Nobel Fizik Ödülü'nü özel görelilik teorisi ile değil bu buluşu nedeniyle -hidrojen atomu modelini kuran Niels Bohr ile birlikte- 1922 yılında aldı. Bohr'un atomun kuantum teorisine Werner Heisenberg, Erwin Schrödinger ve Paul Dirac tarafından son halinin verilişini, yani kuantum mekaniğinin keşfini 1925-1930 arası diye kabul edebiliriz. Gerçi günümüzde atom çekirdeklerini oluşturan proton ve nötronların iç yapısını araştırma noktasını bile geçtik, ama genelde kuantum mekaniğini anlatırken 1930'larda yapılan buluşların ötesine pek geçilemiyor. Çünkü kuantum fiziğinde klasik fiziktekinden çok farklı bir dil ve alışılmadık, yep-



yeni kavramlar kullanılır. Kuantum mekaniğini anlıyorum demek ve doğru anlatabilmek hiç kolay değil. 1930'ların Kuantum Devrimi'nin gündelik yaşamımıza en çarpıcı yansımaları kanımca 1940'lardan sonra nükleer enerji üretiminin ve kullanımının yaygınlaşması, 1950'lerde transistorların devrelerde kullanılmasıyla başlayan mikroelektronik uygulamalar ve 1960'lardan sonra lazerlerin bulunması ve bunlara dayalı yeni iletişim teknolojilerinin geliştirilmesidir. Kuantum mekaniğinin gelişimi günümüzde de durmuş değil, hiç beklenmedik sürpriz buluşlar ve uygulamalarla 21.yüzyılda da sürüyor.

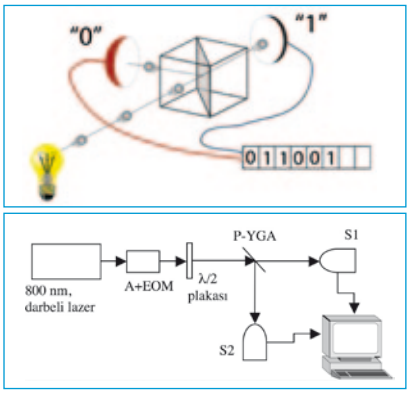
Kuantum etkilerinin yerel olmaması, teorinin keşfedildiği ilk günlerden başlayarak büyük tartışmalara neden oldu. Albert Einstein 1935'de "EPR paradoksu" diye adlandırılan bir düşünce deneyi üzerinde duruyor, kuantum etkilerinin fiziğin en temel varsayımlarından biri olan göreli neden-sonuç ilişkilerini bozacağını düşünüyordu. Yani kuantum etkileri yoluyla ışıktan hızlı bilgi iletiminin yapılabilirliği söz konusuydu. Einstein, bu mümkün olamayacağına göre kuantum mekaniğinin temelinde tutarsızlık olduğunu iddia ediyordu. Kuantum mekaniğinin felsefi temelinin oluşumuna büyük katkıları bulunan Niels Bohr Einstein'ın bu iddialarını anında yanıtladı. Ancak 1980'lere gelene dek Bohr'un savunduğu kuantum mekaniği yorumunun mu, yoksa Einstein'ın iddiasının mı haklı olduğunu kanıtlayacak herhangi bir gözlemsel veri yoktu. Teknolojinin ilerlemesiyle olanaklı hale gelen ve 1982'de yapılan deneyler kuantum mekaniğinin yerel olamayacağını, yani Einstein'ın haklı olmadığını artık göstermiştir. Bu olgunun klasik fizik kavramlarından ne denli farklı düştüğü, popüler düzeyde "Schrödinger'in kedisi" denen bir düşünce deneyi ile anlatılmak istenir. Kuantum mekaniğinin yerel olmaması ve buna benzer alışılmadık niteliklerinin ciddiye alınması ve bunlara uygulama aranması için bir 10 yıl daha geçti. Bu anlamda 1995 çok keskin bir dönüm yılıdır. Ayrıntılarına burada giremeyeceğim pek çok nedenden dolayı kuantum iletişim ve bilişim teknolojileri ile nanoteknolojinin başlangıcı olarak algılanan 1995 yılına 2. Kuantum Devrimi deniyor. 21.yüzyılla beraber artık kuantum mühendisliği çağındayız.

Bilgi çağı denen çağımızda, ülkelerin ve kişilerin değerli varlıkları artık bilgisayarlarda depolanan ve elektronik ağlarda taşınan verilerden ibaret. Bu tip verilere banka hesapları, devletin, sanayi ve ticaret kuruluşlarının gizli bilgileri gibi pek çok farklı örnekler verilebilir. Kişiler ve kurumlar arasında aktarılan bu bilgilerin gizliliğini sağlamak, değiştirilmesini engellemek, kaynağından emin olmak gibi temel güvenlik servisleri, kriptoloji biliminin matematiksel çözümleriyle sağlanıyor. Kripto anahtarlarının dağıtımında özellikle asimetrik algoritmalar önemli bir yer tutuyor. Ancak son yıllarda 5-6 bitlik kuantum bilgisayarlarının yapılabilirliğinin gösterilmiş olması, bu bilgisayarların büyük ölçekte gerçeklenmesiyle, kriptolojide önemli bir yer tutan günümüzün asimetrik algoritmalarını kırılabilir hale getirecektir. Bu,

Kuantum Fiziksel Rastgele Sayı Üreteci

Kuantum fiziksel rastgele sayı üretimi, kuantum fiziğinin ölçüm aksiyomunun bir sonucu olarak ortaya çıkar. Ölçüm aksiyomuna göre yarı geçirgen bir aynanın girişine tek fotonlar gönderildiğinde, geçirme ve yansıma çıkışlarındaki iki algılayıcıdan yalnızca biri eş-anlı algılama yapacaktır. Dolayısıyla yarı geçirgen aynanın çıkışındaki iki algılayıcıda yapılan algılamalar 0 ve 1 ile kodlandığında, yapılan algılamaların serisi ideal bir rastgele sayı üretecektir.

Kuantum fiziksel rastgele sayı gösterimi için kullanılması planlanan deneysel altyapı Şekil 1'de gösterilmektedir. Bir darbeli lazerin ışıma gücü yüksek oranda düşürülerek darbe başına 0,05 foton üretilen mertebeye getirilir. Bir λ/2 plakası ile gücü düşürülmüş lazer ışımasının doğrusal polarizasyonu 45° döndürülür. Polarize yarı geçirgen ayna (P-YGA) kullanılarak λ/2 plakasının çıkışındaki lazer ışımasının geçiren ve yansıtan kollara ayrılması sağlanır. Lazerin gücünün çok düşürüldüğü limitte, P-YGA'nın iki çıkışında bulunan tek foton sayaçlarından en fazla biri darbe başına foton algılayacaktır. Bu algılayıcıların algılamaları 0 ve 1 ile kodlanarak elde edilen bit serisi ile rastgele sayı üretimi gerçekleştirilmiş olacaktır.

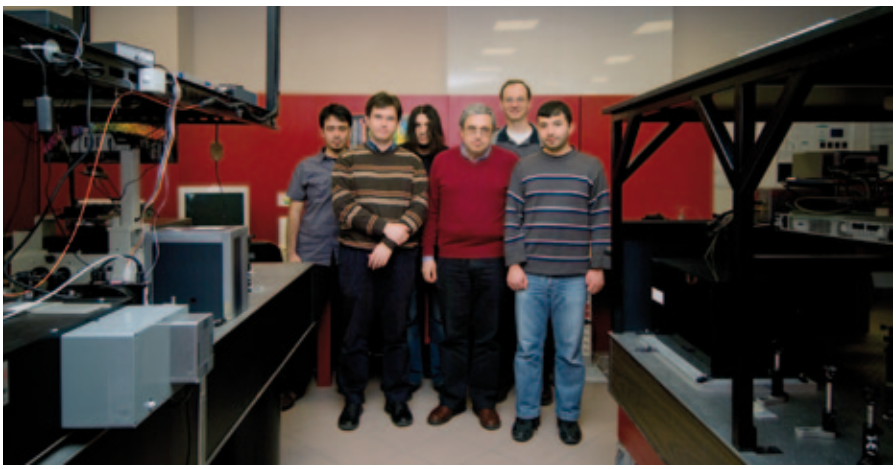


Kuantum fiziksel rastgele sayı üreteci için kullanılması öngörülen deneysel düzenek. A, lazer güç düşürücü filtreler; EOM, Elektro-optik modülatör; P-YGA, Polarize yarı geçirgen ayna; S1, S2 tek foton sayacı

Tek foton kaynaklarının temininden sonra kuantum kriptoloji sistemlerinin performansı büyük ölçüde tek fotonları bile algılayabilen tek foton sayaçlarının performansına bağlıdır. Tek foton sayaçları fotonları elektronlara çeviren aygıtlardan, hızlı güçlendirici devrelerden ve oluşan sinyalleri ölçebilen devrelerden oluşur. Günümüzde avalanş-fotodiyotlar, fotogüçlendiriciler (*photo-multipliers*), çok kanallı levha (*multichannel plate*) ve süperiletken Josephson eklemli (*Josephson junction*) aygıtlar, fotonları yüksek kuantum verimlilikle elektronlara çevirir.

kriptolojinin temel güvenlik unsuru olan kripto anahtarlarının güvenli dağıtımına yönelik büyük bir tehdittir. Kuantum anahtar dağıtımı bu tehdide karşı öne sürülmüş pratik bir çözümdür. Halihazırda büyük ölçekli kuantum bilgisayarı henüz gerçeklenememiş olmasına rağmen, başarılı kuantum anahtar dağıtım sistemlerinin çalışan örnekleri verilmiştir. Gizli bilgilerin başarıyla korunmasının bir ülkenin ekonomik ve sosyal yaşamındaki önemi aşikârdır. Günümüzde özellikle gelişmiş devletler birbirlerinin sırlarını öğrenmek için yüksek teknolojiye dayalı dinleme ağları ve kripto analiz altyapıları oluşturmuştur. İleri devletler bu aşamalardan da ileri giderek kuantum kriptolojiye bankacılık gibi özel sektör uygulamalarında da yer verir olmuşlardır.

Günümüzün kritik teknolojileri arasında bulunan kuantum kriptoloji konusunda uluslararası düzeyde çalışmaların yürütüldüğü birçok araştırma merkezi vardır. Bu konuda lider şirketler (merkezi Boston'da olan BBN, New York'ta olan MagiQ ve Cenevre'de olan idQuantique) çeşitli bankalar ve finans kuruluşları için kuantum kriptoloji cihaz ve yazılımları sunmaktadır. Her ne kadar çeşitli askeri kuruluşların ve gizli servislerin de kuantum kriptolojiden istifade ettiği düşünülse bile, gizlilik kuralları nedeniyle bu konuda geçer veri elde etmek olanaksızdır. Bilinen tek açık hükümet uygulaması, İsviçre'de 2007 Cenevre Kanton seçimlerinde kâğıt oyların girildiği bilgisayarlar ile tüm oylarla ilgili verilerin toplandığı merkez arasındaki bilgi transferinin emniyeti için kuantum kriptoloji kullanılmasıdır. Dünyada pek çok ülke kendi kuantum bilgi teknolojileri ve özellikle kriptoloji merkezlerini kurmuş ve kurmakta. Avrupa'daki tüm ülkelerin, uzak doğuda Singapur ve Tayland dahil tüm ülkelerin, Güney ve Kuzey Amerika ülkelerinin ve Avustralya'nın kuantum teknolojileri konusunda uzmanlaşmış merkezleri vardır. Bu merkezler üniversite bünyesinde veya

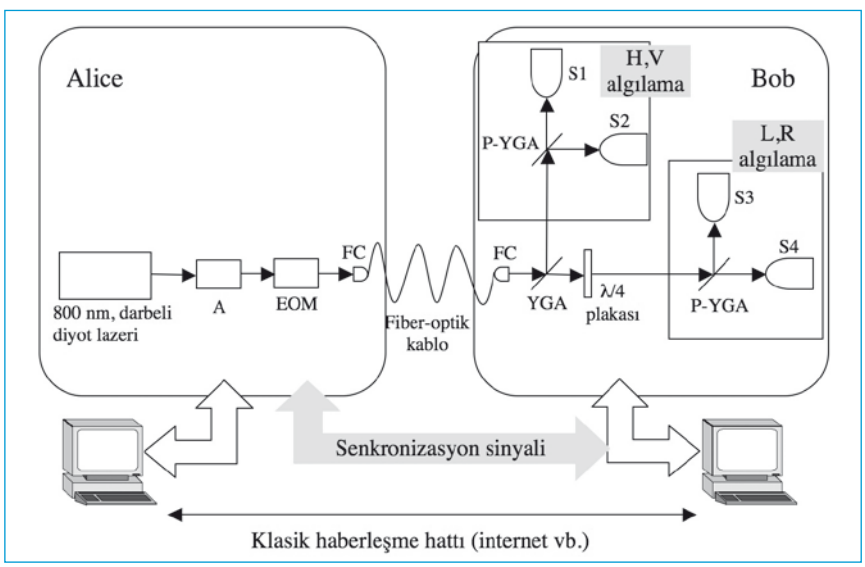


Prof. Dr. Tekin Dereli ve proje ekibi Koç Üniversitesi'ndeki laboratuvarlarında

Kuantum Anahtar Dağıtımı

Tek fotonlar kullanılarak kurulan bir haberleşme hattında ideal güvenlikte bilgi alışverişi gerçekleştirmek de mümkün. Böyle bir haberleşme hattında, dinleme yapan bir casusun kaydedeceği bilgiler göndericiden alıcıya ulaşamaz. Dolayısıyla alıcı için bir bilgi değeri taşımaz. Öte yandan alıcı tarafına bir bilgi ulaştığında, bu bilginin bir casus tarafından dinlenmemiş olduğu da kesin olur. Bu özellik kullanılarak, kriptoloji sistemlerinde ideal güvenlikte anahtar dağıtımı gerçekleştirilebilir. Tek fotonlar kullanılarak yapılan bu anahtar dağıtımına "kuantum anahtar dağıtımı" denir.

Kuantum anahtar dağıtımı için kurulması planlanan deneysel düzenek Şekil 2'de gösterilmektedir. Işık kaynağı olarak, kuantum fiziksel rastgele sayı üreteci uygulamasında da kullanılması öngörülen, 40-50 MHz'lik oranlarda 1 nanosaniyeden düşük zaman uzunluğuna sahip darbeler üretebilen bir lazer kullanılır. Darbeli lazerin gücü düşürülerek darbe başına ortalama olarak çok düşük sayıda (<~ 0.05) foton üretilen limite ulaşılır. Lazerden çıkan fotonlar hızlı bir elektro-optik modülatör kullanılarak doğrusal ya da çembersel tabanda polarizasyonlara kodlanır. Bob tarafında fotonlar bir yarı geçirgen ayna, polarize yarı geçirgen aynalar ve bir λ /4 plakası yardımı ile dik ya da çembersel tabanda algılanır.



Kuantum anahtar dağıtımı için kullanılması öngörülen deneysel düzenek. A, lazer güç düşürücü filtreler; YGA, Yarı geçirgen ayna; P-YGA, Polarize yarı geçirgen ayna; EOM, Elektro-optik modülatör; S1, S2, S3, S4, tek foton sayaçları; FC, fiber uyarıcı

ulusal ya da ticari Ar-Ge kuruluşları bünyesinde oluşmuştur. Nihai proje ancak bu merkezler arasındaki ortak çalışmaların yaratacağı sinerji ile başarıya ulaşmaktadır. Örneğin askeri amaçlı kuantum teknolojileri ulusal merkezlerin ve üniversite merkezlerinin ortak çalışması ile gerçekleştirilirken, bankalar için yapılan bir projede şirketler ve üniversiteler beraber çalışmıştır. Başarılı bir örnek olarak Toshiba ve Fujitsu gibi şirketlerin kuantum teknoloji merkezlerinin, Tokyo Üniversitesi kuantum bilişim gruplarıyla ortak çalışmaları verilebilir. IBM, NEC, Fujitsu, Toshiba gibi birçok şirketin yanı sıra hükümetler de özellikle kuantum bilgi teknolojileri konusuna öncelik vermektedir. Bu nedenle rekabet halindeki şirketler bile ortak merkezler kurmuştur. Mitsubishi ile NEC, Tokyo Üniversitesi ile ortak bir merkez kurmuştur. Avrupa Birliği, Amerika'nın elindeki Echolon sistemi sebebiyle endişe duymakta ve buna cevaben kuantum teknolojilerini kullanmak niyetini dile getirmektedir. Bu sebeple, çerçeve programları gibi destek programlarında kuantum haberleşme öncelikli konulardandır. Japonya ve Çin bilim bakanlıkları da kuantum teknolojilerini öncelikli alanları arasına almıştır. Çin 2007 de ilk başarılı kuantum iletişim ağını Pekin-Tianjin arasında operasyonel hale getirdiğini açıklamış ve Çin Network Şirketi bünyesinde ticari kılındığını duyurmuştur. Amerika da bu rekabet karşısında DARPA önderliğinde kuantum teknolojilerine ayırdığı kaynakları artırmıştır. BBN şirketine sadece 2008 yılında 3,5 milyon dolar yardım yapılmıştır. Bu şirket, hükümetten aldığı toplam 15 milyon dolar destekle üniversiteler ve ulusal araştırma merkezleri ile beraber kuantum kriptoloji ve kuantum haberleşme konularında yoğun faaliyet göstermektedir. Amerikan Ulusal Ölçüm Merkezi (NIST) gibi kuruluşlar da uzun mesafeli kuantum haberleşme ağlarına yönelmiştir.

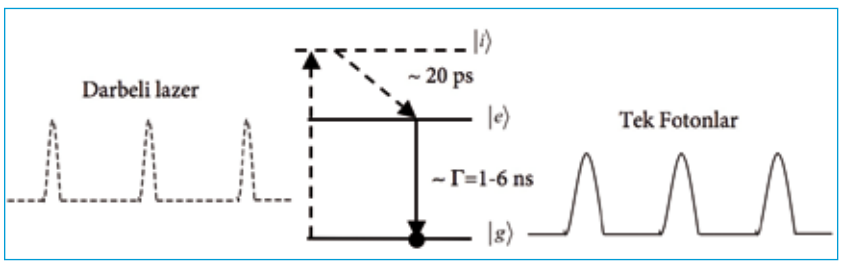
Türkiye'nin ilk "state-of-the-art" (günün gereklerine uygun) kuantum teknolojileri araştırma laboratuvarlarından biri, bu sene başında Devlet Planlama Teşkilatı'nca 3 yıl desteklenmesi kabul edilen bir altyapı projesiyle Koç Üniversitesi'nde kurulacaktır. Projede görev alan Prof. Dr. Tekin Dereli, Doç. Dr. Özgür Müstecaplıoğlu ve Doç. Dr. Alper Kiraz kuantum fiziğinde uzman, ülkemizde ve yurt dışında tanınan öğretim üyeleridir. Yüksek lisans öğrencileri Yasin Karadağ, Ramazan Uzel ve Utkan Güngördü proje çalışmaları kapsamında tezlerini hazırlamaktadır. Bu laboratuvarda ve buna paralel olarak TÜBİTAK UEKAE bünyesinde kurulmakta olan Kuantum Teknolojileri Araştırma Laboratuvarları'nda yapılacak ortak çalışmalar ile ülkemizin ilk kuantum kriptografi sistemi geliştirilecek ve kuantum bilişim konusunda ülkemizde gelecekte yapılacak çalışmalara öncülük edecek bilgi birikimi, altyapı ve sinerji oluşturulmuş olacaktır.

Günümüzde kuantum kriptografi ağırlıklı kripto anahtar dağıtım sistemleri iki ortamda gerçeklenmektedir: Fiber op-

Tek Foton Kaynağı Gösterimi

Tetiklemeli tek foton kaynakları ideal olarak bir tetikleme sonucu bir ve yalnız bir foton yayan aygıtlardır. Pratikte foton toplama verimliliğinden kaynaklanan sınırlamalar ile her tetikleme sonucu yayılan foton toplanamasa da, bu aygıtlar ile her tetikleme sonucu bir ya da 0 foton yayılımı sağlanabilmektedir. Tetiklemeli tek foton kaynakları, iki seviyeli sistemin darbeli lazer ile uyarılmasıyla elde edilir. Şekil 3'te gösterildiği gibi bu uyarım yönteminde lazerin dalgaboyunu, yayılan tek fotonların dalgaboyundan farklı tutmak için üçüncü bir enerji seviyesi sıkça kullanılır. Darbeli lazerin her bir darbesi, iki seviyeli sistemin bir defa uyarılmış (|i>) seviyeye geçişine neden olur. Bu sistem daha sonra |e> seviyesine hızlı bir şekilde geçer ve |e> ile |g> seviyeleri arasındaki geçişte kendiliğinden ışıma ile tek bir foton yayar. Bu şekilde, her bir darbenin tek bir foton ışımasını tetiklemesi sağlanabilir. Her bir darbenin tek bir foton ışımasını tetiklemesi için, darbe zaman aralığının kendiliğinden (spontane) ışıma zamanından yeterince küçük olması ve darbe enerjisinin de iki seviyeli sistemi, uyarılmış enerji seviyesi olan |i>'ye çıkaracak kadar yüksek olması gerekir. Bu tür deneysel gösterimlerde şu ana kadar iki seviyeli sistem olarak tek boya molekülleri, tek InAs kuantum noktaları, tek CdSe kuantum noktaları, tek atomlar, elmas içindeki N (azot) - boşluk merkezleri veya tek karbon nanotüpleri kullanılarak, oda sıcaklığında veya sıvı Helyum sıcaklıklarında gösterimler gerçekleştirilmiştir. Proje kapsamında, uygun bir iki seviyeli sistem seçilerek tetiklemeli tek foton kaynağı gösterimi gerçekleştirilecektir.

Kullanılacak deney düzeneği Şekil 4'te gösterilmektedir. Bu düzenekte düşük yoğunlukta iki seviyeli sistemler içeren örnek, sıvı Helyum soğutucusunda (cryostat) korunur. Darbeli lazer ile örnek üzerinde optik çözünürlükle belirli bir alan (~1 mm^2) uyarılır. Bu alanda bulunan tek bir iki seviyeli sistem uyarılır ve toplanan ışıma çizgisi bir bant geçiren girişim filtresi kullanılarak Hanbury Brown ve Twiss deney düzeneğine gönderilir. Bu düzenekte rastgele algılama elektronik aygıtları kullanılarak ışımanın ikinci derece faz uyumu fonksiyonu ölçülür. İkinci derece faz uyumu fonksiyonunun ölçülmesi ile tetiklemeli tek foton ışıması gösterimi gerçekleştirilir.



Tetiklemeli tek foton kaynağının çalışma prensibi.

tik hat üzerinden haberleşen sistemler ve havadan (*free space*) haberleşen sistemler. Her iki sistem için de şimdiye kadar uygulanmış veya uygulanması planlanan dört farklı yaklaşım vardır: 1) Zayıflatılmış lazer kaynakları kullanan sistemler: Bu yaklaşımda lazerler tarafından üretilen zayıflatılmış ışık darbeleri fiber veya hava yoluyla karşı tarafa iletilir. Fiber üzerinden zayıflatılmış lazer kaynakları kullanan sistemler, tek mod fiber üzerinden çalışırlar ve 1330 nm veya 1550 nm dalgaboyu civarında çalışırlar. Hava üzerinden zayıflatılmış lazer kaynakları kullanan sistemler ise atmosferik optik haberleşme sistemlerinden yararlanır. 2) Tek foton kaynağı kullanan sistemler, her seferinde tek foton ürettikleri için bilgi sızıntısı ihtimalini ortadan kaldırır. 3) Dolaşık (*entangled*) foton kaynağı kullanan sistemlerde ise iki kuantum sistemi arasındaki yerel olmayan (*non-local*) kuantum mekaniksel etkilerden yararlanılır. Bu yerel olmayan etkiler, anahtar değişimi için kullanılabilmektedir. 4) Sürekli değişken (*continuous variable*) kullanan sistemlerde anahtar, kuvvetli optik darbelerin fazlarındaki, genliklerindeki veya kutuplanmalarındaki küçük sapmalarla kodlanır. Bu kodlama ikili veya sürekli ta-

Zafer Gedik

Mühendislik ve Doğa Bilimleri Fakültesi, Sabancı Üniversitesi

Kuantum Bilgisayarları

Tek bir bilgisayar yerine her biri farklı bir evrende, aynı anda çalışan birçok bilgisayar kullanarak işlemleri çok daha hızlı yapabilir miyiz? Dünyadaki tüm bilgisayarları kullansak bile, evrenin yaşından daha fazla zaman gerektirecek hesaplamaları kısa sürede tamamlayabilir miyiz? Kuantum bilgisayarları sayesinde her iki soruya da olumlu cevap verebiliriz. Üstelik bu aygıtların ilkel örneklerine bakılırsa kuantum bilgisayarlarının kullanıma girmeleri çok uzak görünmüyor.

Kuantum bilgisayarlarının klasik bilgisayarlarla çözülemeyen hangi problemleri verimli bir şekilde çözebilecekleri tümüyle anlaşılmış olmasa da kesin olarak bildiğimiz, sadece onlara has bir üstünlüklerinin olduğudur: Rastgele sayılar üretmek. Belirlenimci yapıları nedeniyle klasik bilgisayarlarla elde edilen sayılar hiçbir zaman tam rastgele sayılar olamamaktadır. Kuantum mekaniğinin temel ilkeleri arasında yer alan rastgelelik, aynı özelliğe sahip sayılar elde etmek için doğal bir kaynak oluşturur.

Kuantum bilgisayarını klasik bir bilgisayardan ayıran nedir? Doyurucu olmasa da kısa bir cevap şöyle verilebilir: Aygıt, klasik fizik yerine kuantum fiziğinin ilkelerine göre çalışmaktadır. Bilgisayarları bizim seçtiğimiz bir ilk halden başlayıp son hale giden birer makine olarak düşünebiliriz. Son hal aslında istediğimiz cevabı ya da bilgiyi taşıyan bir durumdur. İşte bu iki hal arasında sistemin nasıl devineceği birtakım fizik kurallarınca belirlenir. Örneğin mevcut birçok bilgisayarda olduğu gibi klasik elektronik devre denklemleri bu kuralları belirleyebilir. Sadece giriş ve çıkışlara bakarsak, hepsinde ikilik tabanın elemanları olan 0 ve 1'lerden başka bir şey görmeyeceğimiz için farkı anlayamayabiliriz. Fark, bilgisayarda çalıştırabileceğimiz algoritmalarda görülebilir. Ayrıca kuantum algoritmaları çoğu kez bir başarı olasılığıyla birlikte verilirler, yani bilgisayarın istediğimiz cevabı bulamama olasılığı da vardır. Bu durumda başa dönüp tekrar hesap yapmamız gerekir.

Kuantum mekaniğinin bilim felsefesine getirdiği yeniliklerden biri de gözlemcinin ya da yapılan gözlemin yorumlanmasının tartışmaya açık olmasıdır. Çok sayıda evren ya da paralel evrenler modeli konuyla ilgili fikirlerden biridir. Kuantum bilgisayarları için paralel evrenler fikrini her tür bilgiyi yazmada kullanabileceğimiz 0 ve 1'lerle açıklayabiliriz. Klasik bilgisayarlarda 0 ve 1 değerlerini bit adını verdiğimiz birimlere kaydederiz. Kuantum bilgisayarındaysa kuantum bitleri ya da kısaca kubitler bulunmaktadır. Giriş ve çıkışta sadece 0 ve 1'leri görsek de kuantum bilgisayarının ara hallerini betimlerken kubitlerin hem 0 hem de 1 oldukları haller de varmış gibi görünür. Kuantum bilgisayarlarını klasik bilgisayarlardan ayıran belki de en önemli özellik işte bu üst üste binme (0 ve 1'in üst üste binmesi) halleridir. "Olur mu öyle şey? Ya 0 ya 1'dir!" diye ısrar eder ve değerinin ne olduğunu gözlemeye kalkarsak bu ara hallerde, başlangıç şartları aynı olmasına rağmen, bazen 0 bazen 1 görürüz. Kopenhag yorumlaması adı verilen yaklaşımda deneyin her tekrarında sadece olasılıkların bilinebileceği düşünülür. Paralel evrenler yorumlaması ise bu olasılık tabanlı, bir anlamda her şeyin rastgelelik üzerine kurulduğu yaklaşım yerine 0 ve 1'in ikisinin de ama farklı evrenlerde gözlendiği fikri üzerine inşa edilmiştir.

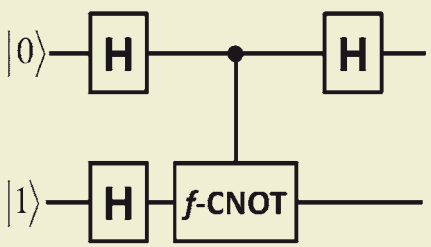
Üst üste binme hallerini matematiksel olarak $p|0\rangle+q|1\rangle$ şeklinde gösteriyoruz. Kubitlerin $|0\rangle$ ya da $|1\rangle$ şeklinde yazılması kuantum mekaniğinde Dirac tarafından geliştirilmiş bir gösterim şeklidir. Bu kubit değeri neymiş diye bakmaya kalkarsak p^2 olasılıkla 0, q^2 olasılıkla 1 görürüz. Buradan, $p^2+q^2=1$ olması gerektiğini tahmin etmek zor değildir. Aslında p ve q karmaşık (kompleks) sayılar da olabilir ama biz şimdilik kendimizi gerçek sayılarla sınırlayalım. Hatta $p^2=q^2=1/2$ olduğu durumlar basit bir kuantum algoritmasını anlamamıza yeterli olacaktır. Giriş sadece 0 ya da 1 olabiliyorsa klasik bir kubit için mümkün olmayan, örneğin $|0\rangle+|1\rangle/\sqrt{2}$ ya da $|0\rangle-|1\rangle/\sqrt{2}$ gibi halleri nasıl elde edebiliriz? İşte kuantum mekaniksel davranış burada işin içine girer. Klasik bilgisayarlardaki gibi burada da kapılar (kubitlerin hallerini değiştiren birimler) inşa etmek mümkündür. Örneğin, ışık tanecikleri fotonlar için laboratuvarda gerçekleştirmesi çok kolay olan Hadamard kapısı bunlardan biridir. Hadamard kapısı girişine $|0\rangle$ uygulandığında $|0\rangle+|1\rangle/\sqrt{2}$, $|1\rangle$ uygulandığındaysa $|0\rangle-|1\rangle/\sqrt{2}$ verir. Kapıları kontrollü olarak uygulamak da mümkündür. Örneğin, bir kubit değil işlemini (0'ı 1, 1'i 0 yapma) başka bir kubitin "0 duru-

banlardan birinde olabilir. Proje çalışmalarının başlangıç aşamasında, tek-modlu optik fiber üzerinden zayıflatılmış lazer kaynakları kullanan bir sistem geliştirilecektir.

Eğer Koç Üniversitesi ve UEKAE birlikte yukarıda bahsi geçen kuantum kriptoloji altyapısını ve teknik gelişimini sağlayabilirlerse, ülkemiz gelişmelerden geri kalmayarak bu sahada da söz sahibi olacaktır. Kurulacak bu laboratuvarlar ile, ideal güvenilirlikte haberleşme hatları ve mevcut klasik bilgisayarlardan çok daha hızlı çalışabilen bilgisayarlar vaad eden bu önemli alanda Türkiye'de ilk defa rekabetçi bir güç oluşturulması hedeflenmektedir. Bu altyapı sayesinde RSA (Rivest, Shamir, Adleman) kripto-sistemi gibi birçok algoritmaya karşı ve halihazırda ülkemizde kullanılan E-imza, internet bankacılık, internet alışverişi gibi sistemlere yönelik olası tehdit oluşturan kuantum hesaplamalara dayanıklı, yeni algoritmaların tasarlanması imkânı doğacaktır. Kuantum kriptografi sahasında kazanılan bilgi birikiminin kuantum hesaplama alanına doğru gelişmesine olanak sağlanacak, böylece birçok yeni uygulama için de bilgi birikiminin yolu açılmış olacaktır.

munda uygula, 1 olması durumunda uygulama," demek mümkündür. Önemi ve yaygınlığı nedeniyle bu işleme bir isim verme gereği görülmüş, kontrollü değilleme adı verilmiştir. Hadamard kapısını kısaca H, kontrollü değilleme kapısını da kısaca CNOT ile göstereceğiz. İşi biraz daha karıştırıp f - CNOT kapısını tanımlayabiliriz ki, $|x\rangle|y\rangle \overset{f\text{-CNOT}}{\rightarrow} |x\rangle|y\rangle \oplus f(x)\rangle$ şeklinde tanımlanan bu kapı $f(x)= x$ durumunda CNOT'a indirgenir. Burada $\oplus$ işlemi modüler toplamı göstermektedir (mod 2). Yani $0 \oplus 1 = 1 \oplus 0 = 1$ ve $0 \oplus 0 = 1 \oplus 1 = 0$'dır.

Kuantum algoritmaları bir problemi nasıl hızlı çözebilmektedirler? Basit bir benzetme yaparsak, örneğin, iki çubuğun boylarını karşılaştırıp hangisinin daha uzun olduğunu anlamaya çalıştığımızı düşünelim. Bir yöntem, iki çubuğun da boylarını ölçüp sonuçları karşılaştırmaktır. Diğer bir yöntemse iki çubuğu yan yana koyup doğrudan hangisinin daha uzun olduğunu görmektir. Klasik bilgisayarın ilkini, kuantum bilgisayarının da ikincisini yaptığını düşünebiliriz. Bu benzetmeyi daha açık bir hale getirmek için ilk kuantum algoritmamız olan Deutsch algoritmasından bahsetmek yerinde olacaktır. H ve CNOT kapıları bu algoritmayı uygulamak için yeterlidir. Amacımız bir fonksiyonun 0 ve 1 için değerlerinin aynı olup olmadığını anlamak olsun. Yani $f(0) = f(1)$ mi yoksa $f(0) \neq f(1)$ mi? Tıpkı çubuk boylarını karşılaştırma probleminde olduğu gibi $f(0)$ ve $f(1)$'i hesaplayarak, yani iki işlem yaparak bu soruya cevap verebiliriz. Ancak bunu kuantum bilgisayarı, daha doğrusu basit bir kuantum işlemcisi kullanarak tek hesapla yapmak mümkündür. Yani f fonksiyonunu yalnız bir kez hesaplayarak 0 ve 1'de aynı değeri alıp almadığını tespit edebiliriz. Bunun için gereken, aşağıdaki kuantum devresi'dir.



Kuantum işlemcisi Deutsch algoritması yardımıyla fonksiyonu yalnız bir kez hesaplayarak 0 ve 1'deki değerlerinin aynı olup olmadığını belirleyebilir.

Yukarıdaki kubitin en son değerinin $f(0) = f(1)$ durumunda hep $|0\rangle$, $f(0) \neq f(1)$ durumundaysa hep $|1\rangle$ olduğunu görmek basit bir hesapla mümkündür. Burada asıl önemli olan f – CNOT kapısının yalnız bir kez uygulanmasının, bir başka deyişle fonksiyonun yalnız bir kez hesaplanmasının yeterli olmasıdır. David Deutsch bunu paralel evrenler fikrinin doğrudan bir kanıtı olarak değerlendirmektedir. Deutsch algoritması nükleer manyetik rezonans ve iyon kapanı yöntemiyle çalışan kuantum bilgisayarlarında başarıyla uygulanmıştır.

İki işlem yerine sadece bir işlemle aynı hesabı yapabilmek çok önemli bir fark değilmiş gibi görünebilir ama kimi kuantum algoritmaları için bundan çok daha fazla hızlanma söz konusudur. Mesela kriptolojide yaygın olarak kullanılan sayıların asal çarpanlara ayrılmaları problemini, asırlardır süren çabalarla verimli bir klasik algoritma bulunamamasına rağmen, kuantum algoritmalarıyla hızlı bir şekilde çözmek mümkündür. Bir başka deyişle yeterince büyük bir kuantum bilgisayarıyla çarpanlara ayırma esasına dayalı tüm bilgi koruma engellerini aşmak mümkündür. Peter Shor'un 1994'te ortaya attığı ve daha sonra çeşitli şekillerde geliştirilen algoritma bu yüzden çok önemlidir.

İki seviyeli tüm kuantum sistemleri kubit olarak kullanılmaya adaydır. Ancak mesele sadece kubit yapmak değil çok sayıda kubiti, anlamlı işler yapabilecek bir bilgisayar için belki bin ya da daha fazlasını, bir araya getirmek, daha da önemlisi kubitleri istediğimiz hallerde hazırlayıp istediğimiz işlemleri uygulayabilmektir. İşte bunların hepsini yapabildiğimiz sistemler henüz çok sınırlıdır. Mevcut bilgisayarlarda kubit sayısı aşağı yukarı on civarındadır. Örneğin, 7 kubitli bir bilgisayarla Shor algoritmasını kullanarak 15'in 3 ve 5'in çarpımı olduğunu gösterebiliyoruz.

Kuantum bilgisayarlarının daha büyük ölçekte yapılmalarının önündeki en önemli engellerden biri bilgisayarın çevreyle etkileşim sonucu kuantum özelliklerini kaybetmesidir. Örneğin, 0 ve 1'in karışımı bir haldeki kubit, henüz hesaplamalar bitmeden indirgenir ve böylece üst üste binme özelliğini kaybederse bilgisayar istenilen işi başaramayacaktır. Bu yüzden bilgisayarların çevreden yalıtımlarına büyük özen gösterilmektedir.

Kriptoloji uygulamaları açısından önemli bir kuramsal soru, kuantum bilgisayarlarıyla bile çözülemeyen problemlerin hangileri olduğudur. Bu problemlerin saptanmasıyla kuantum algoritmalarının tehdit oluşturmadığı güvenli şifreleme yöntemleri geliştirmek mümkün olacaktır.