KUANTUM BİLGİSAYARLAR VE ŞİFRELEME

Q-Day'e Hazırlık: Shor Algoritmasından NIST Post-Kuantum Standartlarına, 'Şimdi Topla, Sonra Çöz' Tehdidinden Türkiye'nin Kuantum Stratejisine

Derleme Makale / Review Article

Dr. Burak Olgun
burakolgun@solutionhome.net
Solution Home Bilişim Tekn. ve Dan. Hizm., İstanbul

Anahtar Kelimeler: *Kuantum Bilgisayar • Post-Kuantum Kriptografi • Shor • NIST FIPS 203/204/205 • HNDL • ML-KEM • Q-Day*

burakolgun.com

ÖZET

Kuantum bilgisayarlar, klasik bilgisayarların çözmekte güçlük çektiği ya da çözemeyeceği problemleri süperpozisyon, dolanıklık ve kuantum girişim prensipleri aracılığıyla işleme kapasitesiyle dijital çağın kriptografik altyapısına varoluşsal bir tehdit oluşturmaktadır. Peter Shor'un 1994'te geliştirdiği algoritma, büyük sayıların asal çarpanlarına ayrılması sorununu — günümüz RSA şifrelemesinin matematikal temelini — polinom zamanda çözebilecek kuantum devrelerini teorik olarak tanımlamaktadır. Google'ın 2024 sonunda duyurduğu Willow çipi, qubit sayısı artarken hata oranının üstel biçimde azaldığını — hata eşiğinin altına inildiğini — kanıtlayarak büyük ölçekli hata toleranslı kuantum hesaplamanın fizibilitesini tescil etmiştir. NIST, Ağustos 2024'te sekiz yıllık standardizasyon sürecinin ürünü olan FIPS 203 (ML-KEM), FIPS 204 (ML-DSA) ve FIPS 205 (SLH-DSA) post-kuantum kriptografi standartlarını yayımlamıştır. Bu derleme makale; kuantum bilgi işlemin temel prensiplerini, Shor ve Grover algoritmalarının kriptografik etkilerini, 'Şimdi Topla Sonra Çöz' (Harvest Now Decrypt Later — HNDL) tehdit modelini, NIST PQC standartlarını ve kafes tabanlı kriptografiyi, kritik altyapıların geçiş sürecini, Türkiye'nin kuantum stratejisini ve kurumların bu tehdide karşı alması gereken önlemleri kapsamlı biçimde ele almaktadır.

Anahtar Kelimeler: *kuantum bilgisayar, post-kuantum kriptografi, Shor algoritması, Grover algoritması, NIST FIPS 203, FIPS 204, FIPS 205, ML-KEM, ML-DSA, SLH-DSA, CRYSTALS-Kyber, CRYSTALS-Dilithium, kafes tabanlı kriptografi, HNDL, Q-Day, kripto çeviklik, Türkiye kuantum stratejisi, TÜBİTAK BİLGEM*

ABSTRACT

Quantum computers pose an existential threat to the cryptographic infrastructure of the digital age, with the capacity to process problems that classical computers struggle or fail to solve through superposition, entanglement, and quantum interference principles. The algorithm developed by Peter Shor in 1994 theoretically defines quantum circuits that can solve the problem of factoring large numbers into prime factors — the mathematical foundation of modern RSA encryption — in polynomial time. Google's Willow chip announced at the end of 2024 registered the feasibility of large-scale fault-tolerant quantum computing by demonstrating that error rates decrease exponentially as qubit counts increase. NIST published the post-quantum cryptography standards FIPS 203 (ML-KEM), FIPS 204 (ML-DSA), and FIPS 205 (SLH-DSA) in August 2024, the product of an eight-year standardization process. This review article comprehensively addresses the fundamental principles of quantum information processing, the cryptographic impacts of Shor and Grover algorithms, the Harvest Now Decrypt Later (HNDL) threat model, NIST PQC standards and lattice-based cryptography, the transition process for critical infrastructures, Turkey's quantum strategy, and the measures organizations should take against this threat.

Keywords: *quantum computing, post-quantum cryptography, Shor algorithm, Grover algorithm, NIST FIPS 203, FIPS 204, FIPS 205, ML-KEM, ML-DSA, SLH-DSA, lattice-based cryptography, HNDL, Q-Day, crypto-agility, Turkey quantum strategy, TÜBİTAK BİLGEM*

kurakdgn.com

1. Giriş

1994 yılında matematikçi Peter Shor, büyük tam sayıların asal çarpanlarına ayrılması ve ayrık logaritma hesaplama problemlerini polinom zamanda çözebilecek bir kuantum algoritması tanımladı. O dönemde bu buluş büyük ölçüde teorik nitelikteydi; çünkü Shor algoritmasını çalıştırabilecek kuantum donanımı mevcut değildi. Otuz yıl sonra, 2024'te tablo köklü biçimde değişmektedir: Google'ın 105 qubitlik Willow çipi, qubit sayısı arttıkça hata oranının üstel biçimde azaldığını — 'hata eşiğinin altına inildiğini' — kanıtlamıştır. Techvorta.com'un (2026) değerlendirmesine göre bu gelişme 'kuantum bilgisayar yolculuğunu temelden değiştiren kırılma noktasıdır.'

Kuantum tehdidin aciliyeti yalnızca gelecekteki bir risk değildir; 'Şimdi Topla, Sonra Çöz' (Harvest Now Decrypt Later — HNDL) stratejisi tehdidi bugüne taşımaktadır. Jena'nın (2025) European Journal of Computer Science and Information Technology'deki çalışmasının belirttiği gibi: 'HNDL tehdit modeli, rakiplerin bugün uzun vadeli şifrelenmiş verileri sızdırdığı ve bu verilerin gelecekte kuantum yollarla çözüleceğini öngördüğü gerçeğini ortaya koymaktadır.' Bu saldırı türü, kuantum bilgisayarlar henüz RSA'yı kırmaya yeterli olmasa da bugün başlamış durumdadır.

NIST'in yanıtı, 2016'dan 2024'e uzanan sekiz yıllık bir uluslararası standartlaştırma süreciyle somutlaşmıştır. Ağustos 2024'te yayımlanan FIPS 203 (ML-KEM), FIPS 204 (ML-

DSA) ve FIPS 205 (SLH-DSA) standartları, kuantum sonrası kriptografinin temel yapıtaşlarını oluşturmaktadır. Bu standartlar 2035 yılına kadar RSA, ECDSA ve Diffie-Hellman gibi kuantuma karşı savunmasız algoritmalar için tek geçerli geçiş hedefi olmaya devam edecektir (NIST IR 8547, 2024).

Bu makalenin amacı; kuantum bilgi işlemin temellerini, mevcut kriptografik sistemlere yönelik tehdidi, NIST standartları ve kafes tabanlı kriptografiyi, HNDL risk modelini, kritik altyapı geçiş süreçlerini, Türkiye'nin kuantum hamlesini ve pratik kurumsal hazırlık önerilerini kapsamlı biçimde incelemektir. Makale adli bilişim ve bilgi güvenliği perspektifiyle kaleme alınmış olup hukuki, teknik ve kurumsal boyutları bir arada değerlendirmektedir.

2. Kuantum Bilgi İşlemin Temelleri

2.1 Klasik Bit'ten Qubit'e

Klasik bilgisayarlar bilgiyi ikili sistem üzerinden işler: Her bit ya 0 ya da 1 değerini alır. Kuantum bilgisayarlar ise kuantum mekaniğinin üç temel prensibini kullanan qubit'ler üzerinde çalışır. Bu prensipler birbirinden temelden farklı hesaplama kapasitesi sunar.

Süperpozisyon (Superposition): Bir qubit, ölçüm yapılana kadar 0 ve 1 durumlarının matematiksel süperpozisyonunda var olabilir. Bunu bir yazı-tura atıldıktan ancak bakılmadan önce hem yazı hem tura olması olarak düşünebiliriz. n qubitlik bir sistem 2^n farklı durumu aynı anda temsil edebilir; bu durum paralellik açısından klasik bilgisayarla kıyaslanamaz bir avantaj sağlar.

Dolanıklık (Entanglement): İki veya daha fazla qubit arasında klasik fizikle açıklanamayacak korelasyonlar kurulabilir. Dolanık qubitlerden birinin ölçümü, diğerinin durumunu anında belirler — aralarındaki mesafeden bağımsız olarak. Bu özellik, kuantum ağlarda güvenli iletişim ve dağıtık kuantum hesaplama için kritik altyapıyı oluşturmaktadır.

Kuantum Girişimi (Interference): Dalga girişimine benzer biçimde kuantum girişimi, yanlış cevapların olasılığını azaltırken doğru cevapların olasılığını artırır. Kuantum algoritmaları, bu prensibi kullanarak hesaplamayı yönlendirir. Shor ve Grover algoritmalarının verimliliği büyük ölçüde bu mekanizmaya dayanır.

2.2 Kuantum Bilgisayar Türleri ve Donanım Yaklaşımları

Günümüzde farklı fiziksel substratlar kullanarak kuantum bilgisayar geliştiren birden fazla yaklaşım mevcuttur. Süperiletken qubitler (IBM, Google): Millikelvin sıcaklıklarda çalışan ve CMOS üretim teknolojisine yakın süperiletken devreler. IBM ve Google bu alanda öncü konumdadır. IBM'in Nighthawk çipi, 2025 sonu itibarıyla kullanıcılara sunulacak olup 120 qubit ile 218 bağlayıcı içermektedir (IBM, 2025).

İyon tuzağı qubitler (IonQ, Honeywell/Quantinuum): İyonize edilmiş atomlar elektromanyetik alanlarla tutulur. Yüksek bağlılık süresi ve düşük hata oranıyla öne çıkar; ancak ölçekleme daha yavaştır. IonQ, 2028'e kadar kriptografik açıdan önemli kuantum bilgisayar (CRQC) hedefini ilan etmiştir (postquantum.com, 2025).

Fotonik qubitler (PsiQuantum, Xanadu): Fotonları qubit olarak kullanan bu yaklaşım oda sıcaklığında çalışabilir ve veri merkezi benzeri ölçekleme potansiyeli sunar. Microsoft'un

burakoguz.com

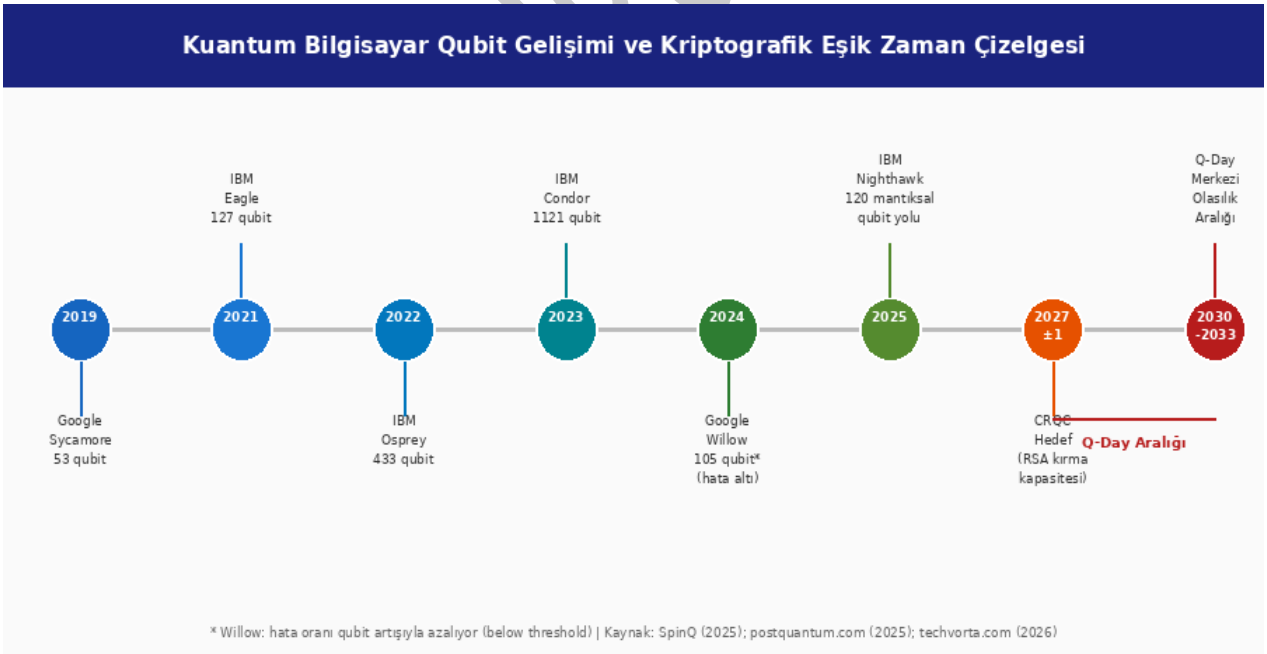
topografik qubit (Majorana tabanlı) girişimi ise yüksek risk, yüksek getiri bir yaklaşımı temsil etmekte; başarılı olması halinde CRQC için gereken qubit ek yükünü dramatik biçimde azaltabilecektir (postquantum.com, 2025).

2.3 NISQ Çağı ve Hata Düzeltmenin Önemi

Günümüz kuantum bilgisayarları 'Gürültülü Orta Ölçekli Kuantum' (Noisy Intermediate-Scale Quantum — NISQ) çağında yer almaktadır. Bu makineler gerçek dünya problemleri için yeterli qubit sayısına sahip olmakla birlikte yüksek hata oranları hesaplama güvenilirliğini kısıtlamaktadır. Shor algoritmasını RSA-2048'i kıracak ölçekte çalıştırmak için yaklaşık 4.000 mantıksal (hata düzeltilmiş) qubit gerektiği tahmin edilmektedir; her mantıksal qubit ise mevcut teknolojide yüzlerce ile binlerce fiziksel qubit gerektirmektedir.

Google'ın Willow çipinin 2024'teki kritik katkısı tam da burada yatmaktadır. SpinQ'nun (2025) aktarımına göre Willow, 'qubit sayısı arttıkça üstel hata azalması — hata eşiğinin altına inme — olgusunu kanıtladı.' Bu, ölçeklenebilir hata düzeltmenin gerçekten mümkün olduğunun ilk deneysel kanıtıdır. IBM'in 2024'te Nature'da yayımladığı makale ise 144 veri qubitinde 12 mantıksal qubit kodlayan bivariate bicycle qLDPC kodunu sunarak hata düzeltme verimliliğini önemli ölçüde artırmıştır.

3. Kuantum Bilgisayar Gelişimi: Kilometre Taşları ve Yol Haritaları



Şekil 1. *Kuantum Bilgisayar Qubit Gelişimi ve Q-Day Risk Zaman Çizelgesi*

3.1 Google Willow: 'Hata Eşiği Altına' İnmek

Google'ın Aralık 2024'te duyurduğu ve 2025 boyunca kapsamlı biçimde analiz edilen Willow çipi, 105 süperiletken qubit içermektedir. Willow'un temel başarısı, bir benchmark hesaplamasını klasik süperbilgisayarın 10^25 yılda tamamlayabileceği sürede yaklaşık beş

dakikada tamamlamasıdır. Ancak daha kritik olan başarı; qubit sayısı arttıkça hata oranının azalmasıdır — kuantum hesaplama tarihinin çözmeye çalıştığı temel sorunun üstesinden gelindiğinin göstergesi. UC Berkeley'den Fred Chong bu gelişmeyi '2025 hata düzeltme dalgasında bir tsunami' olarak nitelendirmiştir (techvorta.com, 2026).

3.2 IBM Yol Haritası: 2029 Hata Toleranslı Kuantum Hedefi

IBM, sektörün en ayrıntılı ve kamuoyuyla en açık paylaşılan yol haritasına sahip kuruluştur. Postquantum.com'un (2025) kapsamlı değerlendirmesine göre IBM'in 2025-2029 dönemi için kritik kilometre taşları şöyle sıralanmaktadır: 2026 — Kookaburra (1.386 qubitlik çok çipli işlemci, üç çipi birleştirerek 4.158+ qubitlik sistem). 2027-2028 arası: mantıksal qubitlerde ciddi ilerleme ve hata düzeltme etkinliğinin kanıtlanması. 2029: Dünyanın ilk büyük ölçekli hata toleranslı kuantum bilgisayarının teslimi hedefi.

IBM'in Kasım 2025'te duyurduğu deneysel Loon işlemcisi, 'hata toleranslı kuantum hesaplama için gereken tüm temel işlemci bileşenlerinin IBM tarafından ilk kez kanıtlandığını göstermektedir' (IBM, 2025). Bu duyuru, yalnızca ölçek değil mimari olgunluk açısından da kritik bir sinyaldir.

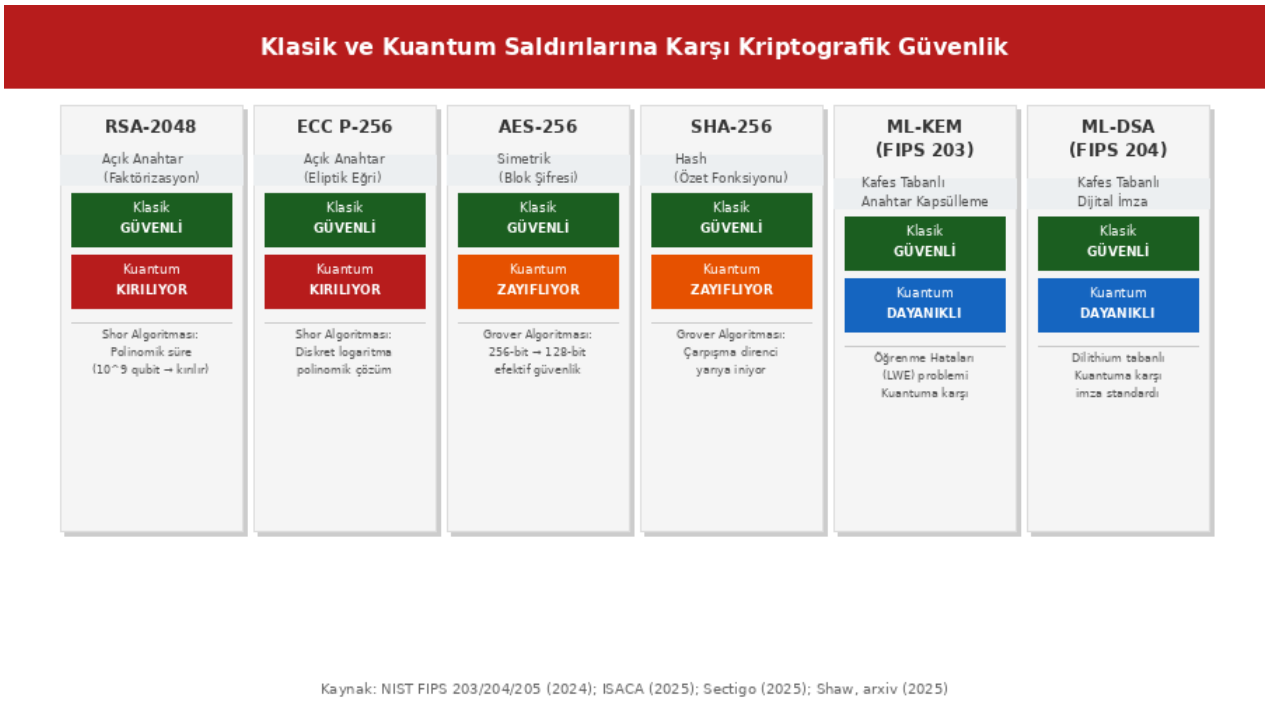
3.3 Q-Day: Ne Zaman Gerçekleşebilir?

Q-Day, kuantum bilgisayarların mevcut şifreli iletişimi kırabilecek ölçeğe ulaştığı gipotetik tarihi ifade etmektedir. Global Risk Institute'ün 2024 Kuantum Tehdit Zaman Çizelgesi Raporu (Mosca ve Piani), merkezi olasılık dağılımını 2033-2037 aralığına yerleştirmektedir. Qryptonic'in (2025) aktarımına göre IBM doğa makalesindeki hata düzeltme ilerlemeleri, gereken fiziksel qubit sayısını yüzde altmış azaltmakta ve RSA kırma kapasitesi için 2027 (±1 yıl) tahminine işaret etmektedir.

Bu farklı tahminlerin nedeni, hata düzeltme verimliliğindeki belirsizliğe bağlıdır: Mantıksal qubit başına kaç fiziksel qubit gerektiği, hata oranlarının nasıl ölçekleneceği ve kuantum ağ mimarisinin nasıl gerçekleşeceği henüz kesin değildir. Introtoquantum.org'un (2025) dürüst analizine göre: 'IBM 2024'te çok daha muhafazakâr bir adım atarak 2033'te yalnızca 100.000 qubit iddiasında bulundu — ancak bu makinenin hata düzeltme kapasitesini karşılaması bekleniyor.' Bu tablonun kilit mesajı şudur: Q-Day'in tam tarihi belirsiz olsa da geçiş için gereken süre değil.

burakbsn.com

4. Mevcut Kriptografiye Kuantum Tehdidi



Şekil 2. *Klasik ve Kuantum Saldırılarına Karşı Kriptografik Algoritmaların Durumu*

4.1 Shor Algoritması: Açık Anahtar Şifrelemesinin Sonu

RSA şifrelemesi, büyük sayıları asal çarpanlarına ayırmanın klasik bilgisayarlar için üstel süre gerektiren bir problem olduğu olgusuna dayanır. 2048 bitlik bir RSA anahtarının klasik yöntemlerle kırılması, evrenin yaşından uzun sürer. Shor algoritması bu denklemi köklü biçimde değiştirir: Yeterli qubit sayısına ve düşük hata oranına sahip bir kuantum bilgisayarda RSA-2048, kuantum Fourier dönüşümü ve dönem bulma mekanizmasıyla polinom zamanda kırılabilir.

Sectigo'nun (2025) özlü tanımıyla: 'Shor Algoritması, kuantum bilgisayarların tam sayıları klasik bir bilgisayardan çok daha verimli biçimde çarpanlarına ayırabileceğini göstermekte ve bu durum kuantum bilgisayarların RSA ve ECC'yi kırmada daha verimli olmasını sağlamaktadır.' ISACA'nın (2025) değerlendirmesine göre Shor'un hedef aldığı algoritmalar şunlardır: RSA (büyük sayı çarpanları), DSA, ECDSA ve Diffie-Hellman (diskret logaritma). Bu algoritmaların tamamı, günümüzün bankacılık, e-devlet, TLS/HTTPS ve dijital imza altyapısının temelini oluşturmaktadır.

4.2 Grover Algoritması: Simetrik Şifrelemeye Etkisi

Grover algoritması, yapılandırılmamış arama problemlerini O(√N) adımda çözen bir kuantum arama algoritmasıdır. Bu, n bitlik bir anahtarın kaba kuvvet (brute force) aranmasında sağlanan kareköklük hızlanmaya karşılık gelir. Shaw'ın (2025) arxiv çalışmasının ifadesiyle: 'Grover algoritması, simetrik ve hash tabanlı şemaların etkin güvenliğini azaltır. AES-128, 64 bit güvenliğe düşer; SHA-256 ise 128 bit güvenliğe iner.'

Pratikte bu bulgunun çıkarımı şudur: AES-256, Grover saldırısından sonra 128 bitlik etkin güvenliğini korumaktadır — bu hâlâ güvenli kabul edilmektedir. AES-128 ise 64 bite düşerek zayıflamaktadır. Bu nedenle post-kuantum geçiş planlarında simetrik şifreler için mevcut uzunlukları iki katına çıkarmak (AES-128 → AES-256) önerilen temel önlemlerden biridir. SHA-256'nın yerini SHA-384 veya SHA-512 alabilir; ancak RSA ve ECC'nin aksine simetrik şifreleme ve hash fonksiyonları için mevcut algoritmaların güncellenmesi yeterlidir — tamamen yeni bir algoritma ailesine geçiş gerektirmez.

4.3 Blockchain ve Kripto Para Birimleri Üzerindeki Etki

Blockchain teknolojisi, kriptografik anahtarlar ve dijital imzaların güvenliğine doğrudan bağımlıdır. Bitcoin ve Ethereum dahil büyük kripto para birimlerinin kullandığı ECDSA imza şeması, Shor algoritması karşısında son derece savunmasızdır. SEC'e sunulan bir politika belgesinde (Costa, 2025) şu uyarı yer almaktadır: 'Kriptografik açıdan önemli bir kuantum bilgisayar (CRQC), trilyon dolar değerindeki varlıkları koruyan temel güvenliği kırabilir ve sistemik riske, yıkıcı yatırımcı kayıplarına ve piyasa güveninin tamamen erozyonuna yol açabilir.'

Citi'nin Ocak 2026 tarihli raporuna göre Federal Rezerv'in Eylül 2025 çalışması, Şimdi Topla Sonra Çöz saldırısını incelemiş ve dağıtık defter ağları için veri mahremiyeti risklerini değerlendirmiştir.' Bu risk, kripto para ekosisteminin çözülmeden önce post-kuantum imza algoritmalarına geçmesi gerektiğine işaret etmektedir.

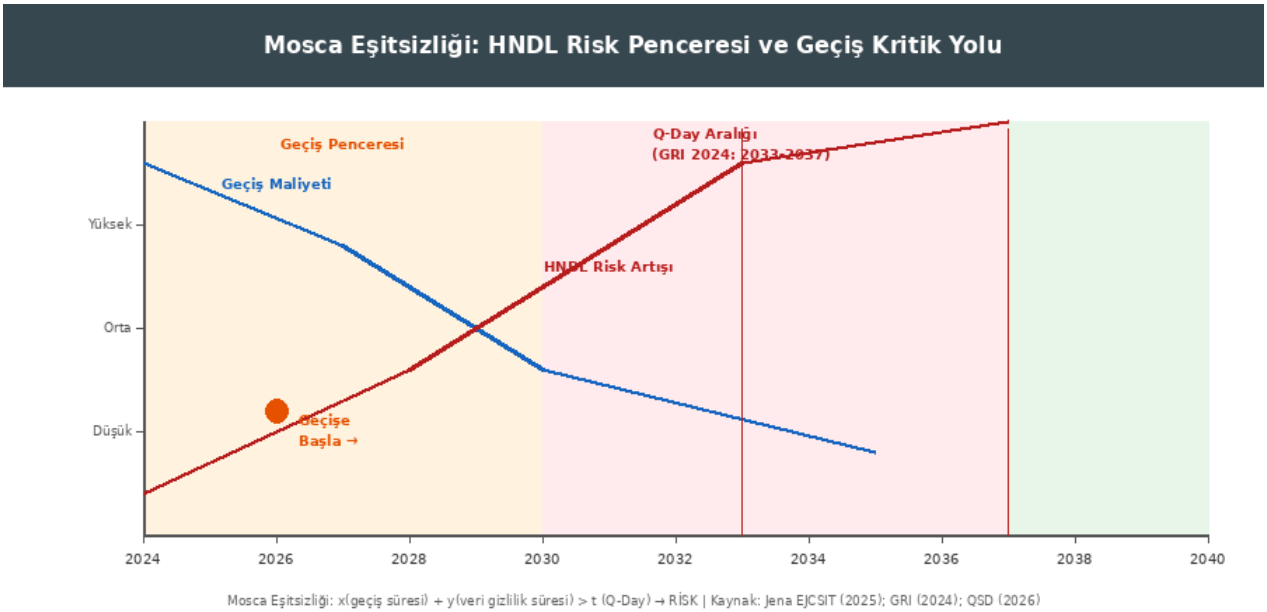
5. 'Şimdi Topla, Sonra Çöz': HNDL Tehdidi

5.1 HNDL Nasıl Çalışır?

'Harvest Now, Decrypt Later' (HNDL) stratejisi, kuantum tehdidin geleceğe ertelenmiş bir risk olmadığını; aksine, bugün aktif olarak gerçekleşen bir tehdit olduğunu ortaya koymaktadır. Kavram basittir: Bir ulusal tehdit aktörü veya gelişmiş kalıcı tehdit (APT) grubu, bugün şifrelenmiş trafiği — TLS el sıkışma kayıtlarını, VPN tünellerini, e-posta içeriklerini — toplar ve güvenli depolama alanlarında arşivler. Kuantum bilgisayarlar kriptografik eşiği aştığında bu arşiv çözülebilir hale gelir.

Kuantum Security Defence'in (2026) aktarımına göre Mosca eşitsizliği bu riski matematiksel olarak somutlaştırmaktadır: x (geçiş süresi) + y (verinin gizlilik gerektirdiği süre) > t (Q-Day) ise veri risk altındadır. Uygulamaya döküldüğünde: 2026'da PQC geçiş programı başlatan bir kuruluş, gerçekçi üç yıllık geçiş süresiyle (x=3) ve 15 yıllık gizlilik gerektiren verilerle (y=15) çalışıyorsa, verinin güvende olması için Q-Day'in 2044'ten önce gelmemesi gerekmektedir. GRI'nin 2024 raporu ise Q-Day'i 2033-2037 aralığına yerleştirmektedir. Bu veri güvende değildir.

burakolgun.com



Şekil 3. *Mosca Eşitsizliği: HNDL Risk Penceresi ve Geçiş Kritik Yolu (2024–2040)*

5.2 HNDL'nin Mevcut Kanıtları

HNDL saldırısının teorik değil pratik bir tehdit olduğuna dair kanıtlar giderek artmaktadır. Qryptonic'in (2025) ABD Kongre duruşmasına ilişkin analizine göre: 'Yabancı düşmanlar halihazırda 'şimdi çal, sonra çöz' stratejisi uyguluyorlar.' FBI ve NSA'nın kamuya açık bildirimleri, belirli ulus-devlet aktörlerinin büyük ölçekli şifrelenmiş veri toplama operasyonları yürüttüğünü doğrulamaktadır.

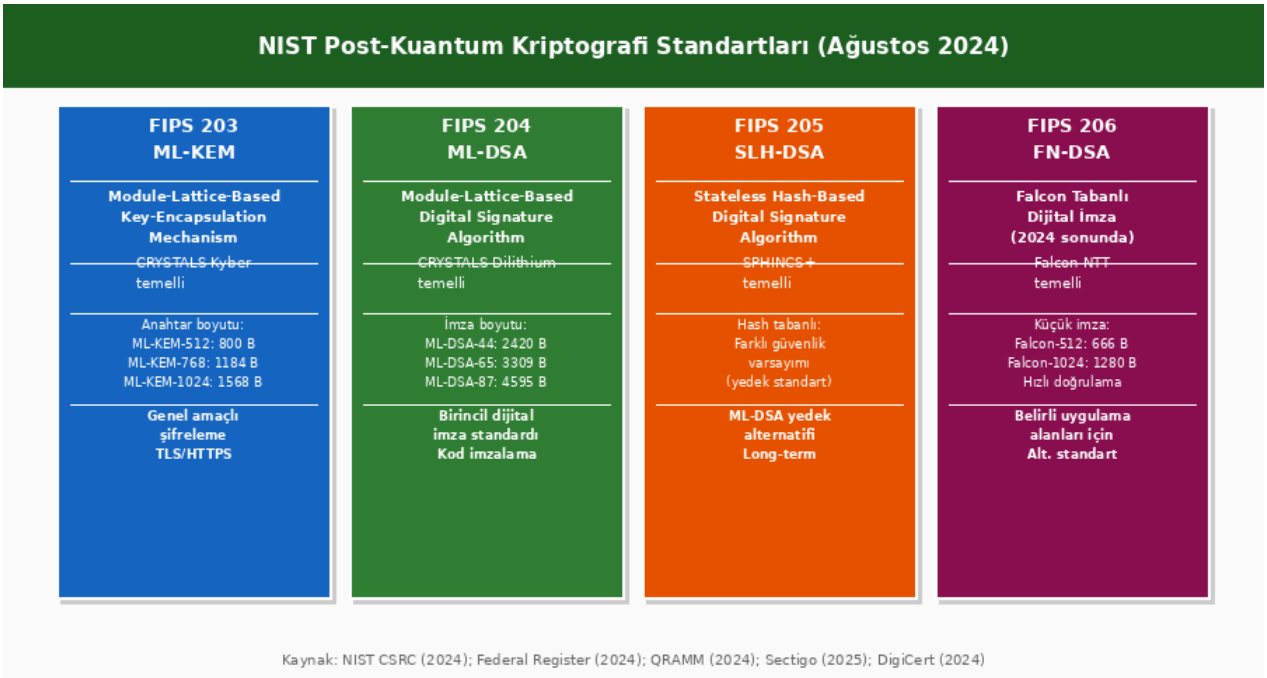
Mastercard'ın 2025 tarihli beyaz kitabında bu tehdit şöyle özetlenmektedir: 'HNDL'nin amacı, RSA/ECC bölümünü gelecekte bir CRQC kullanarak kırarak simetrik gizli anahtarları ortaya çıkarmak ve ardından verilerin şifresini çözmektir.' Bu anlamda HNDL, TLS oturumlarının özellikle tehlikeli bir hedef olduğunu ortaya koymaktadır: TLS el sıkışma aşamasında kullanılan asimetrik şifrelemenin gelecekte kırılması, o oturumda iletilen tüm içeriğin ifşasına neden olabilir.

5.3 HNDL'ye Karşı Tedbirler: Hibrit TLS ve İleri Gizlilik

HNDL tehdidine karşı iki temel teknik önlem öne çıkmaktadır. Forward Secrecy (İleri Gizlilik), her oturum için ayrı geçici anahtar kullanılmasını sağlar; bu sayede geçmiş oturumların uzun vadeli anahtarların ele geçirilmesiyle çözülmesi engellenir. Ancak ileri gizlilik, kuantum sonrası dönemde kullanılan anahtar değişim mekanizması kuantuma karşı savunmasızsa yetersiz kalır.

Kuantum Security Defence'in (2026) önerisi şöyledir: 'Aktif iletişimler için hibrit anahtar değişimi: Geçiş süresince hem klasik (ECDH) hem post-kuantum (ML-KEM) anahtar değişimini birlikte kullanan hibrit TLS, her iki sisteme karşı da güvenlik sağlar.' Bu yaklaşım, bir tarafın yalnızca klasik kriptografi kullandığı ortamlarda geriye dönük uyumluluk sorununu da çözer.

6. NIST Post-Kuantum Kriptografi Standartları



Şekil 4. *NIST Post-Kuantum Kriptografi Standartları: FIPS 203, 204, 205 ve Planlanan FIPS 206*

6.1 Sekiz Yıllık Standardizasyon Süreci

NIST'in post-kuantum kriptografi standardizasyon projesi, 2016'da küresel çağrıyla başladı ve sekiz yıl süren, sanayi, akademi ve hükümetlerin katılımıyla yürütülen kapsamlı bir değerlendirme sürecini kapsadı. Başlangıçta 82 başvuru alınan süreçte, güvenlik analizleri, performans değerlendirmeleri ve kriptografik kırılma girişimlerinden oluşan birden fazla eleme turu gerçekleştirildi. Federal Register'ın (2024) resmi duyurusuna göre FIPS 203, FIPS 204 ve FIPS 205 standartları 14 Ağustos 2024'te yürürlüğe girdi.

6.2 FIPS 203 — ML-KEM: Anahtar Kapsülleme Standardı

FIPS 203, Module-Lattice-Based Key-Encapsulation Mechanism (ML-KEM) standardını tanımlar. CRYSTALS-Kyber algoritmasından türetilen ML-KEM, RSA ve ECDH'nin yerine geçmesi öngörülen birincil anahtar değişim mekanizmasıdır. QRAMM'ın (2024) değerlendirmesine göre üç güvenlik düzeyi sunulmaktadır: ML-KEM-512 (AES-128 eşdeğeri güvenlik, en küçük anahtar boyutu), ML-KEM-768 (AES-192 eşdeğeri, dengeli seçenek) ve ML-KEM-1024 (AES-256 eşdeğeri, en yüksek güvenlik).

NSA'nın CNSA 2.0 kılavuzu, ulusal güvenlik sistemleri için ML-KEM-1024 kullanımını zorunlu kılmakta ve 2030'a kadar tam geçişi öngörmektedir. ML-KEM'in temel matematiksel zorluğu Modüler Kafes Öğrenme (Module-LWE) problemidir: Hem klasik hem kuantum hesaplamaya karşı dayanıklılığı, bilinmezlik probleminin bu konfigürasyonda polinom değil üstel hesaplama gerektirmesine dayanır.

6.3 FIPS 204 — ML-DSA: Dijital İmza Standardı

FIPS 204, Module-Lattice-Based Digital Signature Algorithm (ML-DSA) standardını tanımlar. CRYSTALS-Dilithium'dan türetilen ML-DSA, ECDSA ve RSA-PSS'nin yerini alması öngörülen birincil dijital imza algoritmasıdır. Kod imzalama, sertifika imzalama, belge imzalama ve kimlik doğrulama protokollerinde kullanım için NIST'in önerilen varsayılan standardıdır. Üç parametre kümesi mevcuttur: ML-DSA-44 (küçük imza boyutu, daha hızlı), ML-DSA-65 (dengeli) ve ML-DSA-87 (en yüksek güvenlik, 4.595 baytlık imza boyutu).

Kuantum Security Defence'in (2026) tespitine göre ML-DSA'nın matematiksel temeli, ML-KEM ile aynı kafes problemlerini kullanan 'Fiat-Shamir with Aborts' yaklaşımıdır: Anahtar üretimi yapılandırılmış kafeslerden genel-özel anahtar çifti oluşturur. İmzalama sürecinde, kabul edilebilir bir imza elde edilene kadar süreç tekrarlanabilir. Doğrulama, genel anahtarla imzanın özgünlüğünü denetler.

6.4 FIPS 205 — SLH-DSA: Hash Tabanlı Yedek İmza

FIPS 205, Stateless Hash-Based Digital Signature Algorithm (SLH-DSA) standardını tanımlar ve SPHINCS+'dan türetilmiştir. ML-DSA'dan temel farkı, güvenlik varsayımının farklı matematiksel temele dayanmasıdır: Hash fonksiyonlarının güvenliğine dayanan SLH-DSA, kafes tabanlı algoritmaların gelecekte zayıf bir yanının keşfedilmesi halinde bir yedek alternatifi oluşturmaktadır. DigiCert'in (2024) aktarımına göre SLH-DSA, 'diğer algoritmalara göre daha büyük ve daha yavaştır' — bu durum onu performansın kritik olmadığı uzun vadeli arşivleme ve kod imzalama için uygun kılmaktadır.

7. Kafes Tabanlı Kriptografi: Matematiksel Temeller

7.1 Kafes Problemi Nedir?

Kafes kriptografisi, yüksek boyutlu kafeslerdeki matematiksel problemlerin zorluğuna dayanmaktadır. Geometrik olarak bir kafes, bir vektör uzayında n adet doğrusal bağımsız vektörden oluşan düzenli bir nokta ızgarasıdır. Bu problemlerin iki temel formu, kafes kriptografisinin matematiksel zeminini oluşturur.

Shortest Vector Problem (SVP): Bir kafeste sıfır olmayan en kısa vektörü bulmak. Boyut arttıkça bu problem hem klasik hem kuantum bilgisayarlar için üstel zorlukta büyümektedir.

Learning With Errors (LWE): Kasıtlı olarak küçük hata eklenen doğrusal denklem sistemini çözmek. Regev (2005) tarafından geliştirilen LWE problemi, ML-KEM ve ML-DSA'nın temelini oluşturmaktadır. Modüler kafes versiyonu (Module-LWE) performans avantajı sağlarken güvenlik düzeyini korumaktadır.

7.2 Neden Kuantuma Karşı Dayanıklı?

RSA ve ECC'nin aksine, kafes problemleri Shor algoritmasından yararlanamaz: Shor, çarpanlarına ayırma ve ayrık logaritma problemlerini çözmek için Kuantum Fourier Dönüşümü

burakolgun.com

kullanır; ancak SVP ve LWE bu matematiksel yapıya sahip değildir. Grover aramasından da kayda değer bir kareköklük avantajı elde edilememektedir.

NIST'in sekiz yıllık değerlendirme süreci, aktif saldırı araştırmaları dahil olmak üzere kapsamlı kriptanaliz gerçekleştirmiştir. Fractal.ai'nin (2024) özetine göre: 'RSA'nın Shor algoritmasıyla kırılabilmesinin aksine, NIST onaylı PQC algoritmaları kuantum bilgisayarların bilinen kapasitelerine karşı dirençlidir. Bununla birlikte performans ve depolama açısından ödünleşimler mevcuttur.'

7.3 Performans Karşılaştırması: RSA vs ML-KEM

Post-kuantum algoritmalar, RSA ile karşılaştırıldığında farklı performans profilleri sergiler:

Tablo 1. *RSA-2048 ve ML-KEM Anahtar Boyutu ile Performans Karşılaştırması*

Parametre	RSA-2048	ML-KEM-512	ML-KEM-768	ML-KEM-1024
Güvenlik Düzeyi	~112 bit	128 bit	192 bit	**256 bit**
Genel Anahtar Boyutu	256 bayt	800 bayt	1.184 bayt	1.568 bayt
Şifreli Metin Boyutu	256 bayt	768 bayt	1.088 bayt	1.568 bayt
Kuantum Güvenliği	**KIRILIYOR**	Güvenli	Güvenli	**Güvenli**
Anahtar Üretim Hızı	~1.600 op/s	~800.000 op/s	~550.000 op/s	~400.000 op/s

Not. Kaynak: QRAMM (2024); NIST FIPS 203 (2024); Quantum Security Defence (2026); ISACA (2025).

8. Kritik Altyapıların PQC Geçişi

8.1 Kripto Çevikliği (Crypto-Agility) Kavramı

Kripto çevikliği (crypto-agility), bir sistemin kriptografik algoritmalarını geniş çaplı mimari değişiklik gerektirmeksizin güncelleyebilme kapasitesini tanımlar. Bu kavram, post-kuantum geçişin merkezine oturmuştur: Bir sistemin PQC algoritmalarına geçişi, bunları izole biçimde değiştirme kapasitesini gerektirmektedir. IBM'in çerçevesine göre kripto çevikliği; kriptografik envanteri, güncellenebilir modüler mimariyi, agnostik protokolleri ve koordineli güncelleme süreçlerini kapsamaktadır (Shaw, 2025).

ISACA'nın (2025) vurguladığı pratik zorluk şudur: 'Mevcut kriptografik standartları yeni post-kuantum standartlarıyla değiştirmek, dünya çapındaki bağlantısallık ve yerleşik protokoller nedeniyle önemli teknik güçlükler doğurmaktadır.' Bu durum, tüm sistemlerin aynı anda güncellenmesi yerine aşamalı, riske dayalı bir geçiş stratejisini zorunlu kılmaktadır.

8.2 Bankacılık ve Finans Sektörü

Bankacılık sektörü, hem yüksek değerli verilerinin uzun süreli gizlilik gerektirmesi hem de gerçek zamanlı işlem altyapısının kriptografiye derin bağımlılığı nedeniyle özellikle savunmasız bir konumdadır. Citi'nin (2026) raporuna göre İsrail Merkez Bankası Ocak 2025'te 'kuantum hesaplama kapasitelerinden kaynaklanan siber riskler için bankacılık sistemi

hazırlığını' değerlendiren bir kılavuz yayımlamıştır. Aynı rapor, Federal Rezerv'in Eylül 2025 tarihli çalışmasının dağıtık defter ağları için HNDL riskini incelediğini aktarmaktadır.

Mastercard, 2025 tarihli beyaz kitabında kurumsal geçiş metodolojisini kapsamlı biçimde ele almıştır. Risk değerlendirmesi, kriptografik envanter, SoA benzeri uygulanabilirlik bildirgeleri ve geçiş önceliklendirmesi bu metodolojinin temel bileşenlerini oluşturmaktadır.

8.3 Hükümet ve e-Devlet Sistemleri

ABD Beyaz Sarayı, Ocak 2025'te 'Ülkenin Siber Güvenliğinin Güçlendirilmesi ve Teşvik Edilmesine İlişkin Yürütme Emri'ni yayımladı; bu emir PQC geçişini federal bir öncelik olarak tanımlamaktadır. AB Komisyonu, Haziran 2025'te post-kuantum kriptografiye geçiş için 'Koordineli Uygulama Yol Haritası' yayımlamış; Ekim 2025'te ise Kuantum Yasası hazırlıklarına ilişkin katkı talep etmiştir (Citi, 2026).

NIST'in kendi zaman çizelgesi şöyledir: 2035 yılına kadar kuantuma karşı savunmasız algoritmaları standartlardan kaldırmayı planlamakta; yüksek riskli sistemlerin çok daha erken geçişini öngörmektedir (NIST IR 8547, 2024). NSA'nın CNSA 2.0 kılavuzu, yazılım ve donanım yazılımı imzalamasında 'hemen geçiş başlayın' direktifini verirken eski altyapı için 2033'e kadar geçiş süresini tanımaktadır.

8.4 PKI ve Sertifika Altyapısı

Açık Anahtar Altyapısı (PKI), internet güvenliğinin temel omurgasını oluşturmaktadır. Sertifika Otoriteleri (CA), web sunucuları, e-posta şifreleme, kod imzalama ve kimlik doğrulama sistemlerinin tamamı PKI'ya bağımlıdır. Sectigo'nun (2025) tespitine göre: 'PKI, yalnızca iki standartlaştırılmış algoritma olan RSA ve ECC'ye dayanmaktadır. Kuantum bilgisayarlar bu dijital güveni tehdit etmektedir.'

PKI geçişinin özellikle zorlayıcı boyutu, kök sertifika otoritelerinin güncellenmesidir. Kök CA sertifikalarının ömrü genellikle 25-30 yıldır; bu sertifikaların imzalama algoritmaları ECDSA veya RSA ise tüm sertifika hiyerarşisi savunmasız hale gelir. DigiCert'in (2024) değerlendirmesine göre NSA, yazılım ve donanım yazılımı imzalaması için 'hemen geçiş başlayın' direktifi vermektedir.

9. PQC Geçiş Planlaması: Metodoloji ve Araçlar

9.1 Kriptografik Envanter (CBOM)

Post-kuantum geçişin ilk adımı, kuruluşun mevcut kriptografik kullanımını sistematik biçimde envanterlemektir. Kriptografi Malzeme Listesi (Cryptography Bill of Materials — CBOM), bu amaç için geliştirilen bir çerçevedir. Shaw'ın (2025) çalışmasına göre CBOM, 'yazılım bağımlılık graflarını, ikili dosya analizini ve ağ denetimini' kapsayan çok katmanlı bir kriptografik keşif metodolojisini içermektedir.

Bir CBOM; kullanılan tüm algoritmaları (RSA, ECDSA, AES vb.), bu algoritmaların kullanıldığı yazılım bileşenlerini ve sürümlerini, anahtar boyutlarını, kullanım bağlamını

burakoguz.com

(şifreleme, imzalama, anahtar değişimi) ve değiştirme önceliğini belgelemelidir. NIST NCCoE SP 1800-38, bu metodolojinin referans rehberini oluşturmaktadır.

9.2 Risk Önceliklendirme Matrisi

PQC geçişinde risk önceliklendirmesi için şu çerçeve uygulanabilir:

- **Öncelik 1 — Hemen Geçiş:** Kök CA sertifikaları ve kod imzalama anahtarları. Bu uzun ömürlü kimlik bilgileri, HNDL saldırısında tüm sertifika zincirini etkiler.
- **Öncelik 2 — Kısa Vadeli (1-2 yıl):** TLS/HTTPS sunucu sertifikaları, API kimlik doğrulama, belge imzalama. Aktif iletişimlerde hibrit TLS önerilebilir.
- **Öncelik 3 — Orta Vadeli (2-3 yıl):** İç ağ şifreleme, VPN altyapısı, veritabanı şifreleme anahtarları.
- **Öncelik 4 — Uzun Vadeli (3-5 yıl):** Gömülü sistemler, IoT cihazları ve donanım yazılımı. Donanım değişim döngüleriyle koordineli geçiş planlanmalıdır.

9.3 Yasal ve Uyumluluk Gereksinimleri

PQC geçişinin hukuki boyutu hızla gelişmektedir. ABD'de federal kurumlar için NIST IR 8547 zaman çizelgeleri bağlayıcıdır. AB'de NIS2 Direktifi ve yaklaşan Kuantum Yasası, kritik altyapı operatörleri için geçiş yükümlülükleri getirecektir. Citi'nin (2026) raporuna göre AB Komisyonu'nun Haziran 2025 yol haritası, üye devletler için koordineli geçiş takvimini belirlemektedir.

Türkiye bağlamında BDDK'nın (Bankacılık Düzenleme ve Denetleme Kurumu) ve BTK'nın (Bilgi Teknolojileri ve İletişim Kurumu) bu alandaki düzenleyici adımlarını takip etmesi kritik önem taşımaktadır. Bilgi ve İletişim Güvenliği Rehberi kapsamında kuantum güvenli kriptografi gereksinimlerinin tanımlanması, Türkiye'nin uluslararası uyum sürecindeki stratejik gündem maddelerinden biri olmalıdır.

10. Türkiye'nin Kuantum Stratejisi ve Kriptografik Hazırlık

10.1 TOBB ETÜ İlk Kuantum Bilgisayar

Türkiye, Kasım 2024'te TOBB Ekonomi ve Teknoloji Üniversitesi (TOBB ETÜ) tarafından geliştirilen ilk yerli kuantum bilgisayarını kamuoyuyla paylaştı. Quantumzeitgeist'ın (2024) aktarımına göre 'TOBB ETÜ, altyapısı sürekli gelişimi destekleyecek şekilde tasarlanmış bir kuantum ekosistemi oluşturmayı, küresel rekabetçi avantaj için girişimlerin yerli kuantum donanımı ve bileşenleri geliştirmesine yardımcı olmayı hedeflemektedir.'

Türkiye'nin bu hamlesi, kuantum teknolojisini yalnızca kullanan değil üreten ülkeler arasında yer alma hedefini yansıtmaktadır. Cumhurbaşkanı Erdoğan, bu konuda şunları söylemiştir: 'Bu kritik gelişmeyle Türkiye'yi küresel sahnede kilit bir oyuncu olarak konumlandırmayı hedefliyoruz.' Planlanan süperiletken çip üretim tesisi, yüksek kapasiteli işlemciler üretiminin önünü açacaktır.

burakbun.com

10.2 TÜBİTAK BİLGEM UEKAE: Kuantum Kriptografi Altyapısı

TÜBİTAK BİLGEM UEKAE, Türkiye'nin kuantum bilgi güvenliği araştırmalarındaki kilit kurumudur. BİLGEM'in web sitesine (2023) göre UEKAE, kuantum kriptografi, kuantum rastgele sayı üreteci (QRNG), tek fotonlu kuantum anahtar dağıtımı (QKD) ve kuantum hayalet görüntüleme alanlarında ulusal ve uluslararası projeler yürütmüştür. 2023 yılı başında Kuantum Teknolojileri Bölümü kurularak bu alandaki çalışmalar kurumsal bir yapıya kavuşturulmuştur.

Savunma sektöründe ise SSB (Savunma Sanayii Başkanlığı) Ağustos 2024'teki Savunma Sanayii İcra Komitesi toplantısında Kuantum Teknolojileri Geliştirme Merkezi kurulmasını onaylamıştır. Herdem hukuk bürosunun (2025) aktarımına göre bu merkez 'kuantum iletişim, şifreleme, tespit ve ileri hesaplama' alanlarında faaliyet yürütecektir.

10.3 Uluslararası İş Birliği: QuantERA 2025

TÜBİTAK, QuantERA 2025 Çağrısı kapsamında Türkiye'nin uluslararası kuantum teknolojileri araştırma projeleriyle iş birliğini hızlandıracak. QuantERA III Konsorsiyumu'nun başlattığı bu çağrı, kuantum fenomenleri ve kaynakları ile uygulamalı kuantum bilimi konularında sınır ötesi iş birliğini teşvik etmektedir. Türkiye Today'in (2025) aktarımına göre proje önerileri iki konu başlığında yer alabilmekte; kurumsal pay üst limiti olarak en fazla 650.000 TL talep edilebilmektedir.

10.4 Türkiye'nin PQC Geçiş Öncelikleri

Türkiye, küresel standartlara paralel bir PQC geçiş gündemini hayata geçirme konumundadır. Kritik öncelikler şu başlıklar altında ele alınabilir: e-Devlet ve Türkiye Cumhuriyet Kimlik Numarası (TC Kimlik No) tabanlı kimlik doğrulama sistemleri, yüksek gizlilik gerektiren devlet yazışmaları, savunma haberleşme altyapısı ve finansal sistem mesajlaşması (SWIFT, bankalararası iletişim).

Türkiye'nin BDDK düzenlemelerinin kuantum güvenliğini kapsaması, Ulusal Siber Güvenlik Stratejisi'nin PQC geçiş takvimini içermesi ve BTK'nın TLS/PKI altyapısı için PQC geçiş kılavuzu yayımlaması, bu alanda atılması gereken düzenleyici adımların başında gelmektedir. BİLGEM UEKAE'nin post-kuantum algoritma test ve sertifikasyon platformu kurması da ulusal yetenek açısından stratejik önem taşır.

11. Sektörel Etki Değerlendirmesi

11.1 Sağlık Sektörü ve Tıbbi Veri Gizliliği

Sağlık verisinin gizlilik ömrü özellikle uzundur: Bir hastanın tıbbi geçmişi onlarca yıl boyunca gizli tutulması gereken kişisel veri kapsamına girer. Mosca eşitsizliği açısından değerlendirildiğinde 2024 yılında oluşturulan bir sağlık kaydının 30-40 yıl gizlilik koruması gerektirmesi, HNDL riskinin en yüksek olduğu veri kategorilerinden birini oluşturmaktadır. ABD'de HIPAA, AB'de GDPR'ın gerektiği gibi uygulananilmesi için sağlık kuruluşlarının kriptografik altyapılarını PQC'ye geçirmesi zorunludur.

bilgiguvenligi.com

11.2 Elektrik Şebekeleri ve Kritik Altyapı

Elektrik şebekeleri, su sistemleri ve ulaşım altyapısı operatörel teknoloji (OT) sistemleri kullanmakta; bu sistemlerin güncellenmesi ve yamalı tutulması son derece güçtür. Çoğu OT cihazı on yıl veya daha uzun ömrüyle konumlandırılmış olup kriptografik yükseltme için tasarlanmamıştır. DHS'in (tarihsiz) değerlendirmesine göre: 'Mevcut kriptografik standartların yeni post-kuantum standartlarıyla değiştirilmesi, dünya çapındaki bağlantısallık ve yerleşik protokoller nedeniyle önemli teknik güçlükler doğurmaktadır.'

11.3 Akıllı Sözleşmeler ve DeFi

Merkezi Olmayan Finans (DeFi) ekosistemi ve akıllı sözleşmeler, ECDSA imzasına derin bir bağımlılık taşımaktadır. Ethereum'da cüzdan güvenliği, işlem imzalama ve akıllı sözleşme kimlik doğrulaması ECDSA tabanlıdır. Ethereum Foundation, ECDSA'dan post-kuantum imzaya geçiş için araştırmalar sürdürmektedir; ancak mevcut altyapının geriye dönük uyumluluk gereksinimleriyle PQC'ye geçişi son derece karmaşık bir mühendislik sorununu oluşturmaktadır.

12. 2025-2026 Döneminin Öne Çıkan Gelişmeleri

12.1 Kuantum Anahtar Dağıtımı (QKD): Fiziksel Güvenlik

Post-kuantum kriptografi (yazılım tabanlı) ve Kuantum Anahtar Dağıtımı (Quantum Key Distribution — QKD, donanım tabanlı), birbirini tamamlayan iki farklı güvenlik yaklaşımını temsil etmektedir. QKD, kuantum mekaniğinin temel yasalarına dayanan fiziksel güvenlik sunar: Gizlice dinleme girişimi ölçüm bozukluğuna yol açarak tespit edilebilir hale gelir. Çin'in dünya çapındaki en geniş QKD ağı olan Beijing-Shanghai omurgası, 2022'de 2.000 km uzunluğa ulaşmıştır.

Türkiye'de TÜBİTAK BİLGEM UEKAE, tek fotonlu QKD sistemleri üzerine araştırmalarını sürdürmektedir. Kuantum güvenli iletişim için uzun vadeli strateji; PQC (yaygın dağıtım için uygun maliyetli) ve QKD'nin (kritik bağlantılar için) hibrit kullanımına dayanmaktadır.

12.2 McKinsey'nin 100 Milyar Dolar Kuantum Teknoloji Piyasa Öngörüsü

ABD Kongre duruşmasında aktarılan McKinsey analizi, kuantum teknoloji pazarının 2040'a kadar 100 milyar doların üzerine çıkabileceğini öngörmektedir (Qryptonic, 2025). Bu büyüme, kuantum güvenli siber güvenlik pazarının stratejik önemini ortaya koymaktadır. Citi'nin (2026) analizine göre ise 2024'te kuantum teknolojisine yapılan yatırımlar yüzde elli büyüyerek yaklaşık 2 milyar dolara ulaşmış; hükümetler ise 3,1 milyar dolar harcamıştır.

12.3 Yapay Zeka ve Kuantum: Sinerjiler ve Riskler

Yapay zeka ve kuantum bilgisayarların kesişimi çift yönlü etki doğurmaktadır. Olumlu yönde: Kuantum makine öğrenmesi (QML) algoritmaları, belirli AI görevlerinde üstel hızlanma

burakgun.com

potansiyeli sunmaktadır. Olumsuz yönde: LLM tabanlı araçlar, kriptografik zayıflıkları otomatik olarak tespit eden yeni araç setleri geliştirmekte (Shaw, 2025); bu durum eski kriptografik uygulamaların keşfedilme ve istismar edilme riskini artırmaktadır. 2030'dan itibaren ise yapay zeka destekli kuantum hata düzeltme sistemleri Q-Day takvimini öne çekebilir.

13. Kurumsal Hazırlık Çerçevesi ve Öneriler

13.1 PQC Hazırlık Değerlendirme Modeli

Bir kuruluşun PQC hazırlık düzeyini değerlendirmek için beş olgunluk kademesi önerilmektedir:

- **Kademe 1 — Farkındalık:** Üst yönetim ve BT ekipleri kuantum tehdidin farkında değil. PQC planlaması yok.
- **Kademe 2 — Keşif:** Kriptografik envanter çalışması başlatıldı. Tehdit değerlendirmesi yapılıyor. CBOM oluşturuldu.
- **Kademe 3 — Planlama:** Risk önceliklendirme tamamlandı. Geçiş yol haritası hazırlandı. Bütçe tahsisi yapıldı.
- **Kademe 4 — Uygulama:** Yüksek öncelikli sistemlerde PQC geçişi başladı. Hibrit kriptografi devreye alındı. İç denetim başlatıldı.
- **Kademe 5 — Olgunluk:** Tüm kritik sistemler PQC'ye geçmiş. Kripto çevikliği tamamen hayata geçirilmiş. Sürekli izleme aktif.

13.2 Pratik Öneriler: 12 Aylık Hızlı Başlangıç Planı

Kuruluşlar için önerilen 12 aylık öncelikli eylem takvimi:

- **İlk 1-3 ay — Kriptografik Envanter:** Tüm yazılım, donanım ve ağ bileşenlerindeki kriptografik kullanımların CBOM çerçevesinde belgelenmesi.
- **2-4. ay — Risk Değerlendirmesi:** Mosca eşitsizliği uygulanarak veri gizlilik gereksinimleri ve geçiş süresi hesaplanması. Q-Day senaryoları modellenmesi.
- **3-6. ay — Önceliklendirme ve Yol Haritası:** Yüksek risk varlıklarının belirlenmesi ve geçiş takviminin NIST IR 8547 rehberi doğrultusunda oluşturulması.
- **6-9. ay — Pilot Uygulama:** ML-KEM veya ML-DSA'nın düşük riskli test ortamında pilot uygulaması. Hibrit TLS yapılandırması.
- **9-12. ay — Kademeli Geçiş:** Öncelik 1 varlıklarının (kök CA, kod imzalama) geçişinin tamamlanması. İç denetim ve belgeleme.

Tablo 2. *Mevcut ve Post-Kuantum Kriptografik Algoritma Eşleşme Tablosu*

Kullanım	Mevcut (Risk)	PQC Geçiş Hedefi	NIST / NSA Direktifi
Anahtar Değişimi	ECDH, RSA-OAEP	ML-KEM (FIPS 203)	NSA CNSA 2.0: ML-KEM-1024 zorunlu (NSS için)

kurdogan.com

Kullanım	Mevcut (Risk)	PQC Geçiş Hedefi	NIST / NSA Direktifi
Dijital İmza	ECDSA, RSA-PSS	ML-DSA (FIPS 204)	NIST: Birincil standart; hemen geçiş önerisi
İmza (Yedek)	RSA-PKCS#1v1.5	SLH-DSA (FIPS 205)	ML-DSA kırılırsa yedek; uzun vadeli arşiv
Simetrik Şifreleme	AES-128	AES-256	Anahtar uzunluğunu 2× artır; değişim gerekmez
Hash	SHA-256	SHA-384 / SHA-512	256→384/512 uzatma; Grover koruması
TLS El Sıkışma	ECDHE + RSA/ECDSA	Hibrit: ECDHE+ML-KEM	Geçiş döneminde hibrit TLS önerilir (IETF RFC)
PKI Sertifikası	RSA-2048/ ECDSA P-256	ML-DSA + Hibrit Sert.	DigiCert, Entrust: Hibrit sertifika geçiş ürünleri

Not. Kaynak: NIST FIPS 203/204/205 (2024); NSA CNSA 2.0 (2022); DigiCert (2024); Quantum Security Defence (2026).

14. Adli Bilişim ve Hukuki Boyutlar

14.1 Dijital İmzanın Hukuki Geçerliliği Riski

Dijital imzanın hukuki geçerliliği, kriptografik güvenilirliğe dayanır. Türkiye'de 5070 sayılı Elektronik İmza Kanunu, güvenli elektronik imzanın hukuki sonuçlarını düzenlemekte; bu imzalar RSA veya ECDSA tabanlı sertifikalar üzerine inşa edilmektedir. Q-Day sonrasında bu imzaların sahtecilik karşısındaki koruması ortadan kalkacaktır: Bir kuantum bilgisayara sahip aktör, özel anahtar olmaksızın RSA tabanlı dijital imzayı taklit edebilir.

Bu tehdidin hukuki boyutu şöyledir: Bugün geçerli olan noterde onaylı dijital imzalar, e-ticaret sözleşmeleri ve resmi yazışmalar, Q-Day sonrası ortamda güvenilirlik sorgulanabilir hale gelecektir. Türkiye'nin 5070 sayılı Kanun kapsamında güvenli elektronik imza standartlarının post-kuantum algoritmaları kapsayacak biçimde güncellenmesi yasal bir zorunluluğa dönüşecektir.

14.2 Şifreli Delil ve Müsadere Sorunu

Kuantum bilgisayarların şifre kırma kapasitesinin artması, hukuki delil bütünlüğü açısından çift yönlü bir etki doğuracaktır. Olumlu yön: Yargılama süreçlerinde şifrelenmiş verilerin erişilebilir kılınması, bazı suç soruşturmalarını kolaylaştırabilir. Olumsuz yön: Yasal muhafaza zincirine (chain of custody) alınmış şifrelenmiş deliller, kuantum bilgisayarlarla değiştirilip değiştirilmediğinin tespit edilmesi zorlaşabilir. Adli bilişimde bütünlük kontrolü için kullanılan kriptografik hash değerlerinin kuantuma karşı dayanıklı algoritmalarla (SHA-384, SHA-512) hesaplanması kritik öneme sahip olacaktır.

14.3 Yeni Bir Hukuki Kategori: Kuantum Caydırma

Kuantum bilgisayarların şifre kırma kapasitesinin devlet aktörlerinin eline geçmesi, uluslararası hukuk açısından yeni soruları beraberinde getirmektedir. NSA ve benzeri istihbarat birimlerinin kuantum kapasiteyi şifreli iletişimlere karşı kullanması, hangi koşullarda hukuka

burakolgun.com

uygun kabul edilir? HNDL kapsamında önceden toplanmış verilerin kuantum araçlarla çözülmesi, uluslararası insancıl hukukun gözetim sınırlarını nasıl etkiler? Bu sorular, henüz yanıtlanmamış uluslararası kamu hukuku meselelerini oluşturmaktadır.

15. Sonuç

1994'te Peter Shor'un tanımladığı algoritma, otuz yıl boyunca büyük ölçüde teorik bir tehdit olarak kaldı. 2024'te bu tablo değişti: Google Willow'un 'hata eşiğinin altına' indiğini kanıtlaması, IBM'in 2029 hata toleranslı kuantum bilgisayar hedefini sürdürmesi ve GRI'nin Q-Day'i 2033-2037 aralığına yerleştirmesi, artık teorik değil mühendislik meselesini tartışıyoruz göstermektedir.

NIST'in Ağustos 2024'te yayımladığı FIPS 203, 204 ve 205 standartları, dijital güvenlik altyapısının post-kuantum çağa geçişi için teknik temel taşları sağlamaktadır. ML-KEM, ML-DSA ve SLH-DSA algoritmaları; RSA, ECDSA ve Diffie-Hellman'ın yerini alacak, kuantum saldırılarına karşı dayanıklı matematiksel zeminlere sahip algoritmalarıdır.

HNDL tehdidi, bu geçişin kritik aciliyetini ortaya koymaktadır: Teknik geçiş için gereken süre ve veri gizlilik gereksinimleri toplamı Q-Day'i zaten aşıyor olabilir. Kuruluşlar için bu sonuç nettir: Kriptografik envanter çıkarmak, HNDL risk penceresini hesaplamak ve yüksek öncelikli sistemlerde PQC geçişini başlatmak, bu on yılın en kritik bilgi güvenliği yatırımını oluşturmaktadır.

Türkiye bağlamında TOBB ETÜ'nün ilk yerli kuantum bilgisayar çalışması ve TÜBİTAK BİLGEM UEKAE'nin kuantum kriptografi araştırmaları, ülkenin bu alanda kapasitesini geliştirmekte olduğunu göstermektedir. Ancak ulusal düzenleyici çerçevenin — BDDK, BTK ve Bilgi Güvenliği Rehberi kapsamında — PQC geçiş gereksinimlerini tanımlaması, kamu ve özel sektörün bu geçişi koordineli biçimde gerçekleştirmesi için zorunludur. Dijital altyapının kuantuma hazır hale getirilmesi, hem ulusal güvenlik hem de dijital ekonomi için varoluşsal bir önem taşımaktadır.

Kaynakça

Anadolu Agency. (2024a, November 20). Türkiye's quantum leap: First computer to go live. https://www.aa.com.tr/en/economy/turkiye-set-to-launch-its-1st-quantum-computer/3399280

Anadolu Agency. (2024b). Türkiye eyes advances in quantum computing with plans for superconducting chip production. https://www.aa.com.tr/en/science-technology

Citi Institute. (2026, January). The trillion-dollar security race is on: Quantum threat. Citigroup. https://www.citigroup.com/rcs/citigpa/storage/public/Citi_Institute_Quantum_Threat.pdf

Cloud Security Alliance. (2024, August 15). NIST FIPS 203, 204, and 205: Finalized — An important step towards a quantum-safe future. https://cloudsecurityalliance.org/blog/2024/08/15

burakgun.com

Costa, D. B. C. (2025, September 3). Post-quantum financial infrastructure framework (PQFIF). SEC Written Input. https://www.sec.gov/files/cft-written-input-daniel-bruno-corvelo-costa-090325.pdf

DigiCert. (2024, November 26). Tracking the progress toward post-quantum cryptography. https://www.digicert.com/blog/the-progress-toward-post-quantum-cryptography

DHS. (tarihsiz). Post-quantum cryptography. U.S. Department of Homeland Security. https://www.dhs.gov/quantum

Federal Register. (2024, August 14). Announcing issuance of FIPS 203, FIPS 204, and FIPS 205. https://www.federalregister.gov/documents/2024/08/14/2024-17956

Fractal.ai. (2024, November 11). The looming threat of quantum computing to data security. https://fractal.ai/article/nists-post-quantum-cryptographic-standards

Herdem Law. (2025, April 15). Türkiye's quantum leap: Establishing a new frontier in defense technology. https://herdemlaw.com/en-us/explore/turkiyes-quantum-leap

IBM. (2025, November 12). IBM delivers new quantum processors, software, and algorithm breakthroughs. IBM Newsroom. https://newsroom.ibm.com/2025-11-12-ibm-delivers-new-quantum-processors

Introtoquantum.org. (2025, June 24). The timelines: When can we expect useful quantum computers? https://introtoquantum.org/essentials/timelines/

ISACA. (2025). Post-quantum cryptography: A call to action. https://www.isaca.org/resources/news-and-trends/industry-news/2025/post-quantum-cryptography-a-call-to-action

Jena, J. (2025). The quantum security deadline: Building crypto-agility against 'Harvest Now, Decrypt Later' threats. European Journal of Computer Science and Information Technology, 13(52), 35–52. https://eajournals.org/ejcsit/vol13-issue52-2025

Mastercard. (2025). Migration to post-quantum cryptography [White paper]. https://www.mastercard.com/content/dam/mccom/quantum-explainer-and-white-paper

Mosca, M., & Piani, M. (2024). Quantum threat timeline report 2024. Global Risk Institute (GRI).

NIST. (2024a). FIPS 203: Module-Lattice-Based Key-Encapsulation Mechanism Standard. National Institute of Standards and Technology. https://csrc.nist.gov/pubs/fips/203/final

NIST. (2024b). FIPS 204: Module-Lattice-Based Digital Signature Standard. National Institute of Standards and Technology. https://csrc.nist.gov/pubs/fips/204/final

NIST. (2024c). FIPS 205: Stateless Hash-Based Digital Signature Standard. National Institute of Standards and Technology. https://csrc.nist.gov/pubs/fips/205/final

NIST CSRC. (2024, December 11). Post-quantum cryptography. https://csrc.nist.gov/projects/post-quantum-cryptography

NIST. (2024d). NIST IR 8547: Transition to post-quantum cryptography standards. National Institute of Standards and Technology.

burakoguz.com

PKI Consortium. (2025, January 15). NIST post-quantum cryptography update [Conference presentation]. PQC Conference, Austin. https://pkic.org/events/2025/pqc-conference-austin-us/

postquantum.com. (2025). IonQ's 2025 roadmap: Toward a cryptographically relevant quantum computer by 2028. https://postquantum.com/industry-news/ionqroadmap-crqc/

postquantum.com. (2025). IBM quantum computing roadmap. https://postquantum.com/quantum-computing-companies/ibm/

QRAMM. (2024, December 24). NIST post-quantum cryptography standards: Complete guide to FIPS 203, 204, 205. https://qramm.org/learn/nist-pqc-standards.html

Qryptonic. (2025, June 24). Congress sounds the alarm: Why 'steal now, decrypt later' demands board-level action today. https://qryptonic.substack.com/p/congress-sounds-the-alarm-why-steal

Quantumzeitgeist. (2024, November 22). Turkey unveils first domestic quantum computer for technological independence. https://quantumzeitgeist.com/turkey-unveils-first-domestic-quantum-computer-for-technological-independence/

Quantum Security Defence. (2026, April 9). Harvest now decrypt later: The threat that is already in motion. https://quantumsecuritydefence.com/insights/hndl-in-motion/

Quantum Security Defence. (2026). NIST FIPS 203, 204, 205: What each standard requires. https://quantumsecuritydefence.com/insights/nist-fips-standards/

Sectigo. (2025, October 25). NIST's official 2024 post-quantum algorithms. https://www.sectigo.com/blog/who-are-nists-post-quantum-algorithm-winners

Shaw, A. (2025). Quantum-safe code auditing: LLM-assisted static analysis and quantum-aware risk scoring for post-quantum cryptography migration. arXiv preprint arXiv:2604.00560. https://arxiv.org/pdf/2604.00560

Shor, P. W. (1994). Algorithms for quantum computation: Discrete logarithms and factoring. Proceedings of 35th Annual Symposium on Foundations of Computer Science, 124–134.

SpinQ. (2025). Quantum computing industry trends 2025: A year of breakthrough milestones. https://www.spinquanta.com/news-detail/quantum-computing-industry-trends-2025

techvorta.com. (2026, April 5). Quantum computing explained: Where the world's most powerful computers stand in 2026. https://techvorta.com/quantum-computing-explained-2026/

TÜBİTAK BİLGEM. (2023). Quantum technologies. https://en.bilgem.tubitak.gov.tr/en/quantum-technologies/

Wikipedia. (2025). NIST Post-Quantum Cryptography Standardization. https://en.wikipedia.org/wiki/NIST_Post-Quantum_Cryptography_Standardization

burakoglu.com