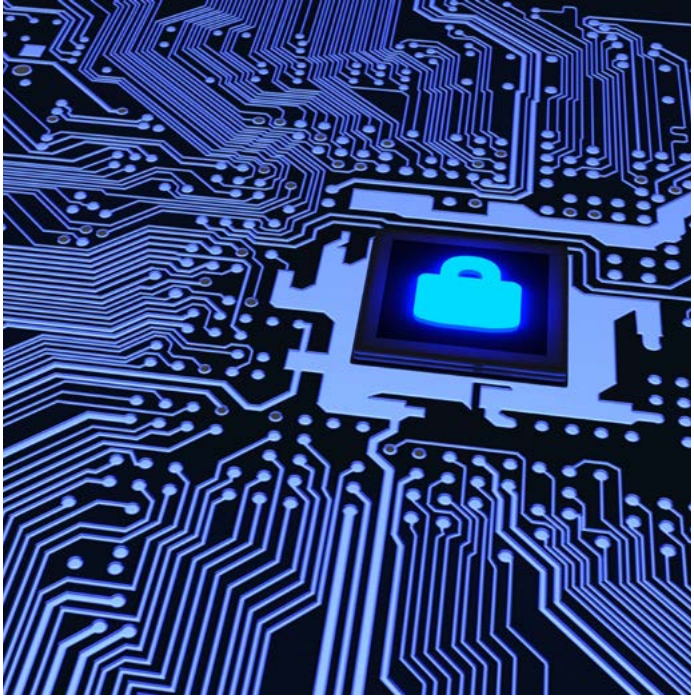
thinktech
STM Teknolojik Düşünce Merkezi



Kuantum Saldırılara Hazırlanma Zamanı

Kuantum bilgisayarlar son dönemlerin en umut vadeden teknolojilerinin başında geliyor ve bitlerle çalışan geleneksel bilgisayarlardan çok daha hızlı olacaklar. Kuantum bilgisayarlar bunu tüm olasılıkları geleneksel bilgisayarlar gibi teker teker değil, aynı anda hesaplamaları sayesinde gerçekleştirecek. Ve bu sayede geleneksel bilgisayarlarla çözülmesi yıllar süren problemler birkaç saniye içerisinde çözülebilecek[1].

Böylesine büyük bir hız elbette hayatımızda birçok şeyi değiştirecek. Ancak getireceği avantajların yanında, birtakım tehlikeler de gündeme gelecek. Örneğin, günümüzün kırılamayan şifrelerini çözmek kuantum bilgisayarlar açısından çocuk oyuncağı olacak.

Pek dikkat etmesek de e-ticaret sitelerini kullanırken, bankacılık işlemleri yaparken, e-posta gönderirken tarayıcımızın adres çubuğunda bir kilit sembolü belirir. Bu, bilgilerimizin şifrelenerek korunduğunu gösterir. Bu tür şifreleme yöntemleri kişisel ve finansal bilgilerimizin korunması açısından hayati önemdedir[2].

İki temel şifreleme türü sözkonusudur: Simetrik ve asimetrik şifreleme. Simetrik şifreleme yönteminde bir anahtar açık metni şifrelerken şifreli metni ise açık hale getirir. Simetrik şifreleme yönteminde anahtarı elinde bulunduran kişi şifreleri kolaylıkça çözebilir. Açık anahtarlı şifreleme olarak da adlandırılan asimetrik şifrelemede ise hem ortak hem de gizli bir anahtar vardır. Mesaj ortak anahtar ile şifrelenir ve karşı tarafın gizli anahtarıyla çözülebilir[3].

Geleneksel şifreleme yöntemleri, basitçe ifade edecek olursak, geleneksel bilgisayarlar tarafından çözülmesi zor matematik problemlerine dayanan gizli anahtarların gücüne bağlıdır. Örneğin 173 ve 191 sayılarını çarparak 33.043 sayısına ulaşmak kolaydır, ancak hangi iki sayının çarpımının 33.043 olduğunu bulmak o kadar kolay değildir[4]. Saldırganlar bu kodları kırmak amacıyla tüm olasılıkları deneyebilir. Ancak uzun sayı çiftleri işlerini epey güçleştirir. Örneğin 2.048 bit uygulamayla oluşturulan 617 basamaklı bir anahtarı çözmek geleneksel bilgisayarların binlerce, hatta milyonlarca yılını alabilir[2].

---

1 https://nakedsecurity.sophos.com/2019/02/07/serious-security-post-quantum-cryptography-and-why-we-are-getting-it/
2 https://www.technologyreview.com/s/613946/explainer-what-is-post-quantum-cryptography/
3 https://techdifferences.com/difference-between-symmetric-and-asymmetric-encryption.html
4 https://www.accenture.com/_acnmedia/pdf-87/accenture-809668-quantum-cryptography-whitepaper-v05.pdf

Ancak 1994 yılında geleneksel şifreleme yöntemlerinin güvenilirliğini sarsan bir fikir ortaya atıldı. Peter Shor tarafından geliştirilen algoritma kuantum bilgisayarların geleneksel şifreleme yöntemlerinin çözülebileceğini ortaya çıkardı. Çünkü geleneksel bilgisayarlarda bit olarak adlandırılan bilgiler yalnızca 0 ve 1 değerlerini alabilirken, kuantum bilgisayarlarda bitlerin yerini alan kubitlerin aynı anda hem 0 hem de 1 olması mümkündür. Süperpozisyon denilen bu durum aynı anda tüm olasılıkları hesaba katabilen kuantum bilgisayarların büyük bir hızla işlem gerçekleştirmesine olanak verir. Kubit sayısı arttıkça işlem hızı katlanarak artar. Örneğin 300 kubitlik bir kuantum bilgisayar evrendeki tüm atomların sayısının toplamından daha büyük sayıları gösterebilir. Bu sayede de şifreli anahtarların tüm olası dizilimleri çok büyük bir hızla test edilebilir[2].

Sahip olduğu bu özellikleriyle kuantum bilgisayarlar asimetrik şifrelemenin sonunu getirecek. Simetrik şifrelemede daha büyük anahtar kullanarak güvenlik düzeyi artırılabilir ve kuantum bilgisayarlara karşı bir koruma sağlanabilir. Bununla birlikte simetrik şifreleme de birtakım kuantum algoritmalarla zaman içerisinde çözülebilecek hale gelebilir.

Yani kuantum bilgisayarlar sayesinde hiçbir şey sır olarak kalmayacak. Devletlerin, şirketlerin sırları kuantum bilgisayarların olanaklarından yararlanan kötü niyetli kişilerin eline kolaylıkla geçebilecek.

Finanstan ticarete, ulaşımdan savunmaya dek birçok sektörün sağlıklı işleyişinin güvenli iletişime bağlı olduğu düşünülürse, kuantum bilgisayarların tüm şifreleri kırması bir anlamda bir kuantum kıyamete de yol açabilecek[5].

Böyle bir durum sadece e-ticaret sektöründe 100 milyarlarca dolar kayıp anlamına gelebilir. Ekonominin genelinde yaşanan kayıplar trilyon dolarları bulabilir. Özel hayat diye bir şeyin kalmaması ve jeopolitik riskler ise işin diğer boyutları[6].

Elbette bunlar hemen gerçekleşmeyecek. Kuantum bilgisayarlar henüz geleneksel bilgisayarların hızına ulaşabilmiş değil. Ancak bu alanda her gün yeni gelişmeler yaşanıyor ve kuantum bilgisayarların gerekli eşiği aşacağı gün giderek yaklaşıyor.

2015 yılında gerçekleştirilen bir araştırmada kuantum bilgisayarların 2.048 bitlik bir RSA sistemini çözmesi için 1 milyar kubite ihtiyaç duyacağı hesaplanmıştı. Ancak yakın zamanda gerçekleştirilen bir başka araştırma, 20 milyon kubitlik bir kuantum bilgisayarın bu şifreyi sekiz saatte çözebileceğini ortaya çıkardı[2]. Yani kuantum bilgisayarlar er geç tüm şifreleri çözecek. Tabii kuantum bilgisayar çağına uygun yeni şifreleme yöntemleri geliştirilmezse.

İşte bu nedenle, güvenlik kaygısı taşıyan kurumlar şimdiden kuantum bilgisayarlar sonrası şifreleme yöntemleri üzerinde çalışmaya başladı. Kuantum bilgisayarların yarattığı tehdide karşı mücadele iki aşamadan oluşacak. İlk aşamada geleneksel şifreleme yöntemleri kuantum saldırılara karşı güçlendirilecek. Kuantum bilgisayarların yaygınlık kazanacağı ikinci aşamada ise geleneksel şifreleme yöntemleri bir yana bırakılarak kuantum şifreleme yolları geliştirilecek[4].

Şu anda ilk aşamadayız. Post kuantum kriptografi adı verilen bu ilk aşama çalışmalarının amacı, geleneksel bilgisayarları kuantum bilgisayarlardan gelebilecek saldırılara karşı korumak.

Örneğin Amerikan Ulusal Standartlar ve Teknoloji Enstitüsü (National Institute of Standards and Technology/ NIST) 2022 yılı itibarıyla kuantum dirençli şifreleme algoritmaları oluşturmak üzere harekete geçmiş halde. 69 ekiple başlanan kuantum bilgisayarlara dirençli şifreleme yöntemleri geliştirme sürecinin ikinci aşamasında, 23 ekip en dirençli şifreleme yöntemini geliştirmek için çalışmaya devam ediyor[6].

5 https://www.quantaneo.com/The-Search-for-Quantum-Resistant-Cryptography-Understanding-the-Future-Landscape_a260.html
6 https://spectrum.ieee.org/tech-talk/telecom/security/how-the-us-is-preparing-for-quantum-computings-threat-to-end-secrecy

NIST bünyesinde gerçekleştirilen çalışmalarda geliştirilen algoritmalar temel itibarıyla iki genel kategoriye ayrılıyor. Bunların ilki hiç karşılaşmamış iki tarafın ortak bir sır konusunda hemfikir olması ilkesine dayalı anahtar oluşturma algoritmaları. RSA ve eliptik eğri gibi açık anahtarlı şifreleme algoritmaları da bu sınıfa giriyor.

Bu çalışmaların ardından sıra kimlik doğrulama amacıyla kullanılan verinin özgünlüğünü, bozulmadığını, değiştirilmediğini gösteren dijital imzaların güvenliğinin sağlanmasına gelecek[7]. Dijital imzalar bir kullanıcı ya da sunucudan gönderilen bilginin o kurum ya da kişiye ait olduğunu kanıtlar. Veri akışı sırasında içeriğin korunmasını sağlar, değiştirilmesini engeller. Bunun yanı sıra gönderenin ve alıcının kimliğini kanıtlar. Yani gönderen gönderdiğini, alan da aldığını inkâr edemez.

Bu yöntemler arasında en popüler ve en umut vadeden yöntemlerin başında Kafes Temelli Şifreleme geliyor. Kod Tabanlı Şifreleme, Çok Değişkenli Polinom Şifreleme, Karma Tabanlı İmzalar da üzerinde çalışılan diğer yöntemler[8].

Tüm çözümler kuantum bilgisayarların bile çözemeyeceği matematik problemlerine dayalı yeni algoritmalar geliştirilmesini gerektiriyor. Bu algoritmaların geliştirilmesine yönelik farklı yaklaşımlar sözkonusu ve bu yaklaşımların her birinin kendine özgü avantajları ve dezavantajları bulunuyor. Örneğin kod bazlı şifrelerin uzun yıllardır kullanılıyor olması gibi bir avantajı bulunuyor. Kafes bazlı şifreler ise çok hızlı algoritmalar sunabiliyor ancak büyük boyutları sıkıntılar doğurabiliyor.

Hangi yöntemin başarılı olacağı ve standart halini alacağı henüz belli değil. Sürecin bu kadar uzamasının nedeni, en ufak bir açığa yer vermeyen çok titiz bir çalışma gerektirmesi. Çünkü online bankacılık işlemlerinden e-ticarete, kişisel bilgilerden e-postalara dek her şeyin güvenliği bu kuantum bilgisayarların hızına ve gücüne karşı koyabilen bu yeni nesil şifreleme yöntemlerine bağlı olacak.

Ancak bir yandan da post kuantum şifreleme üzerinde çalışanların ellerini çabuk tutmaları gerekecek çünkü kuantum bilgisayarların mevcut şifreleri ne zaman çözecek hale geleceği bilinmiyor. Belki de kuantum bilgisayarlar umulandan çok daha çabuk güçlenecek ve geleneksel şifreleme yöntemleri hazırlıksız yakalanacak[9].

7 https://www.nist.gov/news-events/news/2019/01/nist-reveals-26-algorithms-advancing-post-quantum-crypto-semifinals
8 https://eprint.iacr.org/2019/047.pdf
9 https://www.microsoft.com/en-us/research/project/post-quantum-cryptography/