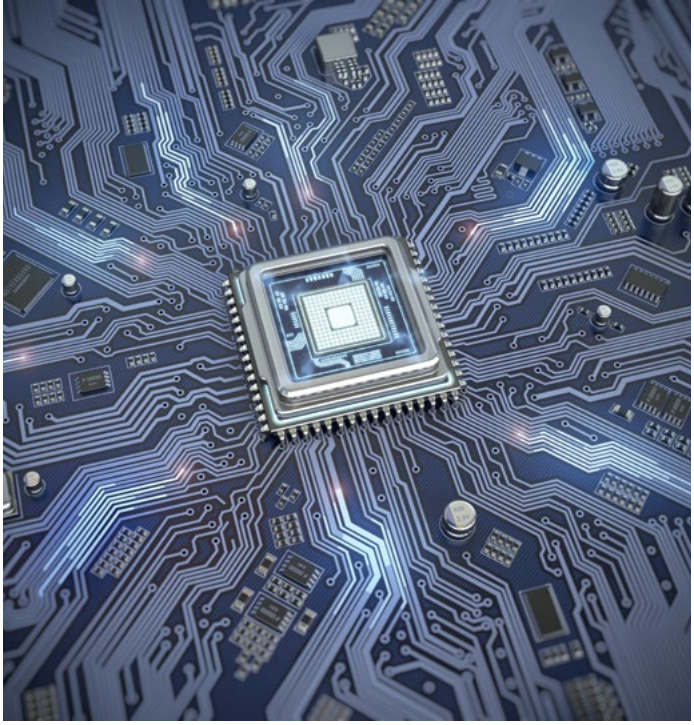
thinktech
STM Teknolojik Düşünce Merkezi

Hack Tehdidine Karşı Kuantum Kriptografisi



İnsanlığın kendine ait olanı saklama dürtüsü milyonlarca, bu amaç için şifreleme metodunu kullanması ise binlerce yıllık tarihe sahip. Yaklaşık 4.000 yıl önce Mısır'ın Menet Khufu kasabasında yaşamış soylu bir kişi olan Knhumhotep II'ye ait mezarın üzerindeki yazılar okunmasın diye karmaşık sembol ve numaralardan yararlanılırken; M.Ö. 5 yılında Spartalılar, birbirlerine yolladıkları gizli mesajları şifrelemek için çok daha karmaşık bir yöntem seçmişti. Bu savaşçı toplumda yollanan mesajları şifrelemek için yazının işlendiği parşömen ya da deri ince, uzun şeritlere bölünürdü. Şeritler halindeyken hiçbir anlam ifade etmeyen bu yazılar, mesajın alıcı ve vericisinde de bulunan, "scytale" adı verilen özel açılı silindire sarıldığında okunabilir hale gelirdi[1,2]. Spartalıların bu yöntemi, modern şifreleme tekniklerinin temeli olarak gösteriliyor. Bugünün şifreleme tekniklerine bir diğer büyük katkı ise Julius Ceasar'dan geldi. Yunan yazar Polyibus'un tekniğini kullanan Ceasar, mektuplarını yazarken her harf yerine, alfabede onu takip eden üçüncü harfi kullanırdı.

Kuantum Konsepti İlk Kez Endüstriyel Alanda

Peki binlerce yıl önce geliştirilen bu metotları insanlık nereye taşıdı? Bugün hepimizin kullandığı modern yöntemler hem şifreleme hem de şifreyi çözmede, rastgele seçilmiş ikili dizilerden faydalanıyor. Diğer yandan gelecekte kuantum kriptografisinin bu sisteme entegre edilmesi; böylece mevcut kriptografi algoritmalarına ek olarak iki bilgisayar arasında anahtarın alıcıya iletilme sürecinin neredeyse tüm güvenlik açıklarından arınmış bir hale getirilmesi hedefleniyor. Kuantum konsepti, bugüne, yani kuantum kriptografisine dek, sadece bilimsel araştırma amaçlı kullanılmıştı. Bu teknolojiyle birlikte kuantum konseptinin endüstriyel alanda ilk kez uygulandığı yeni bir döneme giriliyor[3].

Yakın gelecekte mevcut teknolojinin en sağlam şifrelemelerini bile kırabileceği düşünülen kuantum kriptografisinde veri iletimi algoritmalar ve elektriksel işaretler yerine fotonlar üzerinden gerçekleştiriliyor. Yani mesajın vericisi ile alıcısı arasında iletişim, fotonlarla kuruluyor. Kuantum kriptografisinin fotonlar üzerinden çalışması ciddi bir güvenlik sağlarken, sadece fiber optik ağ ile çalışabilmesine yönelik bir kısıtlama da getiriyor. Bu sistem için aynı zamanda kuantum bilgisayar, yani kuantum mekaniği ile çalışan; sıradan bilgisayarlardan çok daha yüksek işlem gücüne sahip, milyonlarca farklı ihtimali aynı anda inceleyip hesap yapabilen teknolojik aletler kullanılması gerekiyor[4].

Kuantum kriptografisi denildiğinde genellikle Quantum Key Distribution (QKD), yani kuantum anahtar dağıtımı kastedilir. QKD aslında yollanan bilginin değil, alıcı ve verici arasında bir anahtar ya da şifrenin

1 http://www.cypher.com.au/crypto_history.htm
2 https://www.youtube.com/watch?v=TZv_dZB0YBg
3 https://homepage.univie.ac.at/Reinhold.Bertlmann/pdfs/dipl_diss/PetraPajic_BA_QuantumCryptography.pdf
4 https://www.csoonline.com/article/3235970/what-is-quantum-cryptography-it-s-no-silver-bullet-but-could-improve-security.html

güvenli bir şekilde transfer edilebilmesini sağlar. Bu anahtar da iletilen mesajın şifresini açmada ya da o mesajı tekrar şifrelemede kullanılabilir[5]. Yani kuantum kriptografisi verinin kendisini şifrelemez/korumaz, bu verinin transferi için kullanılmaz ve önemli bilgileri güvenli bir şekilde saklamak amacıyla değerlendirilmez. QKD teknolojisi daha ziyade, klasik algoritma ve protokollerle çözülerek anlamlı bir mesaj haline dönüştürülebilecek gizli şifreleri oluşturmak ve bu şifreleri aralarında mesafe olan iki kişi arasında dağıtmak için kullanılır[6].

Temelinde Fizik Kuralları Yatıyor

Peki bu teknoloji adını neden kuantumdan alıyor? Günümüzde yaygın olarak kullandığımız şifreleme metotlarının aksine matematik değil, fizik kurallarını temel alan QKD'nin temelinde yatan iki prensipten ilki, Heisenberg'ün Belirsizlik İlkesi. Bu ilkeye göre foton gibi herhangi bir maddenin kuantum hali, o maddeyi tahrip etmeden ölçülemez[7]. Kuantum haldeki maddeler, örneğin foton, süperpozisyon halde gönderilebilir; bu da onun aynı anda hem 1 hem de 0 rakamlarını temsil edebilmesini sağlar. Maddenin gerçekten 1 mi yoksa 0'ı mı temsil ettiğini görebilmek için, onun ölçülebilmesi ya da gözlemlenmesi gerekir. Sistemin vadettiği yüzde 100 güvenlik iddiası da bu prensibe dayanır. Süperpozisyon haldeki maddeye yönelik herhangi bir ölçüm ya da gözlem girişimi, onda tahribata yol açar. Dolayısıyla kuantum kriptografisi yöntemiyle şifre iletilirken üçüncü bir kişi sürece dahil olmak ister ve fotonu ölçerse, asıl alıcıya tekrar yönlendirdiği foton, hal değiştirmiş/tahrip edilmiş olur. Alıcı bu anlamsız şifreyi aldığı anda, birinin sisteme dahil olduğu anlaşılır ve güvenlik böyle sağlanır[8].

QKD'nin ikinci temel ilkesi ise, foton polarizasyon prensibi. Bu ilke, bir fotonun belirli bir yöne kilitlenebilmesini ya da kutuplanabilmesini tanımlar. Dahası, yine bu ilkeye göre doğru polarizasyona sahip foton filtresi sadece polarize fotonu saptayabilir ya da foton yok olur. Yani sadece gönderilen fotonun polarizasyonunu bilen alıcı, fotonu ölçebilir. Bu, üçüncü bir şahıs da olabilirken; tek yönlülüğe herhangi bir üçüncü şahsı saptayan Belirsizlik İlkesi de eklenince, QKD son derece güvenli bir yöntem olarak öne çıkıyor[9]. Peki fotonun yapısı bozulduysa, onu ilk haliyle klonlayarak aynı polarizasyon doğrultusunda tekrar transfer etmek mümkün mü? Yine kuantum kurallarından "no-cloning theorem" yani klonlanamazlık ilkesi bize, hiçbir kuantum durumunun bire bir kopyalanamayacağını, yani klonlanamayacağını söylüyor[10].

Kuantum kriptografisi Avrupa'da 2007, Amerika Birleşik Devletleri'nde ise 2010 yılından beri, özellikle uluslararası para transferi ve seçim sonuçları gibi önemli verileri korumak için kullanılıyor[5]. Ancak yakın gelecekte QKD'nin daha da yaygınlaşması bekleniyor. Peki QKD'ye neden ihtiyacımız var, bugünün teknolojisiyle devam etmeyecek olmamızın sebebi ne? Bugün verilerimizi hem simetrik, hem de asimetrik şifreleme yöntemleriyle koruyoruz. Simetrik şifrelemede alıcı ve verici arasındaki veri alışverişi için tek bir şifre kullanılırken; asimetrik şifreleme algoritması mesajların şifresini çözmek için bir açık (public), bir de özel (private) olmak üzere iki farklı şifreden faydalanır. Bu sebeple asimetrik şifrelemenin kırılması daha uzun zaman alır. Ancak devletlere ait gizli verilerden ünlülerin fotoğraflarına dek pek çok şeyin ele geçirilip kamuoyuyla paylaşılabildiği 21'inci yüzyılda bu iki yöntem de "hack'lenemez" bir koruma sistemi vadedemiyor. Modern kriptografinin, teknolojik gelişmeler sayesinde elde edilen yüksek işlemci gücü ve matematiğin devinim halindeki gelişimi karşısında hassas bir yere sahip olduğu düşünülüyor. İşte tam bu sebeple geleceğin şifreleme teknolojisinde matematiği, yani mevcut algoritmaları; fizik, yani kuantum destekliyor olacak.

Kuantum eklentisiyle sadece alıcı ve verici arasında veri alışverişi daha güvenli hale gelmiyor, aynı zamanda mevcut simetrik ve asimetrik şifreleme sistemlerinin çok daha hızlı ve kolay bir şekilde kırılabilmesi hedefleniyor. Örneğin, iki farklı şifre ile korunan asimetrik sistemlere bir kuantum bilgisayarı algoritması olan SHOR ile saldırılabileceği belirtiliyor. Özellikle blockchain transferlerini korumada kullanılan asimetrik

5 https://www.extremetech.com/extreme/287094-quantum-cryptography
6 http://www.ucci.it/docs/QC-Pros+Cons-0.4.pdf
7 https://searchsecurity.techtarget.com/definition/quantum-cryptography
8 https://www.wired.co.uk/article/quantum-cryptography-and-the-future-of-security
9 https://cs.stanford.edu/people/adityaj/QuantumCryptography.pdf
10 https://www.physics.umd.edu/courses/Phys402/AnlageSpring09/TheNoCloningTheoremWoottersPhysicsTodayFeb2009p76.pdf

şifreler, modern bilgisayarların asal çarpan bulamama özelliğine dayanıyor. SHOR[11] algoritması ise özellikle asal çarpanlara yönelik geliştirilmiş. Bir rakamı alıp çarpanlarına ayırabilen algoritma, asal çarpan bulma basamaklarını azaltarak zaman da kazandırabiliyor. Örneğin modern bir bilgisayarın asimetrik bir şifreyi kırması için 36 haneli bir sayıda (yani çok sayıda!) basit operasyon yürütmesi gerekirken, bir kuantum bilgisayarı bu işlemi 2 milyondan biraz fazla operasyonla tamamlayabiliyor.

Günlük hayatımızda daha çok kullandığımız simetrik şifreler için geliştirilen GROVER algoritması ise, tıpkı kuantum olmayan bilgisayarlar gibi, mümkün olan tüm olasılıkları deneme prensibine dayanıyor. Ancak, kuantumun süperpozisyon özelliğinden faydalanan algoritma, bu sayede aynı anda birden fazla işlem gerçekleştirebiliyor. Örneğin, modern bir bilgisayarla 78 haneli bir sayıda basit operasyon gerektiren düzenleme işlemini, GROVER algoritmasıyla çalışan bir kuantum bilgisayarı yarı yarıya, yani 39 haneli bir sayıda operasyonla tamamlıyor[11]. Böylece, şifreleri kırmak için gerekli süre ciddi ölçüde azalıyor[12].

Pazar Değeri Yılda Yüzde 38 Artacak

Kuantum kriptografisinin geleceği nasıl değiştirebileceğine de değinmek şart. Güvenli şifre alışverişi sağlayan bu teknoloji özellikle ordu gibi yüksek seviyede güvenliğe gereksinim duyan, hem şimdi hem de gelecekte güvenilirliği olan bir ağ arayışındaki kurumlara hitap ediyor[6]. Global hack tehdidinin hedefindeki büyük şirketler, kuantum kriptografisi sayesinde verilerini güvenli bir şekilde saklamayı ve paylaşabilmeyi hedefliyor. "Hack'lenemez iletişim" fırsatı vadeden bu teknolojinin finans, sağlık ve profesyonel hizmet sunan şirketler için de önemli olduğu belirtiliyor[13]. Mayıs ayında yayımlanan "Global Kuantum Kriptografisi Pazar Raporu"na göre teknolojinin pazar değeri 2018 yılında 102,56 milyon dolarken, 2026 yılında 1.353,70 milyon dolara ulaşacak. Bu da sektörün, yüzde 38,06'lik yıllık bileşik büyüme oranını yakalayacağını ifade ediyor[14].

Kuantum Kriptografisinin Zayıf Noktası

Kuantum kriptografisinin vadettiği güvenlik pek çok şirketi cezbederken; bu teknolojinin önündeki engellerden de bahsetmek gerek. Örneğin günümüzde çok sayıda kuantum kodu ve hata doğrulama tekniği olsa da; kuantum kodlamanın soyut çerçevesiyle daha fiziksel, gerçekçi, büyük ölçekli hata doğrulama uygulamaları arasında ciddi bir ayrım, farklılık olduğu kabul ediliyor. Kuantum bilgi işleminin geleceği çok sayıda olasılığa açık. Çok daha gelişmiş teknikler ortaya konsa dahi; mevcut kübit üretiminin fiziksel inşası ve tutarlılığının kuantum hata doğrulamadan faydalanabilmek için hâlâ yetersiz olduğu itiraf ediliyor. Bu sebeple sektör, kuantum kriptografisinin gelecekte iki farklı kategoriye ayrılacağını düşünüyor. Bunlardan ilki daha fiziksel ve gerçekçi; daha ziyade küçük boyutlu kübit uygulamaları; ikincisi ise daha büyük boyutlu, örneğin 1000 fiziksel kübit boyutunu aşan büyük ölçekli işlemleri kapsayacak. SHOR da bu kategoriye giren, büyük ölçekli bir algoritma[11]. Hem gerçek kuantum kodunun hem de hata doğrulama prosedürlerinin fiziksel seviyede etkin bir şekilde birleştirilebilmesinin, büyük ölçekli işlemler için çok önemli olduğu ifade ediliyor. Son çalışmalarda kuantum bilgisayarlardaki hata oranından dolayı AES-256 algoritmasına saldırmak için 6.000 kübitten fazlasına ihtiyaç olduğu iddia ediliyor[15]. Bu teknolojinin kısıtlamalarından diğeri, daha önce de belirttiğimiz gibi, sadece fiber optik kablo ile çalışabilmesi. Buna ek olarak bir foton bu kablolarla, sönmeye başlamadan önce en fazla 100 kilometre ilerleyebiliyor. Ayrıca 100 kilometreyi aşan mesafelerde, özellikle büyük şehir merkezlerinde iletim yapılıyor ise, amplifikatörlerin kuantum bütünlüğünü bozacağı düşünülüyor. Bu sebeple daha uzun mesafeler için, gönderilen şifreyi tekrar transfer etmek gerekiyor ki bunun için, çok pahalı ve ciddi bir güvenlik donanımı kurulması şart.

QTD teknolojisine yatırım yapan firmalardan BT, bu sorunu uydu yardımıyla çözmeyi hedefliyor. Amaçları, fotonların Dünya'ya yakın konumlanan uydulara gönderilerek tekrar yeryüzündeki istasyonlara iletilebileceği bir sistem kurmak. Daha uzak bir gelecekte olsa da, QKD'yi geliştirirken kuantum dolanıklığı ilkesinden

11 https://codeburst.io/quantum-threat-to-blockchains-shors-and-grover-s-algorithms-9b01941bed01
12 https://www.cryptomathic.com/news-events/blog/quantum-computing-and-its-impact-on-cryptography
13 http://www.toshibamea.com/generic/toshibytes-blogpost12-quantum-cryptography/#
14 https://stocknewsmagazine.com/quantum-cryptography-market-valued-1353-70-million-dollar-2026-report-id-quantique-quintessencelabs-nucrypt-anhui-qasky-quantum-technology-pq-solutions-limited-others/
15 https://arxiv.org/pdf/0905.2794.pdf

faydalanılması bekleniyor. Kuantum dolanıklığı, iki kuantum taneciğinin "mesafesi ne olursa olsun" etkileşim kurabileceğini ifade ediyor[8,16]. Bu, kuantum kriptografisini güvenli iletişim konusunda çok üst bir noktaya taşıyabilir. Peki ya kuantum kriptografisini güvenlik açısından dünyanın merkezine yerleştiren "hack'lenemezlik" özelliği, bu teknolojinin en ciddi zayıf noktası ise? Her gün "ulaşılamaz" olarak tanımlanan verilerin hacker'ların eline geçtiği haberini okuyoruz ve evet, kuantum kriptografisi sayesinde hack tehdidi sonsuza kadar ortadan kalkabilir. Ancak sorun şu ki, en yetkin güvenlik kurumları da, kuantum kriptografisiyle korunan verilere erişemez konumda olacak; o veri devletin resmi bir kurumuna, bir teknoloji devine ya da insanlığa ciddi zarar verebilecek tehlikeli bir girişime ait olsa dahi[17].

16 https://arxiv.org/pdf/quant-ph/9504002.pdf
17 https://cdn.journals.aps.org/files/RevModPhys.74.145.pdf