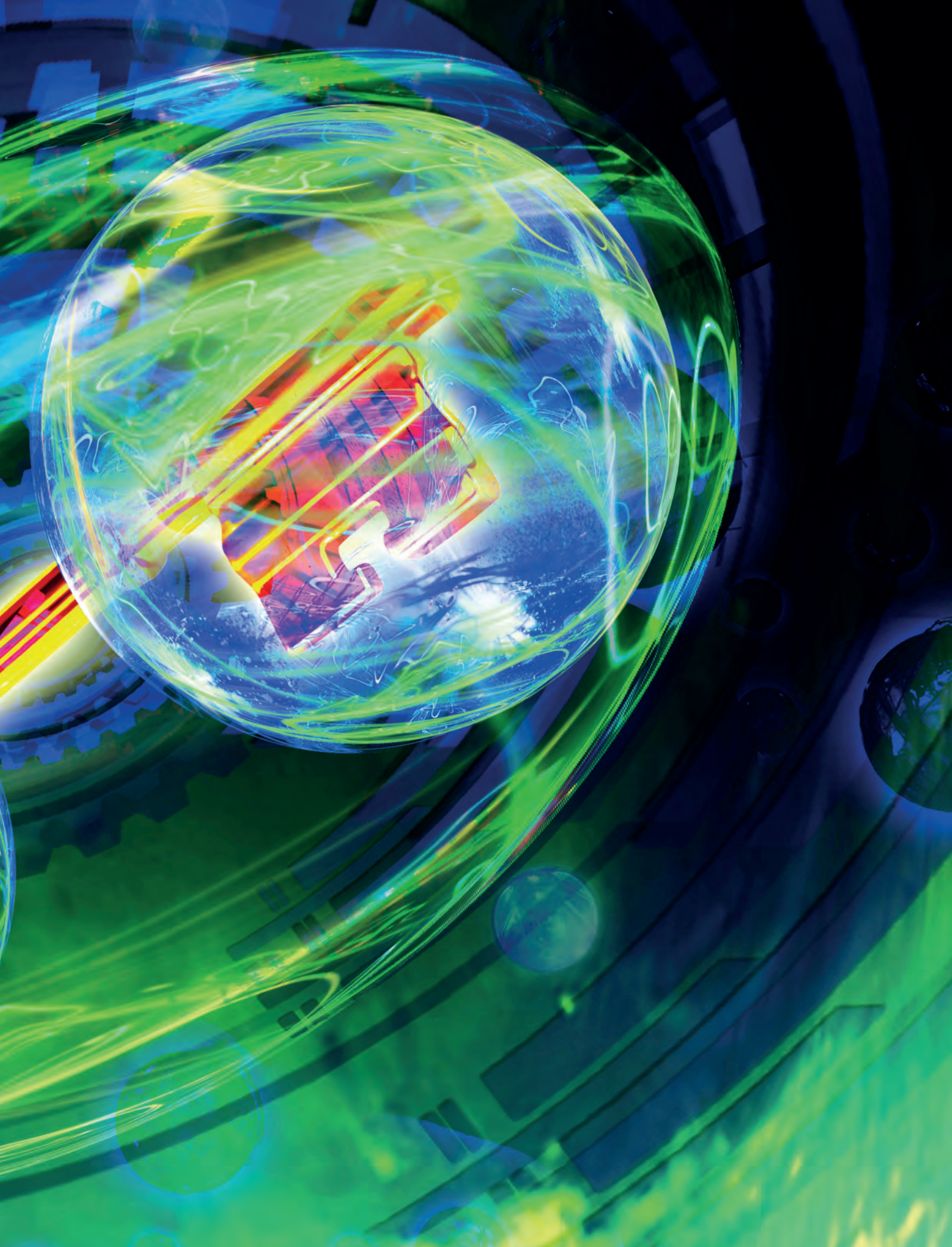
Kuantum Bilgisayarlar Çağında Kriptografi

Dr. Mahir E. Ocak [*TÜBİTAK Bilim ve Teknik Dergisi*

Siber güvenliği bekleyen çok önemli bir tehlike var: kuantum bilgisayarlar. Bugün internet üzerinden aktarılan bilgileri şifrelemek için kullanılan yöntemlerin bazıları kuantum bilgisayarlar karşısında tamamen savunmasız kalacak. Dolayısıyla kuantum bilgisayarlar çağında siber güvenliğin nasıl sağlanacağının şimdiden düşünülmesi gerekiyor. Araştırmacılar bunun için çalışmalara başladı bile



Günümüzde Kriptografi

Günümüzde internet üzerinden aktarılan verileri şifrelemek için kullanılan kriptografi yöntemleri iki ana grupta sınıflandırılır: simetrik ve asimetrik yöntemler.

Simetrik algoritmaların temel özelliği hem şifreleme hem de şifreyi çözmek için aynı "anahtarın" kullanılmasıdır. Gönderici, alıcı tarafından da bilinen bir anahtarı kullanarak aktarılacak metni şifrelendirir, alıcı da yine aynı anahtarı kullanarak şifreli metni çözer. Eğer kullanılan anahtar göndericiden ve alıcıdan başkası tarafından bilinmiyorsa ve bir anahtar sadece bir aktarım için kullanılıyorsa bu yöntem tamamen güvenlidir. Bilginin aktarıldığı hatta sızan bir dinleyici, şifreli metni ele geçirse bile, hangi anahtarın kullanıldığını bilmediği için metni çözemez. Ayrıca her bir aktarım için farklı anahtarlar kullanıldığından çeşitli şifreli metinleri karşılaştırarak anahtarın ne olduğunu bulmasının bir yolu da yoktur.

Simetrik kriptografi ile ilgili temel sorun anahtarın nasıl belirleneceğidir. Örneğin, internet bankacılığı üzerinden işlem yapmak istediğinizi düşünün. Her seferinde en yakınınızdaki şubeye bir koşu gidip güvenilir bir görevliye verileri hangi anahtarla şifrelendirip göndereceğinizi söyleyemeyeceğiniz açıktır. Şifreleme için kullanılacak tek kullanımlık anahtarın da internet üzerinden belirlenmesi gerekir. Peki ama nasıl? Yetkisiz kişilerin eline geçmesi ihtimaline karşılık anahtarın da şifrelenerek gönderilmesi gerekir. Öyleyse anahtarı şifrelemek için kullanılacak anahtar nasıl belirlenecek? Asimetrik kriptografi bu soruna çare bulmak için geliştirilmiştir.

Asimetrik sistemlerde bir değil iki anahtar vardır. Bu anahtarların biri açık anahtar, diğeri gizli anahtar olarak adlandırılır. Alıcı, kendisine mesaj göndermek isteyen birisine şifreleme için kullanmasını istediği açık anahtarı "alenen" söyler. Kendisine gönderilen, açık anahtarla şifrelenmiş mesajları ise hiç kimseye söylemediği gizli anahtarı kullanarak çözer.

Asimetrik sistemlerde açık anahtarlar herhangi bir şifreleme olmaksızın internet üzerinden aktarılır. Herhangi birisinin hatta sızıp açık anahtarı ve bu anahtar kullanılarak şifrelenmiş mesajları dinlemesinde de sakınca görülmez. Çünkü şifrelenmiş mesajları "kolayca" çözmek ancak gizli anahtarın bilinmesiyle mümkündür ve bu anahtarın ne olduğunu sadece alıcının kendisi bilir. İlke olarak şifreli mesajların çözülmesi mümkündür. Ancak gizli anahtar olmaksızın böyle bir şeyi başarmak çok uzun sürecektir. Bir dinleyici yıllarca uğraşıp şifreli metinleri çözmeyi başarsa bile eline geçen bilgilerin "zamanı geçmiş" olacaktır.

Asimetrik kriptografi sistemleri internet üzerinden aktarılan "tüm bilgilerin" şifrelemesi için kullanılmaz. Çünkü hem şifreleme hem de şifreyi çözme işlemleri zaman alır. Bu yüzden asimetrik sistemler, genellikle sadece simetrik bir şifreleme sistemindeki tek kullanımlık anahtarın belirlenmesi için kullanılır. Önce gönderici ve alıcı asimetrik şifreleme yöntemiyle iletişim kurup tek kullanımlık bir şifre belirlerler. Daha sonra bu anahtarı kullanarak aralarında bilgi aktarımı yaparlar. İleri bir tarihte aynı gönderici ve alıcı yeniden iletişim kurmak istediklerinde asimetrik şifreleme yöntemiyle yeni bir tek kullanımlık şifre belirlemeleri gerekir.

Kısacası, internet üzerinden aktarılan bilgilerin güvenliği asimetrik sistemlerle oluşturulmuş şifreli metinleri çözmenin "zorluğuna" dayanır. Ancak şifreli metinleri çözmek imkânsız değildir. Bu yüzden gelişen teknolojiyle birlikte şifreleri kırmak giderek kolaylaşıyor. Söz konusu sadece klasik bilgisayarlar olduğunda bu durumun çok da önemli olduğu söylenemez. Ancak günümüzde geliştirilme aşamasında olan kuantum bilgisayarlar arzu edilen kapasiteye ulaştığında her şey değişecek!

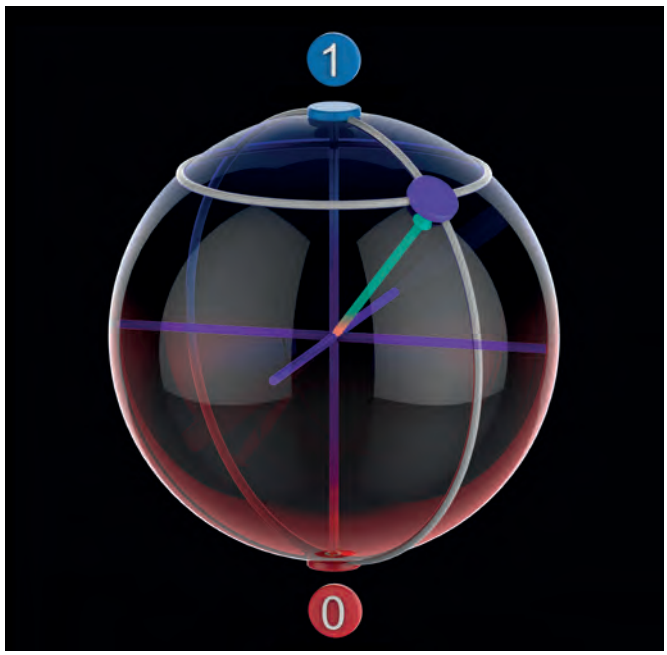
Çok sayıda kübit içeren bir kuantum bilgisayarın temsili gösterimi

Kuantum Bilgisayarlar

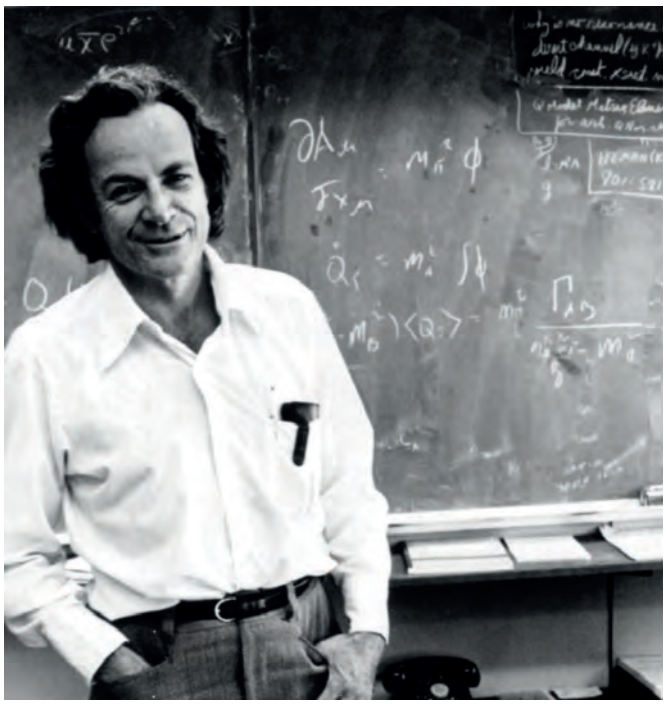
Kuantum bilgisayarları klasik bilgisayarlardan ayıran temel özellik bilginin depolandığı ve işlendiği birimlerdir. Klasik bilgisayarlardaki bitlerin aksine kuantum bilgisayarlardaki kübitler, sadece "0" ve "1" durumlarında değil, bu durumların bir süperpozisyonunda da bulunabilir. Kübitler üzerinde yapılan bir işlem her iki durumu da aynı anda etkiler. Bir kuantum bilgisayarı n tane kübite sahipse, bu kübitler, kuantum mekaniği ilkeleriyle uyumlu bir biçimde, 2^n farklı durumun süperpozisyonunda bulunabilir. Dolayısıyla n tane kübite sahip bir kuantum bilgisayarı, tek bir seferde 2^n tane işlemi paralel biçimde gerçekleştirebilir. Kuantum bilgisayarları klasik bilgisayarlar karşısında güçlü kılan işte bu özellikleridir.

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.

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



Bir kübitin durumunun temsili gösterimi. Kübitler, bitlerin aksine sadece 0 ve 1 durumlarında değil, bu durumların herhangi bir süperpozisyonunda da bulunabilir.



Richard Feynman

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. Peki, o gün geldiğinde siber güvenlik nasıl sağlanacak?

Kuantum Bilgisayarlarla Şifre Kırma

Kuantum algoritmalarla kolaylıkla çözülebilecek, modern kriptografiyle ilgili çeşitli problemler var. Bunların bazıları asimetrik, bazıları da simetrik algoritmalarla ilgili.

Asimetrik kriptografi Günümüzde kullanılan asimetrik kriptografi algoritmalarından biri 1977 yılında Ronald Rivest, Adi Shamir ve Leonard Adelman tarafından geliştirilmişti. Kısaca RSA olarak adlandırılan bu algoritma çiftasal (iki asal sayının çarpımı olarak ifade edilebilen) sayıları çarpanlarına ayırmanın zorluğuna dayanıyor. Örneğin 15

Shor Algoritması

Peter Shor 1994 yılında kuantum bilgisayarla çiftasal sayıların çarpanlarının hesaplanmasına imkân veren bir algoritma geliştirdi. Bu algoritma özetle şu şekilde işler:

1. Asal çarpanlarını bulmak istediğiniz n sayısından küçük bir x tam sayısı alın,
2. m bir tam sayı olmak üzere $x^p=m*n+1$ (ya da $x^p=1 \bmod n$) eşitliğini sağlayan p sayısını bir kuantum bilgisayarı yardımıyla bulun,
3. Bu eşitlik çözüldüğünde $(x^{p/2}-1)(x^{p/2}+1)=m*n$ olduğu görülür. Dolayısıyla $x^{p/2}-1$ ve $x^{p/2}+1$ sayıları n sayısıyla ortak çarpanlara sahip olabilir.

Bu algoritma her durumda n sayısının çarpanlarından birini vermez. Çünkü hesaplanan $x^{p/2}-1$ ve $x^{p/2}+1$ sayıları tam sayı olmayabilir ya da bu sayılardan biri aradığımız n sayısının tam katı olabilir. Böyle bir durumla karşılaşıldığında farklı bir x sayısı seçilerek hesap yeniden yapılır. Ta ki n sayısının çarpanlarından biri bulununcaya kadar.

Bu algoritmayı klasik bilgisayarlarla da uygulamak mümkündür. Örneğin 15 sayısının çarpanlarını bulmaya çalıştığımızı ve seçtiğimiz rastgele x sayısının 2 olduğunu düşünelim. p sayısını bulmak için x=2'nin tam kuvvetlerini birinci kuvvetinden başlayarak sırayla hesaplar ve $x^p= m*n +k$ biçiminde yazarız:

$2^1=0*15+2 \Rightarrow 2^1=2 \bmod 15$,
$2^2=0*15+4 \Rightarrow 2^2=4 \bmod 15$,
$2^3=0*15+8 \Rightarrow 2^3=8 \bmod 15$,
$2^4=1*15+1 \Rightarrow 2^4=1 \bmod 15$.

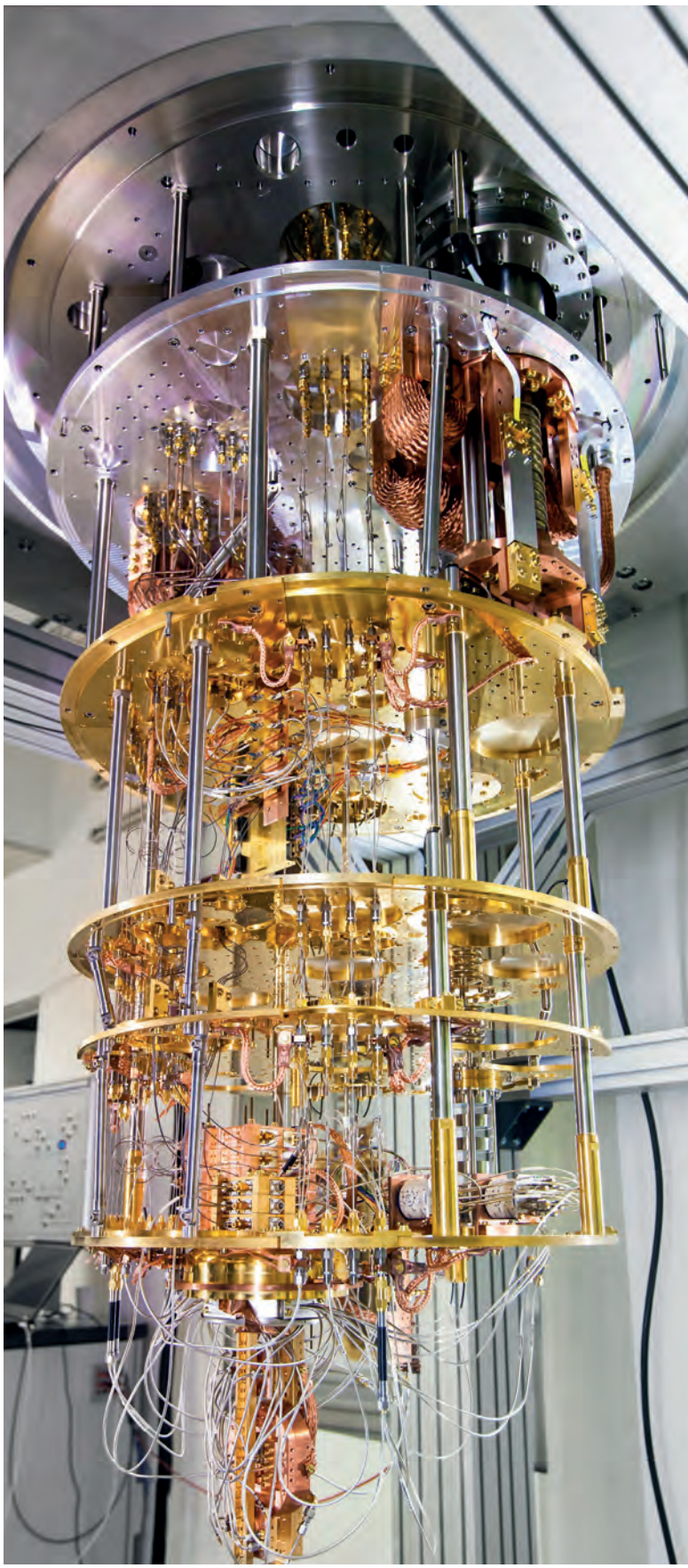
Görüldüğü gibi dört sayısına geldiğimizde aradığımız p sayısını buluruz. Dolayısıyla 15 sayısının muhtemel çarpanlarını $2^{4/2}-1=3$ ve $2^{4/2}+1=5$ olarak hesaplarız, ki her iki sayı da doğrudur.

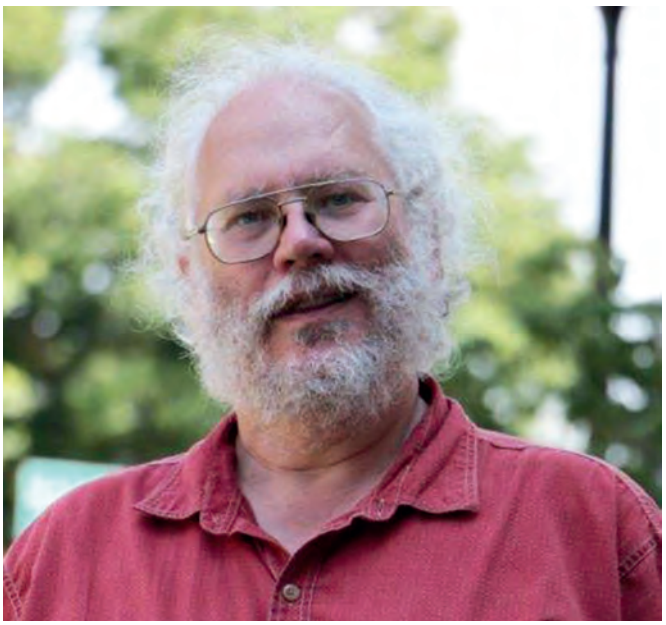
Bu algoritmayı klasik bilgisayarla uygulamaktaki ana sorun p sayısını bulmanın çok uzun zaman almasıdır. Özellikle de çarpanlarına ayrılacak sayı çok büyük olduğunda. Bu algoritmayı kullanmak yerine kabaca 1'den başlayıp tüm sayma sayılarını tek tek denemek bile daha kısa sürer.

Kuantum bilgisayarlarının sağladığı avantaj, süperpozisyon durumları üzerinde yapılan işlemlerle tek bir seferde olmasa bile sadece birkaç denemede p sayısını bulmaya imkân vermeleri. Bunun nasıl gerçekleştiğini anlamak için önce modüler aritmetikle ilgili bir bilgiye daha ihtiyacımız var: Eğer $x^p=1 \bmod n$ ve $x^q=k \bmod n$ ise $x^{p+q}=k \bmod n$'dir. Dolayısıyla p sayısını bulmanın bir başka yolu x sayısının kuvvetlerinin mod n'deki değerlerinde herhangi bir k sayısının hangi sıklıkla ortaya çıktığını tespit etmektir. Örneğin, yukarıda 15 sayısını çarpanlarına ayırmak için verilen örneği tekrar ele alalım. İki sayısının kuvvetlerinin mod 15'teki değerlerini 1'den başlayarak tek tek hesapladığımızda aynı sonuçların her dört seferde bir tekrar ettiğini görürüz. Örneğin 2^2, 2^6, 2^{10} sayılarının tamamı mod 15'te 4'e eşittir. Benzer biçimde 2^3, 2^7, 2^{11} sayılarının tamamı da mod 15'te 8'e eşittir. Aynı sonuçların tekrar etme sıklığı dört olduğu için bulmaya çalıştığımız p sayısının 4 olduğu çıkarımını yaparız.

Bir kuantum bilgisayarıyla aynı sonuçların hangi sıklıkla tekrar ettiğini bulmak için önce kübitlerin durumu muhtemel tüm kuvvet değerlerinin (q) bir süperpozisyonuna getirilir. Daha sonra $x^q=k \bmod n$ hesabı yapılır. İşlemden sonra kübitler muhtemel tüm sonuçların (k) bir süperpozisyonunda olacaktır. Son olarak aynı sonuçların hangi sıklıkla ortaya çıktığını tespit etmek için kübitlere "Fourier dönüşümü" denilen bir işlem uygulanır ve üzerlerinde ölçüm yapılır. Eğer işlemlerde kullanılan x değeri arzu edilen sonucu vermezse, başka bir x değeriyle hesaplar tekrar edilir. Böylece tek bir seferde olmasa bile sadece birkaç denemede p sayısını tespit etmek mümkün olur.

Kısacası kuantum bilgisayarların bu problemi kolayca çözebilmesinin nedeni, klasik bilgisayarların aksine, x sayısının kuvvetlerini tek tek sırayla değil, hepsini birden tek seferde hesaplayabilmeleridir.





Peter Shor

ve 63 iki asal sayının çarpımı olarak yazılabilen sayılardandır. Bu sayıları sırasıyla 3*5 ve 7*9 olarak yazabiliriz. Söz konusu olan bu kadar küçük sayılar olduğunda asal çarpanları bulmak pek zor değildir. 1'den başlayarak tüm sayma sayılarını sırasıyla deneyerek çarpanları bulabilirsiniz. Ancak söz konusu olan yüzlerce basamaklı sayılar olduğunda bu kaba yöntem yararsızdır. En gelişmiş bilgisayarlarla bile yüzlerce basamaklı sayıları asal çarpanlarına ayırmak yıllar sürer. Cevabın kısa süre içinde bulunmasına imkân veren klasik bir algoritma da yoktur. Ancak Peter Shor tarafından 1994 yılında kuantum bilgisayarları için geliştirilmiş bir algoritma çiftasalları çok kısa sürede çarpanlarına ayırmaya imkân veriyor.

Modern kriptografiyle ilgili bir diğer matematik sorusu, kesikli logaritma problemi olarak adlandırılır. Bu problem matematiksel olarak şu şekilde ifade edilir: verilen q, x ve p sayıları için $q^r = x \bmod p$ eşitliğini sağlayan r tam sayısı nedir? Seçilen sayılar çok büyük olduğunda kesikli logaritma problemini çözmek çok zordur. Günümüzde kullanılan Diffie-Hellman ve Eliptik Eğri Kriptografisi gibi şifreleme yöntemleri de bu problemi çözmenin zorluğuna dayanır. Geçmişte yapılan çalışmalar, kesikli logaritma probleminin de kuantum bilgisayarlar tarafından kolayca çözülebileceğini gösterdi. Dolayısıyla Diffie-Hellman ve Eliptik Eğri Kriptografisi de kuantum bilgisayarlar karşısında tamamen savunmasız kalacak şifreleme yöntemleri arasında yer alıyor.

Kısacası modern asimetrik kriptografi belirli matematik problemlerini çözmenin zorluğuna dayanıyor. Ancak bu problemler gelecekte kuantum bilgisayarlar tarafından kolayca çözülebilecek.

Simetrik Kriptografi Bir hackerın simetrik kriptografi yöntemiyle şifrelenmiş bir mesajı çözmeye çalıştığını düşünelim. Anahtarın ne olduğunu bilmez. Anahtarı bulmak için tek tek muhtemel tüm şifreleri denemeye kalkabilir. Ancak bu "kaba kuvvet" yöntemiyle şifreli metni çözmesi çok uzun sürecektir. Üstelik anahtarın uzunluğu arttıkça klasik bir bilgisayarın muhtemel tüm anahtarları taraması için gereken süre de giderek artacaktır. Günümüzde simetrik bir şifreleme algoritmasının güvenli olarak kabul edilmesi için kullanılan anahtar uzunluğunun en azından 80 bit olması isteniyor.

Lov Grover 1996 yılında düzensiz veri tabanlarını taramak için kullanılabilecek bir algoritma geliştirdi. Kuantum bilgisayarlar için yazılmış bu algoritma ile N tane kayıt içeren bir veri tabanı $\sqrt{N}$ adımda taranabiliyor. Kaba kuvvetle anahtar bulmaya çalışmak da bir nevi veri tabanını taramak gibidir. Dolayısıyla Grover'in algoritması simetrik kriptografi ile şifrelenmiş metinleri çözmek için de kullanılabilir. Ancak Grover'in algoritmasının simetrik kriptografi açısından çok da büyük bir tehdit oluşturduğu söylenemez. Yapılması gereken sadece anahtar uzunluğunu biraz daha artırmaktır. Örneğin, bugün klasik bilgisayarlar karşısında 128 bitlik güvenlik sağlayan bir şifreleme yöntemi, kuantum bilgisayarlar karşısında ancak 64 bitlik güvenlik sağlayacaktır. Ancak anahtar uzunluğunu artırarak kuantum bilgisayarlar karşısında da arzu edilen herhangi bir güvenlik seviyesine ulaşmak mümkündür.

Kriptografinin Geleceği

Günümüzde internet üzerinden aktarılan bilgilerin güvenliğini sağlamak için doğrudan ya da dolaylı olarak asimetrik kriptografiden yararlanılıyor. Ancak kuantum bilgisayarlar pratik amaçlar için yararlı işlerin üstesinden gelebilecek kapasiteye ulaştıklarında, asimetrik sistemlerin güvenli olmasını sağlayan matematiksel problemleri çözmek kolaylaşacak ve böylece modern kriptografinin sonu gelmiş olacak. Dolayısıyla kuantum bilgisayarlar çağında kriptografinin yeni bir hâle bürünmesi gerekecek.

Bugün pek çok araştırmacı kuantum bilgisayarlar karşısında bile dirençli şifreleme sistemleri geliştirmek için çalışmalar yapıyor. Bu araştırmaları genel anlamda fiziksel ve matematiksel olarak ikiye ayırabiliriz.

Fiziksel araştırmalarda kuantum bilgisayarlarla baş edebilmek için kuantum mekaniği ilkelerinden yararlanılan kriptografi yöntemleri geliştirilmeye çalışılıyor. Bu yöntemlerin temel özelliği, şifreleme için kullanılacak anahtarın kuantum mekaniği ilkeleriyle uyumlu davranışlar gösteren sistemler kullanılarak belirlenmesidir. Kuantum mekaniksel sistemler üzerinde yapılan ölçümlerin sonuçlarının olasılığa dayalı olması, herhangi birisinin varlığını belli etmeden hatta sızmasını engeller. Çünkü anahtarın ne olduğunu tespit etmek için yapılacak ölçümler aktarılan verilerde bozulmaya sebep olacaktır. Bu düşünce her ne kadar ilke olarak kırılması tamamen imkânsız şifreli metinlerin oluşturulmasına olanak verse de pratikte uygulanması zordur. Bugün bu konu üzerine yapılan çalışmalarda da kuantum kriptografinin nasıl gerçeğe dönüştürülebileceği araştırılıyor.

Gelecekte internet üzerinden aktarılan bilgilerin güvenliğini sağlamanın bir başka yolu da kuantum bilgisayarlar tarafından bile çözülmesi çok zor matematik problemlerine dayalı yeni şifreleme yöntemleri geliştirmek. Bu amaçla yapılan çalışmaları çeşitli gruplar altında sınıflandırmak mümkün. Örneğin, bazı araştırmacılar, asal sayıların yerini matrislerin aldığı algoritmalar üzerine çalışmalar yapıyorlar. Bazı araştırmacılarsa çok değişkenli polinom sistemlerini çözmenin zorluğuna dayalı algoritmalara odaklanıyorlar.

2016 yılında ABD Ulusal Standartlar ve Teknolojiler Enstitüsü (NIST) Kasım 2017'ye kadar kuantum bilgisayarlara karşı dirençli olduğu düşünülen kriptografi algoritmaları teklif etmeleri için araştırmacılara çağrı yaptı. Ocak 2018'de NIST toplamda 82 algoritma önerisi yapıldığını açıkladı. Bu algoritmaların değerlendirilmesi ve gerçekten de kuantum bilgisayarlara karşı dirençli olup olmadıklarının belirlenmesi birkaç yıl sürecek. Önümüzdeki yıllarda henüz klasik bilgisayarlardan üstün kuantum bilgisayarlar geliştirilmeden bilgi alışverişinde kullanılan algoritmaların güncellenmesi sürpriz olmayacak.

Kaynaklar

Mavroeidis, Vasileios, ve ark., "The impact of quantum computing on present cryptography", *International Journal of Advanced Computer Science and Applications*, Cilt9, s. 405-414, 2018.