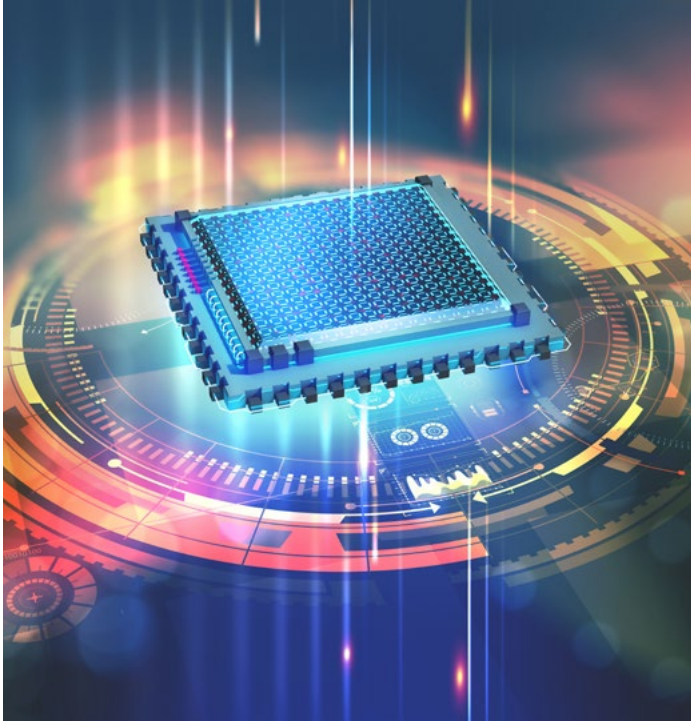
thinktech
STM Teknolojik Düşünce Merkezi

Matematiğin Zor Problemleri, Kriptoloji ve Kuantum Bilgisayarlara Etkisi



Buse TAŞCI

Matematiğin geçmişi M.Ö. 3000'lere, Mezopotamya ve Mısır uygarlıklarının Nil Nehri'nin taşmalarını ölçme ve hesaplamasına dayandırılmaktadır. O günden bugüne kadar geçen sürede matematiğin net bir tanımı hâlâ yapılamamaktadır. Öyle ki, kimileri onu bir sanat, dil, oyun ya da sadece bir araç olarak tanımlayabilmektedir[1]. Matematiğin öğretilen tanımı ise, "Biçimlerin, sayıların ve niceliklerin yapılarını, özelliklerini, aralarındaki bağıntıları tümdengelimli akıl yürütme yoluyla inceleyen ve aritmetik, geometri, cebir gibi dallara ayrılan" bir bilim dalı olmasıdır.

Bilgisayarların keşfi ise tamamen matematiğe dayanır. Bu konudaki ilk çalışmalar 9'uncu yüzyılda yaşamış olan büyük matematikçi El-Harizmi tarafından yapılmıştır. Bilgisayar bilimlerinin en temel kavramlarından biri olan "algoritma" kelimesi El-Harizmi'nin adından türetilmiştir (El Harizmi, Latin alfabesinde Alghorismus olarak okunmaktadır). İlk hesap makineleri, El-Harizmi'den yaklaşık 700 yıl sonra, veri giriş ve çıkışlarını dişli çarkların değişik pozisyonlar almasıyla gerçekleştiren denemelerle Pascal, Leibniz ve Babbage tarafından geliştirilmiştir. 1939 yılında, Atasanoff ve öğrencisi Berry tarafından, ilk elektronik bilgisayar olarak nitelendirebildiğimiz, "ABC" hayata geçirildi. 1960'larda, bu bilgisayarlar gelişerek insan beyninden çok daha hızlı ve hatasız çalışan hesap makineleri haline geldiler. Daha sonra bu gelişim devam ederek bilgisayarları genel amaçlı bir bilgi ve haberleşme aracı haline dönüştürdü, bilişim teknolojileri dediğimiz çok geniş bir teknoloji alanı oluştu ve bilgisayarlar hayatımızın bir parçası haline geldi.

Peki, matematik sadece bilgisayarların filizlenmesinde mi rol oynamıştır? Tabii ki hayır. Bilgisayar bilimleri genel olarak matematik biliminin bir alt kümesini oluşturmaktadır. Bilgisayarlar aslında sadece matematiksel hesaplamaları çok hızlı yapan makinelerdir. Tüm mühendislik süreçleri matematiğe ve onun getirdiği analitik düşünme, problem çözme tekniklerine dayanır. Ayrık matematik ve mantık; bilgisayar bilimi, yazılım mühendisliği ve bilgi sistemleri gibi bilgisayar disiplinlerinin temelini oluşturur. Ayrık matematiğin etkilediği bilgisayar disiplinlerini aşağıdaki gibi gruplandırabiliriz[2]:

- **Mantıksal Devre Tasarımı, İşletim Sistemleri:** Kümeler Teorisi, Bağıntılar ve Fonksiyonlar, Boole Cebri, Olasılık Teorisi
- **Veritabanı Tasarımı, Veri Yapıları ve Algoritmalar:** Kümeler Teorisi, Bağıntılar ve Fonksiyonlar, Boole Cebri, Ağaçlar, Sayılar Teorisi

1 Ülger, A. *Matematiğin Kısa Bir Tarihi*. URL: http://home.ku.edu.tr/~aulger/histofmathematics.html
2 Yenioğlu, Z. A. *Bilişim ve Mühendislik İçin Bir Gereklilik: Matematik*. URL: https://www.matematiksel.org/bilisim-muhendislik-icin-bir-gereklilik-matematik/

- **Bilgisayar Ağları:** Graf Teori, Sayılar Teorisi ve Ağaç Yapıları
- **Veri Madenciliği:** Sayılar Teorisi, Kümeler Teorisi, Olasılık Teorisi, Graf Teori ve Ağaç Yapıları
- **Makine Öğrenmesi ve Yapay Zekâ:** İstatistik, Olasılık Teorisi, Kalkülüs
- **Kriptoloji:** Sayılar Teorisi, Kümeler Teorisi, Boole Cebri

Kriptoloji, bu farklı disiplinlerin en önemlilerinden biri olup; bilgisayar mühendisliği ve elektrik-elektronik mühendisliği gibi farklı dalları bir araya getiren, temeli matematiksel zor problemlere dayanan, güvenli olmayan kanallar arasındaki iletişimi güvenli hale getirmeyi amaçlayan, bilgi güvenliğinin sağlanmasında ve siber güvenlikte büyük rol oynayan bir bilimdir. Matematiksel tekniklerin kullanımıyla; bilginin güvenli, orijinaline uygun halde saklanmasını ve aktarımını sağlar. Sistemler arası bağlantıların artması ve bu sistemlere erişimin kolaylaşması nedeniyle, bilginin maruz kalabileceği birçok saldırıya karşı korunması büyük önem taşımaktadır. Siber güvenliğin ana araçlarından biri olan kriptografi teknikleri ulusal güvenliğin sağlanması açısından da önemlidir.

Özellikle internetin bu kadar yaygınlaşmasından sonra kriptografinin günlük hayatta kullanımı oldukça arttı. İletişim güvenliği ve gizliliğini sağlamak amacıyla kullanılan çevrimiçi haberleşme, güvenli mesajlaşma, güvenli uzaktan erişim (VPN), elektronik imza uygulamaları ve elektronik sertifikalar en sık kullandığımız örneklerdir. Bunların yanı sıra kriptografik teknikler, günümüzde olgunlaşma aşamasında olan dijital paralar, blok zinciri uygulamaları gibi birçok yeni teknolojiye temel oluşturmaktadır.

Matematiğin Bazı Zor Problemleri

Günümüzde kullanılan birçok güvenlik algoritması matematiğin henüz çözülememiş, hesaplaması zor problemlerine dayanmakta ve sistemler aslında bu problemlere göre tasarlanmaktadır. Asimetrik kriptosistemler (açık anahtarlı kriptosistemler) matematiğin en zor problemlerinden olan asal çarpanlara ayırma problemi ve

ayrık logaritma problemini temel almaktadır. Günümüzde bu problemleri büyük sayılar için çözen bir teknoloji henüz kullanılmamaktadır.

1. Asal Çarpanlarına Ayırma Problemi

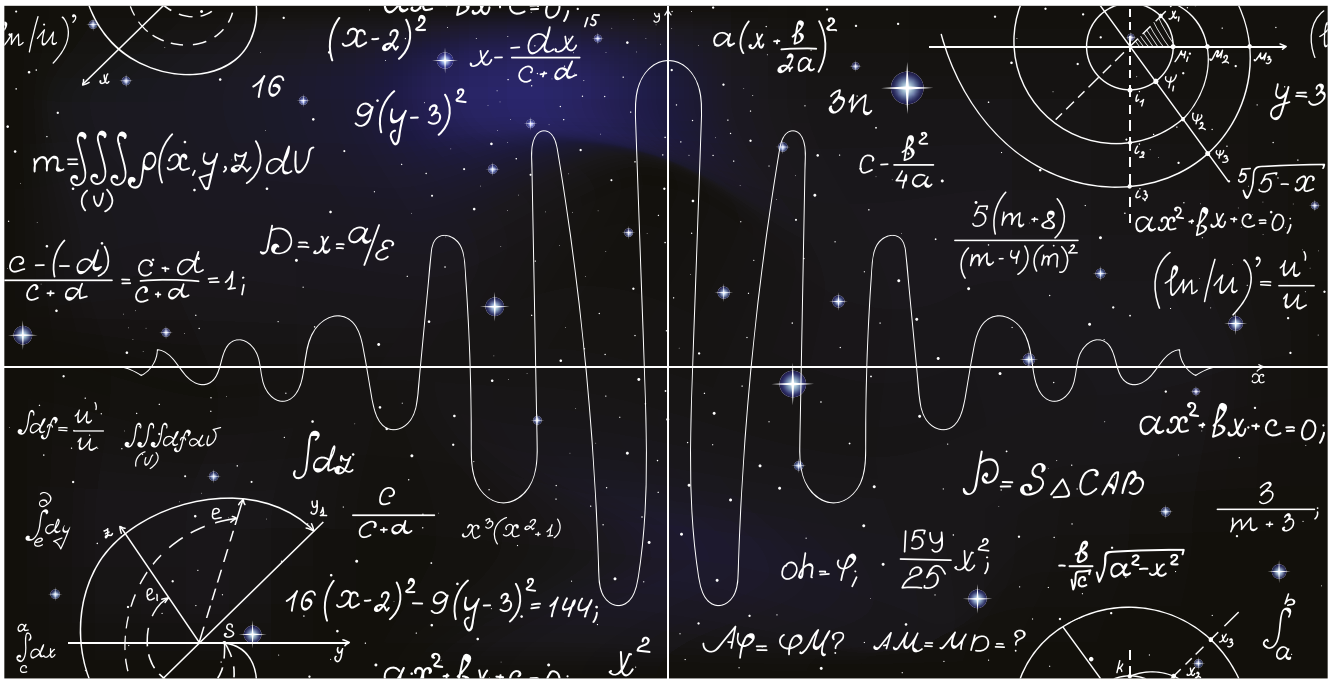
Asal sayılar, matematiğin gizemi hâlâ çözülemeyen alanlarından biridir. Birçok bilim insanı ve matematikçi asal sayılar üzerinde asırlardır çalışmış, çeşitli teoremler ortaya atmış fakat asal sayıların gizemini çözen, asal sayıları üretebilen bir formül/yöntem bulamamıştır. Aynı şekilde asal sayılar herhangi bir örüntüye de bağlı değildir.

Aslında, matematiğin temelinde de sayılar yerine asal sayılar vardır. Yani, asal olmayan her sayı aslında sadece asal sayılardan oluşmaktadır. Aritmetiğin temel teoremine göre, 1'den büyük olan her sayı, asal sayıların çarpımı olarak tek bir şekilde ifade edilebilir ($36=2^2*3^2$). Bir sayının asal olup olmadığı da çeşitli asallık testlerine (Fermat teoremi, Miller-Rabin vb.) göre belirlenmektedir.

Asal olmayan, 2'den büyük bir sayı için, sayıyı çarpanlara ayırmak kolay bir yöntemdir. Çok büyük sayılar için (1024 bit) bu işlem zorlaşmakla beraber, bilgisayarlar için bu, kolay bir işlemdir. Asal olmayan bir sayı kendinden daha küçük sayılara bölünerek çarpanlarına ayrılabilir. Asal sayıların kriptografide kullanılıyor olmasının temel sebebi de budur. Çok büyük iki asal sayı seçtiğimizi ve bunları çarptığımızı düşünelim. Bu çarpımı çarpanlarına ayırmak ne kadar mümkündür? İşte asal çarpanlarına ayırma problemi tam olarak budur.

2009 yılında yapılan bir çalışmayla 768 bitlik bir sayı, birbirine bağlanmış yüzlerce makine iki yıl boyunca çalıştırılarak çarpanlarına ayrılmıştır. Fakat kriptografide önemli olan husus, bir algoritmayı polinom zamanda çözebilmektir. 1024 bitlik iki asal sayının çarpımı günümüz bilgisayarları için kolay bir işlem olmakla birlikte, bu iki sayının çarpımı, klasik bilgisayarlarda polinom zamanda henüz çarpanlarına ayrılamamaktadır. Dolayısıyla, algoritmalar en az 1024 bit anahtar uzunluğu hedef alınarak tasarlanmakta, gereken güvenlik düzeyine göre bu uzunluk artırılmaktadır (Şu an için yaygın kullanılan ve geçerli görülen anahtar uzunluğu 2048 bittir, askeri düzeyde güvenlik sağlamak için ise 4096 bit sayılar kullanılmaktadır).

Günümüzde, açık anahtarlı şifrelemede kullanılan (SSL/TLS protokolleri vb.) RSA algoritması bu probleme dayanarak tasarlanmıştır. Açık anahtarlı bir şifreleme tekniği olan RSA, çok büyük tam sayıları oluşturma ve



bu sayıları çarpanlarına ayırmanın zorluğu üzerine düşünülmüştür. Anahtar oluşturma işlemi için asal sayılar kullanılarak daha güvenli bir yapı oluşturulmuştur.

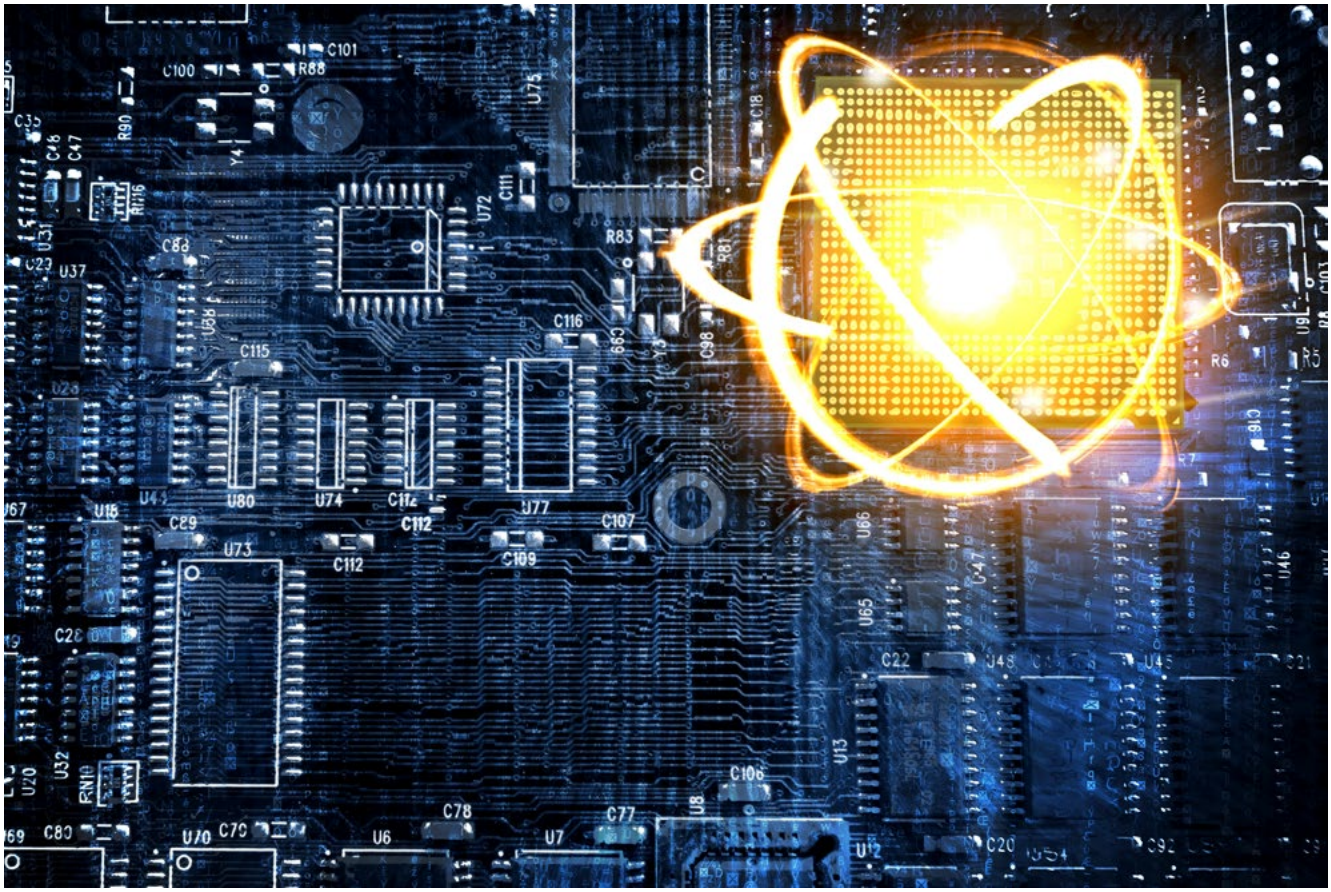
2. Ayrık Logaritma Problemi
Dijital imzalama algoritmalarının tasarımında kullanılmış olan bir diğer önemli problem ise soyut matematiği temel alan ayrık logaritma problemidir.

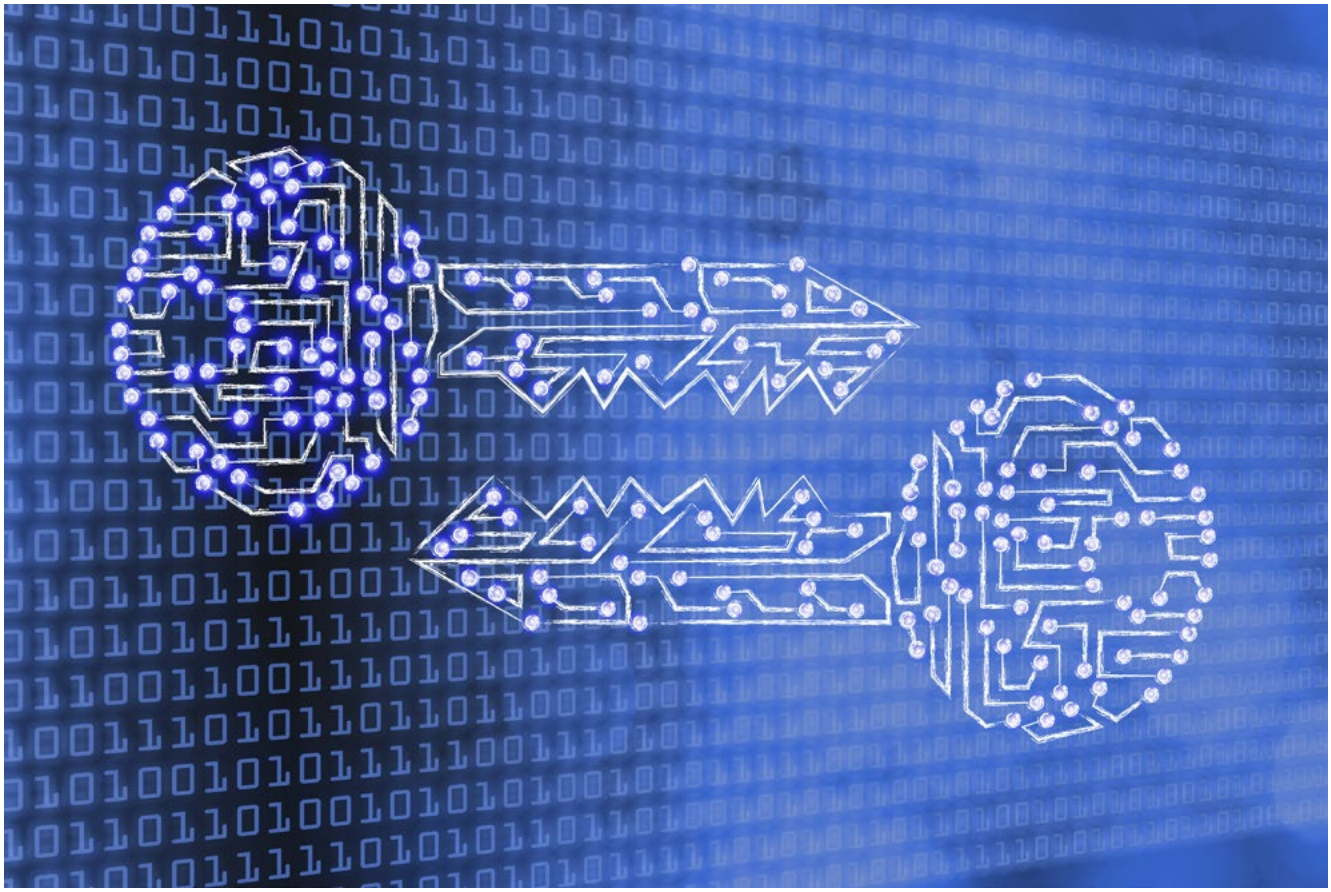
Matematiksel işlemlerde kullandığımız logaritma, doğal ya da karmaşık sayılarda kullanılan, üst alma işleminin tersidir. Ayrık logaritma ise bundan farklı olarak sonlu dairesel (döngüsel) gruplar üzerinde tanımlıdır ve sonlu dairesel bir grup olan $\mathbb{Z}_p^*$ üzerinde (p bir asal sayı) $x^a=b$ $(mod\ p)$ işleminin tersidir. Ayrık logaritma problemi ise bu denklemi sağlayan a değerini bulmanın zorluğudur. Çünkü a sayısına ait tek bir değer yoktur ve çok büyük sayılar kullanıldığında bu küme daha da genişlemektedir.

512 bitlik sayılar kullanıldığında bu işlem klasik bilgisayarlar kullanılarak polinom zamanda yapılamamaktadır. Dünyadaki tüm işlem/hesaplama gücü kullanılsa bile "a" sayısı için var olan tüm olasılıkları denemek yıllar sürebilir.

Diffie Hellman anahtar anlaşması ve Dijital İmzalama Algoritması (DSA) bu problemi temel alır ve kriptografide önemli bir rol oynar.

Kuantum Bilgisayarlar Gelince Ne Olacak?
Bilgi teknolojilerinde önümüzdeki yıllarda beklenen en büyük gelişmelerden biri kuantum bilgisayarların kullanılacak olmasıdır. Klasik bilgisayarlarla kuantum bilgisayarların zorluk dereceleri farklıdır. Bu bilgisayarlar bitler yerine q bitleri kullanmakta, bu da işlem kapasitesi ve hesaplama hızında ciddi bir artış sağlamaktadır. İçerisinde milyonlarca q bit olan bir bilgisayar geliştirilebilirse ya da yaygın kullanılan bir hale gelirse,





kapasitenin bu denli artışı ve hesaplama hızındaki yükselişle birlikte klasik bilgisayarların çözemediği, hesaplamaya dayalı problemlerin daha kolay çözüleceği düşünülmekte ve bu bilgisayarlara uygun yeni algoritmalar geliştirilmektedir.

Günümüzde en gelişmiş kuantum bilgisayarlar prototip aşamasında olup 54 civarında q bit içermektedir. Kuantum bilgisayarların klasik bilgisayarlardan daha verimli bir biçimde çalışmasının önündeki en önemli engel, milyonlarca q bit içeren bir kuantum bilgisayar üretmenin zor olması ve donanım kaynaklı rastgele hata verme ihtimalinin hâlâ yüksek olmasıdır. Ayrıca üretimde kullanılan maddelerin de güvenli olmadığı gündemdedir. Dolayısıyla kuantum bilgisayarların klasik bilgisayarlardan daha iyi performans gösterecek seviyeye gelebilmesi için zamana ihtiyaç olduğu değerlendirilmektedir.

Klasik bilgisayarların yerine geçecek ve yaygın olarak kullanılacak bir kuantum bilgisayar daha uzun vadeli bir hedef olsa da, kuantum hesaplama adına birçok temel ve pratik keşfedilmiş durumdadır. Kuantum sensörleri ve aktüatörleri, bilim insanlarının nano ölçekli hassasiyetle çalışmalarına izin vermektedir. Bu tür araçlar, gerçek kuantum bilgi işlemcilerinin geliştirilmesi için çok değerlidir. Kuantum devrimi zaten başlamış durumdadır ve sadece kriptoloji alanında değil farklı alanlarda gelişimine yönelik önündeki olasılıklar sınırsızdır.

Kriptografide kuantum bilgisayarların kullanılmasına gelince… 1994 yılında, ABD'li matematikçi Peter Shor tarafından geliştirilen "Shor Algoritması" kuantum bilgisayarlar üzerinde, çok büyük sayıları çarpanlarına ayırabilmektedir. Bu durum, birçok araştırmacı tarafından RSA algoritmasının ve asimetrik kriptosistemlerin sonunu getirecek gibi görünse de durum aslında hâlâ belirsizdir. Her ne kadar Shor Algoritması çok hızlı olsa da, bazı araştırmacılar tarafından RSA algoritmasının hızına yetişemeyeceği ya da RSA algoritmasında kullanılan anahtar uzunluğunun artırılmasıyla algoritmanın kuantum bilgisayarlarla bile kırılamayacağı savunulmaktadır[3].

3 Bernstein, D. J. (2017). Post-quantum RSA. *International Workshop on Post-Quantum Cryptography*

Simetrik sistemler içinse güvenlik önemlerini iki ila dört katına çıkarmak; AES256 yerine AES512 geliştirilmesi, özet fonksiyonları (tek yönlü fonksiyonlar) için çıktı boyutlarının artırılması şu an için yeterli gibi görünmektedir.

Bunların yanı sıra, hem klasik hem kuantum bilgisayarlarla yapılan saldırılara yönelik kuantum sonrası kriptografi diye adlandırılan algoritmalar da geliştirilmektedir. Bunlar latis tabanlı, kod tabanlı, özetleme fonksiyonu tabanlı, süper tekil izojen tabanlı ve çok değişkenli ikinci derece polinom tabanlı kriptosistemlerdir. Fakat bu algoritmalar çok yeni olduklarından ve kuantum bilgisayarlar henüz yaygınlaşmamış olduğundan güvenlik analizlerinin yapılması devam etmektedir. 2016 yılında NIST, yeni nesil açık anahtarlı kriptografik algoritma belirlenmesi amacıyla bir standartlaşma süreci başlatmıştır. İlk tur sonuçları 2019 yılının Ocak ayında yayınlanmış; güvenlik, maliyet, performans ve algoritma karakteristiklerine göre 24 algoritma ikinci tura geçebilmiştir.

Tüm bunlar göz önüne alındığında, şu an kullanılan mevcut algoritmaların geçerliliğini koruyup koruyamayacağı bilinmemekle birlikte teknolojinin evrileceği yön doğrultusunda yeni algoritmalar da geliştirilmeye devam edilerek güvenlik risklerinin en aza indirilmesi hedeflenmektedir.

Bu gelişmeler ışığında, bazı kaynaklarda yer alan modern kriptografinin sonunun geleceğine dair iddiaların gerçek dışı olduğu değerlendirilmektedir.