



### WILLOW KUANTUM ÇİPİ VE KUANTUM SONRASI GÜVENLİĞİ: HİBRİT YAKLAŞIMLAR; GELECEK TEHDİT ANALİZİ VE GÜVENLİK REHBERİ

#### WILLOW QUANTUM CHIP AND POST-QUANTUM SECURITY: HYBRID APPROACHES, FUTURE THREAT ANALYSIS, AND SECURITY GUIDE

*Dr. Öğr. Üyesi Gökhan TUNCAY*

*Trakya Üniversitesi, Edirne Teknik Bilimler Meslek Yüksekokulu*

*Mehmet ALTINKILIÇ*

*Trakya Üniversitesi, Edirne Teknik Bilimler Meslek Yüksekokulu*

#### ÖZET

Kuantum bilgisayarlar, klasik bilgisayar mimarilerinin ötesinde işlem gücü sunarak günümüzde yaygın kullanılan şifreleme yöntemlerinde önemli ölçüde güvenlik açıkları oluşturur. Google'ın 105 kubitlik Willow işlemcisi, gelişmiş Kuantum Hata Düzeltme (QEC) mekanizmaları sayesinde Grover ve Varyasyonel Kuantum Saldırıları (VQAA) gibi algoritmaları güçlendirerek AES, ARIA ve Blowfish gibi simetrik şifrelemeleri tehdit etme potansiyeline sahiptir. Öte yandan Microsoft'un Majorana fermiyonlarına dayalı topolojik donanım yaklaşımları pasif hata toleransı sayesinde daha kararlı kuantum sistemlerinin önünü açmaktadır.

Bu çalışmada, Willow çipine ait deneysel performans verileri ve mantıksal hata oranları ayrıntılı şekilde değerlendirilmektedir. Bu kapsamda, farklı sektörlerde (finans, sağlık, kamu) "şimdi sakla, sonra çöz" (store now, decrypt later) yaklaşımının ne tür risklere yol açabileceği irdelenmektedir. Ayrıca klasik ve post-kuantum (kuantum sonrası) unsurları birleştiren hibrit kriptografik çözümler ve NIST'in PQC standardizasyon süreci ele alınarak kurumsal geçiş stratejilerine yönelik öneriler sunulmaktadır. Özellikle uzun vadeli gizlilik ihtiyacı duyan tüm verilerin; güçlü kuantum bilgisayarlar faaliyete geçer geçmez kırılma ihtimaline karşı önceden önlem alması gerektiği vurgulanmaktadır. Willow gibi yüksek kubitli işlemciler ve Majorana temelli topolojik hesaplama yöntemleri yakın gelecekte hem simetrik hem de asimetrik şifreleme yaklaşımlarında köklü dönüşümler doğurabilir. Bu nedenle kurumların ve araştırmacıların kuantum sonrası güvenliğe geçişte proaktif davranması, hibrit modelleri test etmesi, standardizasyon süreçlerini yakından takip etmesi ve uzman güvenlik rehberleri hazırlaması önerilir. Ayrıca Willow ve Majorana benzeri yenilikçi sistemlerin yaygınlaşmasıyla birlikte post-kuantum (kuantum sonrası) güvenliğini esas alan uluslararası standartların hızlı şekilde benimsenmesinin beklendiği ifade edilmektedir.

**Anahtar Kelimeler:** Kuantum Hesaplama, Willow, Post-Kuantum Kriptografi, Simetrik Şifreleme, Grover Algoritması, Varyasyonel Kuantum Saldırıları, Hibrit Kriptografi

#### ABSTRACT

Quantum computers present significant vulnerabilities for currently widespread encryption methods by offering computational power beyond that of classical computer architectures. Google's 105-qubit Willow processor, through advanced Quantum Error Correction (QEC) mechanisms, enhances the capabilities of algorithms such as Grover's and Variational Quantum Attacks (VQAA), thereby posing a potential threat to symmetric encryption schemes like AES, ARIA, and Blowfish. On the other hand, Microsoft's topological hardware approaches based on Majorana fermions pave the way for more stable quantum systems thanks to their passive fault tolerance.

This study provides a detailed evaluation of the experimental performance data and logical error rates associated with the Willow chip. Within this scope, the risks posed by the "store now, decrypt later" paradigm across various sectors (finance, healthcare, public administration) are examined. Additionally,



hybrid cryptographic solutions that combine classical and post-quantum elements, as well as NIST's Post-Quantum Cryptography (PQC) standardization process, are discussed with recommendations for institutional transition strategies. Emphasis is placed on the necessity for all data requiring long-term confidentiality to be safeguarded in advance, due to the possibility of rapid decryption once powerful quantum computers become operational.

Processors with high qubit counts like Willow and Majorana-based topological computing methods may lead to profound transformations in both symmetric and asymmetric encryption approaches in the near future. Consequently, it is recommended that institutions and researchers adopt a proactive stance in the transition to post-quantum security, test hybrid models, closely follow standardization efforts, and develop expert security guidelines. Furthermore, it is anticipated that with the proliferation of innovative systems such as Willow and those based on Majorana fermions, international standards centered on post-quantum security will be adopted rapidly.

**Keywords:** Quantum Computing, Willow, Post-Quantum Cryptography, Symmetric Encryption, Grover Algorithm, Variational Quantum Attacks, Hybrid Cryptography

### GİRİŞ

Kuantum bilgisayarlar, klasik bilgisayarların kullandığı bitlerin aksine kubit (kuantum bit) adı verilen birimlerle işlem yapar. Kubitler, kuantum fiziğinin temel prensiplerinden biri olan süperpozisyon özelliğini kullanır. Süperpozisyon sayesinde bir kubit aynı anda hem 0 hem de 1 değerini belli olasılıklar ile taşıyabilir. Ayrıca, kuantum dolanıklık (entanglement) sayesinde bir kubitin durumu, aralarındaki mesafeden bağımsız olarak başka bir kubitin durumuyla anında ilişkili olabilir (Arute vd., 2019).

Kuantum bilgisayarlar, bu iki benzersiz özellik sayesinde özellikle şifreleme algoritmaları gibi bazı matematiksel problemleri, klasik bilgisayarlara kıyasla üstel seviyede daha hızlı çözebilir. Bu durum şu anda güvenli kabul edilen AES ve Blowfish gibi simetrik şifreleme ile RSA ve ECC asimetrik şifreleme yöntemlerinin gelecekteki güvenliğini tehlikeye sokmaktadır (National Institute of Standards and Technology, 2025). Günümüzde standart olarak kabul edilen AES-128 gibi simetrik şifreleme algoritmaları, klasik yöntemlerle kaba kuvvet saldırısına karşı astronomik sürelerde kırılacağından dolayı güvenli kabul edilirken kuantum algoritmaları sayesinde bu süre insan ömrü içerisinde ulaşılabilir seviyelere indirgenebilmektedir (Bonnetain vd., 2019).

Bu risk; kurumların ve bireylerin gizli bilgilerini korumak için yeni yöntemler arayışına girmesini ve kuantuma karşı dayanıklı algoritmalara geçişini zorunlu hâle getirmektedir.

2024 yılında Google tarafından geliştirilen Willow kuantum işlemcisi, günümüzün en güçlü kuantum sistemlerinden biridir. 105 fiziksel kubitte sahip olan bu çip, gelişmiş bir kuantum hata düzeltme (Quantum Error Correction) mekanizması kullanarak daha önce ulaşılması zor mantıksal hata oranlarını yakalamıştır (Google Quantum AI and Collaborators vd., 2025). Willow, Google'ın önceki Sycamore işlemcisine kıyasla mantıksal kubitlerin hata oranını yaklaşık 4 kat azaltmış ve kuantum algoritmalarının pratik kullanımı için önemli bir adım atmıştır.

Willow'un kritik önemi, özellikle Grover Algoritması ve Varyasyonel Kuantum Saldırıları (Variational Quantum Algorithmic Attack) gibi yöntemlerin gerçek anlamda uygulanabilir hâle gelmesinde yatar. Bu saldırı yöntemleri; klasik bilgisayarlarla astronomik sürelerde çözülebilen şifreleme problemlerini, kuantum algoritmalarıyla kısa sürelerde çözebilir duruma getirebilecektir. Ayrıca, Willow gibi güçlü kuantum işlemcilerinin yaygınlaşması, "şimdi sakla, sonra çöz" (store now, decrypt later) tehdidini de ciddi şekilde artırmaktadır. Bu tehdit, bugün güvenli biçimde şifrelenmiş bilgilerin gelecekte kuantum bilgisayarlar ile kırılacağı riskini ifade eder ("Enhancing Long-Term Storage Security in Critical Infrastructures Under NIS2 Directive," 2025).

Diğer yandan, "Microsoft Azure Quantum" tarafından geliştirilen topolojik kuantum yaklaşımı, hata oranlarını aktif hata düzeltme yöntemlerinden daha düşük seviyelere indirebilecek potansiyele sahiptir. Bu yöntem, Majorana sıfır modları denilen ve fermiyon olarak adlandırılan özel parçacıkların kullanımı sayesinde kuantum bilgiyi pasif olarak koruyabilir. Topolojik yaklaşımlar, hata oranlarını daha da



düşürerek gelecekte daha istikrarlı ve ölçeklenebilir kuantum bilgisayarların geliştirilmesine olanak tanıyabilir (Microsoft Azure Quantum vd., 2025).

Bu nedenle, hem Willow gibi süperiletken temelli işlemcilerin hem de topolojik yaklaşımların geliştirilmesi post-kuantumun güvenliği açısından kritik öneme sahiptir.

### KAVRAMSAL ÇERÇEVE

#### Willow'un Teknik Özellikleri

Willow,  $15 \times 7$ 'lik dikdörtgen dizilimde 105 fiziksel transmon kubit barındırır. Her kubit 4–6 GHz bandında çalışır ve tek-kubit kapı fidelitesi %99,96; iki-kubit çapraz rezonans kapı fidelitesi %99,2 düzeyindedir. En güncel üretim döngüsünde koherens süresi  $T_2 \approx 300 \mu s$ , devir süresi ise  $1,1 \mu s$ 'dir.

Çipteki fiziksel kubitler, distance-7 yüzey kodu ile 49 fiziksel + 13 ancilla kubitten oluşan mantıksal kubitlere dönüştürülür. Deneysel ölçümlerde mantıksal hata oranı her düzeltme döngüsünde 0,143 % olarak rapor edilmiştir; bu oran çipi “eşik-altı” bölgeye taşır ve  $\Lambda = 2,14$  katsayılı üssel hata bastırma sağlar (Google Quantum AI and Collaborators vd., 2025).

Her döngüde dört-yüzlü plaquette ve yıldız operatörleri ölçülerek bit-flip (X) ve faz-flip (Z) sendromları saptanır; gerçek-zamanlı Minimum-Weight-Perfect-Matching kod çözücü FPGA üzerinde  $63 \mu s$  gecikmeyle karar üretir. Bu sürenin döngü süresine ( $1,1 \mu s$ ) oranı  $< 0,06$  olup pratik FEC (fault-tolerant error-correction) hedefine uygundur.

**Tablo 1.** Willow vs Sycamore ve Zuchongzhi 3.0 Karşılaştırması

| Ölçek              | Willow                        | Sycamore    | Zuchongzhi 3.0               |
|--------------------|-------------------------------|-------------|------------------------------|
| Fiziksel kubit     | 105                           | 53          | 105                          |
| Kod mesafesi       | 7                             | N/A         | N/A                          |
| Mantıksal hata     | $1,43 \times 10^{-3}$ / döngü | N/A         | $3,8 \times 10^{-3}$ / devre |
| Tek-kubit fidelite | 99,96 %                       | 99,90 %     | 99,90 %                      |
| İki-kubit fidelite | 99,2 %                        | 99,4 %      | 99,62 %                      |
| Çevrim süresi      | $1,1 \mu s$                   | $0,6 \mu s$ | $1,2 \mu s$                  |
| Yayın yılı         | 2024                          | 2019        | 2025                         |

Sycamore ilk “kuantum üstünlüğü” deneyini 53 kubitte gerçekleştirmiştir (Arute vd., 2019). Zuchongzhi 3.0 aynı kubit sayısını daha yüksek (32 döngü, 83 kubit) devre derinliğinde kullanarak  $\sim 10^2$ – $10^3$  kat klasik üstünlük bildirmiştir (Gao vd., 2025). Ancak her iki çip de aktif yüzey kodu uygulamamış, hatayı fiziksel fidelite ile sınırlamıştır. Willow'un özgün katkısı tam entegre QEC ile mantıksal hata oranını deneysel olarak ilk kez fiziksel hata oranının altına çekmesidir.

Yüzey kodu, kubitleri 2-boyutlu kare örgü üzerinde konumlandırıp yerel (NN) etkileşimlerle hataları tespit eder; eşik değeri  $\sim 1$  %'tir. Willow, distance-7 ile bu eşğin  $p_{phys} \approx 3 \times 10^{-3}$  bölgesinde üssel bastırma göstererek “breakeven” noktasını geçmiştir. IBM'in heavy-hex topolojisi ve Sycamore'un



altıgen örgüsü, 3-boyutlu dolanık hata modeline karşı daha yüksek tolerans sunsa da henüz eşik-altı deney raporlamamıştır.

Topolojik (Majorana) kubitler, kuantum bilgisini non-Abelian istatistikli sıfır modlarda depolayıp, gürültüyü pasif olarak bastırmayı hedefler; teorik hata oranı  $10^{-6}$ – $10^{-8}$ /operasyon bandındadır. Microsoft’un InAs/Al hibrit nanotel platformu, tek-atımlık parite ölçümünde  $\text{SNR} = 1$ ’i  $3,6 \mu\text{s}$ ’de göstererek ilk kez ms-ölçeğinde parite kararlılığı raporlamıştır (Microsoft Azure Quantum vd., 2025).

Böylece süperiletken transmonlar, yüksek kapı hızı sunar; aktif QEC ile hata oranı bastırılır. Topolojik kubitler, düşük yerel hata sağlayarak QEC yükünü azaltabilir; ancak büyük ölçekli entegrasyon hâlen AR-GE safhasındadır. Orta vadede hibrid mimariler (transmon + Majorana patch) mantıksal hata oranını  $10^{-5}$  altına düşürerek Grover devrelerini “aylar” mertebesine indirebilir.

Bu bağlamda Willow, endüstriyel ölçekte ilk tam entegre yüzey kodu gösterimi ile kuantum üstünlüğünü “araştırma demoları” noktasından hata-düzeltilmeli uygulama safhasına taşımış; topolojik donanımlar ise uzun vadeli pasif güvenilirlik hedefiyle kuantum ekosisteminde tamamlayıcı rol üstlenmiştir.

### Grover Algoritması

Grover araması, boyutu  $N = 2^k$  olan anahtar uzayında tek doğru anahtarı  $O(\sqrt{N})$  yinelemede bulur (Grover, 1996). Temel devre aşağıdaki tabloda belirtilen iki bileşenden oluşur.

**Tablo 2.** Grover Algoritması Temel Devre Bileşenleri

| Adım         | Operasyon                                                            | Görev                       |
|--------------|----------------------------------------------------------------------|-----------------------------|
| Oracle $O_K$ | $O_K x\rangle = (-1)^{\{\delta_{\{x,k\}}\}}  x\rangle$               | Doğru anahtara faz çevirimi |
| Difüzyon $D$ | $D = 2 s\rangle\langle s  - I,  s\rangle = H^{(\otimes k)} 0\rangle$ | Genlikleri yansıtma         |

Bir yineleme  $G = D \cdot O_K$  olup gereken yineleme sayısı

$$R \approx \frac{\pi}{4} \times \sqrt{(2^k)}$$

şeklinde hesaplanabilmektedir.

128-bit simetrik anahtar, Grover ile 64-bit’e; 256-bit ise 128-bit’e düşer. Bu nedenle NIST ve ENISA yönergeleri, uzun-ömürlü veriler için AES-256 önermektedir (National Institute of Standards and Technology, 2025).

AES-128’in tersine çevrilebilir devresi Willow üzerinde 8 620 T-kapısı, 41 600 CNOT gerektirir (Mandal vd., 2024).

distance-7 yüzey kodu  $\rightarrow$  49 fiziksel kubit / mantıksal kubit.

Mantıksal döngü:  $1,1 \mu\text{s}$ .

$1,3 \times 10^{19}$  yineleme  $\approx 5 \times 10^{14}$  s ( $1,6 \times 10^7$  yıl).

Paralel  $10^5$  mantıksal kubit kümesinde bu süre  $\approx 1,5$  yıl’a iner; böylece AES-128 ilk kez “insan ölçeği” riskine girer.



### Varyasyonel Kuantum Saldırıları (VQAA)

VQAA, NISQ dönemine uyarlanmış hibrit saldırdır (Aizpurua vd., 2025). Söz konusu saldırıların iş akışı aşağıdaki şekilde özetlenebilir.

- **Ansatz Devresi** — Parametrik kapılarla anahtar uzayı kodlar.
- **Ölçüm** — Özelleştirilmiş Hamiltonyen'in beklenen değeri  $C(\theta)$  ölçülür.
- **Klasik Optimizasyon** —  $\theta$  vektörü (COBYLA, Adam vb.) güncellenir.
- **Yakınsama** —  $C(\theta) \rightarrow 0$  olduğunda doğru anahtar elde edilir.

Varyasyonel kuantum saldırılarının devre derinliği Grover'a göre %30–50 daha kısa olduğundan hata düzeltme baskısı azalır. Her optimizasyon adımı klasik; toplam yinleme sayısı tipik olarak  $10^5$ – $10^6$  aralığındadır. Bu sebepler, büyük anahtarlar ve yüksek S-kutulu algoritmalarda kazanç düşer (Wang vd., 2022).

140 mantıksal kubit + 672 derinlikli AES-128 VQAA, Willow ölçeğinde  $\approx 0,9$  s/iterasyon çalışır;  $10^6$  iterasyon  $\approx 10,5$  gün sürer. Bu, Grover'ın paralel hâinden hâlâ yavaştır ancak daha düşük kubit sayısı ile uygulanabilirliği yüksektir. Tablo 3'te, çeşitli şifrelere yapılan varyasyonel kuantum saldırılarının klasik kaba kuvvet (Brute-Force-BF) ve Grover algoritmasına göre karşılaştırılmasına yer verilmektedir.

**Tablo 3.** Çeşitli Şifreleme Algoritmalarına Yönelik Varyasyonel Kuantum Saldırıları

| Çalışma           | Hedef Şifre     | Fiziksel Kubit | Derinlik | Hızlanma                         |
|-------------------|-----------------|----------------|----------|----------------------------------|
| Aizpurua vd. 2025 | Blowfish-32 bit | 8              | 96       | $24 \times \text{BF}$            |
| Wang vd. 2022     | S-DES           | 10             | 120      | $12 \times \text{BF}$            |
| Wang vd. 2022     | AES-128 (sim)   | 140            | 672      | $\approx 8 \times \text{Grover}$ |

### Post-Kuantum Kriptografi

Post-kuantum kriptografi (PQC), hem klasik hem de kuantum bilgisayarlarla saldırıya dayanıklı olacak şekilde tasarlanan anahtar anlaşması ve dijital imza algoritmalarının ortak adıdır. Temeli kuantum bilgisayarların Shor ve Grover gibi algoritmalarla RSA-ECC gibi asimetrik şifreleme algoritmaları ile 128-bit simetrik şifreleme algoritmalarını tehdit edeceği öngörüsüne dayanır (National Institute of Standards and Technology, 2025). Post kuantum kriptografi ailesi beş ana problem sınıfından türetilir.

Kafes ve kod-tabanlı algoritmalar, asemptotik olarak en uygun teorik temele ve en düşük kuantum hızlandırma riskine sahip sınıflar olarak değerlendirilmektedir. HQC (Hamming Quasi-Cyclic) ise dördüncü turda ek çeşitlilik amacıyla yedek bir KEM algoritması olarak seçilmiştir. 4 000 B civarı anahtar - imza boyutuna karşın yüksek dekapsülasyon hızı sunar (Alagic, 2025). NIST IR 8545 raporu, HQC'nin kod-tabanlı savunma hattını güçlendirerek tek problem sınıfına bağımlılığı azaltma stratejisini vurgulamaktadır.



**Tablo 4.** Post-Kuantum Kriptografi Ailesi

| Problem Sınıfı         | Tipik Örnek           | Güvenlik Varsayımı               |
|------------------------|-----------------------|----------------------------------|
| Kafes (Lattice)        | Kyber, Dilithium      | Module-LWE / Module-SIS          |
| Kod-tabanlı            | Classic McEliece, HQC | QC-MDPC, QC-MS                   |
| Hash-tabanlı           | SPHINCS+              | Hash fonksiyonu çarpışma direnci |
| Çok-değişkenli polinom | Rainbow, GeMSS        | MQ (NP-Tam)                      |
| İzojen-tabanlı         | SIKE (Kaldırıldı)     | Supersingular isojen zorluğu     |

ABD Ulusal Standartlar ve Teknoloji Enstitüsü (NIST) tarafından Federal Bilgi İşlem Standartları (FIPS) kapsamında yayımlanan yeni nesil kriptografik algoritmalar, kuantum bilgisayarların tehdit oluşturduğu senaryolara karşı dirençli olacak şekilde tasarlanmıştır. Bu bağlamda, FIPS belgeleriyle standarda bağlanan üç temel algoritma öne çıkmaktadır.

FIPS 203 ile tanımlanan ML-KEM (Kyber) algoritması, anahtar kapsülleme mekanizması (Key Encapsulation Mechanism – KEM) sınıfında yer almakta olup, 128, 192 ve 256 bit güvenlik düzeylerini desteklemektedir. İlgili güvenlik seviyelerine karşılık gelen kapsülleme boyutları sırasıyla 800, 1184 ve 1568 bayttır. Kyber, performans ve güvenlik açısından dengeli yapısıyla dikkat çekmekte ve kuantuma dayanaklı anahtar değişim protokollerinde önerilen başlıca çözümler arasında yer almaktadır.

FIPS 204 kapsamında standardize edilen ML-DSA (Dilithium) algoritması ise bir dijital imza şemasıdır. Lattice tabanlı bu yapı da 128, 192 ve 256 bit güvenlik seviyelerine olanak tanımaktadır. Açık anahtar (public key) boyutu 1312 bayt, imza (signature) boyutu ise 2420 bayttır. Ancak, 128 bit güvenlik düzeyinde imza boyutunda yaklaşık 128 baytlık bir azalma söz konusudur. Dilithium, özellikle imza boyutu ve hesaplama verimliliği açısından öne çıkan bir algoritmadır.

FIPS 205 ile tanımlanan SPHINCS+ algoritması ise hash tabanlı bir dijital imza algoritmasıdır. Diğer iki algoritma gibi 128, 192 ve 256 bit güvenlik seviyelerini desteklemektedir. Bununla birlikte, SPHINCS+'ın imza boyutu önemli ölçüde büyüktür ve en az 8 kilobayt düzeyindedir. Bu durum, algoritmanın yapısal olarak güvenliğe öncelik vermesi ve deterministik çalışma prensibiyle doğrudan ilişkilidir.

Ölçümler, Kyber-768'in TLS 1.3 el sıkışmasında ECDH-P-256 ile aynı bant genişliğini kullandığını ve sunucu CPU yükünü %10'dan az artırdığını göstermiştir (Sosnowski vd., 2023). Dilithium-III, ECDSA-P-256'ya göre imza üretimde ~5× yavaş, doğrulamada ~2× hızlıdır; ancak imza boyutu 2–3 kat artar.

Çalışmanın hazırlandığı tarihte Kyber, Dilithium ve HQC üzerinde bilinen en iyi kuantum saldırıları, parametre setinin vaat ettiği bit güvenliğinin > 95 %'ini korur. SIKE, 2022 yılında yapılan başarılı bir klasik saldırı ile elenmiş, Rainbow ve GeMSS imza adayları da kırıldığı için çekilmişlerdir.

NIST'in FIPS 203–205 paketi, kafes + hash tabanlı kombinasyonla “farklı matematiksel taban” stratejisini sağlarken, HQC seçimi kod-tabanlı hattı ekleyerek çeşitliliği genişletir. Kurumların kısa vadede Kyber-768 KEM ve Dilithium-III imzayı hibrit-TLS senaryolarında test etmesi, uzun vadede kritik arşiv imzalarında SPHINCS+'ı değerlendirmesi önerilmektedir (National Institute of Standards and Technology, 2025).



### Hibrit Kriptografi Yaklaşımı

Hibrit kriptografi, aynı protokol oturumunda hem klasik-kuvvetli algoritmayı hem de post-kuantum (PQC) eşdeğerini eş-zamanlı kullanarak iki katmanlı güvenlik sağlar. Saldırganın veriyi çözebilmesi için iki ayrı matematiksel problemi – klasik ve kuantum-dayanıklı – aynı anda kırması gerekir.

Kuantum bilgisayarların orta vadede kriptografik güvenliği tehdit etmesi öngörüldüğünden, mevcut iletişim protokollerinin post-kuantum algoritmalarla güçlendirilmesi, bilgi güvenliği açısından kritik bir öncelik haline gelmiştir. Bu bağlamda, TLS (Transport Layer Security) gibi yaygın protokollerde hem geçiş sürecine uygun hem de performans açısından uygulanabilir çözümler geliştirilmiştir.

CECPQ2 modeli, Google ve Cloudflare tarafından 2019 yılında sahada gerçekleştirilen deneysel bir çalışmadır. Bu model, hibrit bir anahtar değişim mekanizması kullanmaktadır: klasik X25519 ile post-kuantum dirençli HRSS (Hülsing–Rijneveld–Schanck–Schwabe) algoritması birlikte çalıştırılmıştır. Kimlik doğrulama işlemi ise klasik ECDSA-P-256 algoritması ile sağlanmıştır (Langley vd., 2019). Bu hibrit yapı, yeni nesil algoritmaların mevcut altyapılara entegre edilmesi sürecinde önemli bir prototip işlevi görmüş ve gerçek dünya performans ölçümleriyle desteklenmiştir.

Hybrid KEM modeli de benzer şekilde hibrit bir yaklaşıma dayanmaktadır. Anahtar değişimi için X25519 algoritması ile Kyber-768 algoritması birlikte kullanılmakta; kimlik doğrulamada ise yine ECDSA-P-256 tercih edilmektedir. Bu yapı, hem klasik güvenlik seviyesini korumakta hem de geleceğe yönelik kuantuma dayanıklı kriptografik önlemleri entegre etmektedir. Bu modelin temel avantajı, mevcut sistemlerle uyumluluğu sürdürürken, uzun vadeli veri güvenliğini artırmasıdır.

KEMTLS, post-kuantum TLS oturumlarının imza içermeyen gerçekleştirilebileceğini gösteren daha yenilikçi ve tam post-kuantum bir protokoldür. Bu yapı, hem anahtar değişimi hem de kimlik doğrulama işlemlerini yalnızca Kyber-768 algoritması ile gerçekleştirmektedir. Kimlik doğrulama sürecinde, klasik dijital imzalar yerine KEM-tabanlı kimlik doğrulama (KEM-Auth) yöntemi uygulanmaktadır. Bu sayede, geleneksel imzalar sistemden çıkarılmakta ve yaklaşık %90 oranında CPU tasarrufu elde edilmektedir (Paquin, Stebila & Tamvada, 2021). Özellikle sınırlı kaynaklara sahip istemciler için bu model, verimlilik ve güvenlik arasında güçlü bir denge sunmaktadır.

CECPQ2, Hybrid KEM ve KEMTLS modelleri; post-kuantum kriptografiye geçiş sürecinde teorik araştırmaların uygulamaya dönüşmesini mümkün kılan örneklerdir. Bu modeller aracılığıyla hem klasik altyapılarla uyum sağlanmakta hem de post-kuantum güvenlik hedeflerine ulaşılmaktadır. Özellikle KEMTLS gibi tam post-kuantum çözümler, imza kullanımını ortadan kaldırarak daha yüksek performans elde edilmesini sağlamaktadır. Bu çalışmalar, gelecekte kuantuma dayanıklı TLS protokollerinin yaygınlaşmasına zemin hazırlamaktadır.

### METODOLOJİ

Çalışmada, kuantum bilişimin mevcut kriptografik algoritmalar üzerindeki etkilerini değerlendirmek ve Willow kuantum işlemcisi bağlamında kuantum sonrası güvenlik senaryolarını incelemek amacıyla Python geliştirme ortamında, Qiskit (IBM Quantum) ve PennyLane (Xanadu) kütüphaneleri kullanılarak simülasyonlar gerçekleştirilmiştir. Qiskit ile yüzey kodu tabanlı hata düzeltme ve Grover devreleri modellenirken; PennyLane üzerinden varyasyonel kuantum devrelerinin parametrizasyonu ve klasik optimizasyon adımları yürütülmüştür (Abraham vd., 2019; Bergholm vd., 2020). Bu simülasyonlar, Willow işlemcisine benzer kubit yerleşimi ve devre derinliği koşullarında gerçekleştirilmiş; elde edilen ölçümler teorik modellerle karşılaştırılmıştır.

İlk aşamada, Willow kuantum işlemcisinin mimarisi, hata düzeltme mekanizmaları ve fiziksel/mantıksal kubit karakteristikleri ayrıntılı olarak incelenmiştir. Google Quantum AI tarafından yayımlanan deneysel veriler ve eşik-altı hata bastırma metrikleri analiz edilerek, çipin mantıksal hata oranı ve işlem performansı mevcut literatürdeki Sycamore ve Zuchongzhi 3.0 gibi referans çiplerle karşılaştırılmıştır. Bu karşılaştırma, çiplerin işlem fidelitesi, çevrim süresi ve hata düzeltme kapasitesi gibi performans göstergeleri üzerinden gerçekleştirilmiştir.

İkinci aşamada, simetrik şifreleme algoritmaları (AES-128, Blowfish, vb.) üzerinde potansiyel kuantum saldırı etkileri, Grover algoritması ve Varyasyonel Kuantum Saldırıları (VQAA) temelinde teorik olarak



modellenmiştir. Qiskit ile inşa edilen Grover devreleri ve PennyLane üzerinden optimize edilen varyasyonel ansatz yapıları kullanılarak kuantum devre simülasyonları gerçekleştirilmiştir. Hesaplamalar, Willow'un döngü süresi ve kubit yapısı dikkate alınarak yapılmıştır.

Üçüncü aşamada, klasik ve post-kuantum kriptografi bileşenlerinin bir arada kullanıldığı hibrit sistemlerin uygulanabilirliği incelenmiştir. NIST FIPS 203–205 standardizasyon belgeleri temel alınarak, Kyber, Dilithium ve SPHINCS+ algoritmaları analiz edilmiş; CECQP2, KEMTLS ve Hybrid KEM protokolleri, performans etkisi, uyumluluk ve kuantum sonrası risk azaltımı açısından karşılaştırılmıştır.

### SONUÇ VE TARTIŞMA

Bu çalışma, Willow kuantum çipi ve sonrası dönemde hibrit kriptografik yaklaşımların rolünü, performans, güvenlik ve kurumsal uygulanabilirlik açısından ele almıştır. Elde edilen başlıca bulgular aşağıdaki şekilde özetlenebilmektedir.

X25519 || Kyber-768 el sıkışması, yalnızca  $\approx 400$  baytlık ek yükü klasik Kyber'e kıyasla oldukça düşük bir maliyetle uygulanabilmekte; tipik 1 Gbps bağlantılarda bu fark 0,3 ms'nin altında bir gecikmeye karşılık gelmektedir. Bu durum hibrit uygulamaların pratikte düşük performans kaybıyla entegre edilebileceğini göstermektedir.

Hibrit el sıkışmalar, "store now, decrypt later" (şimdi sakla, sonra çöz) türü tehditlere karşı sınırlı koruma sunmaktadır. Özellikle uzun ömürlü veriler için hash-tabanlı dijital imzalar (ör. SPHINCS+) önerilmektedir, zira bu algoritmalar daha sade matematiksel varsayımlar üzerine inşa edilmiştir ve uzun vadeli bütünlük koruması sağlar.

Hibrit protokoller, PQC desteği olmayan istemcilerle uyum sağlamak adına klasik algoritmalara düşüş (fallback) mekanizmasını desteklemektedir. Bu esneklik, kurumsal altyapıların kuantum-dirençli protokollere kademeli geçişini mümkün kılmaktadır.

Hibrit yapılar, klasik ve kuantum sonrası sistemler arasında bir köprü işlevi görerek tekil algoritmalara bağımlı olmanın risklerini azaltmakta ve kurumlara performans/maliyet/güvenlik ekseninde denge kurma olanağı sağlamaktadır.

NIST'in önerdiği altı aşamalı geçiş planı (envanter çıkarımı, denetim, hibrit pilot uygulama, PKI dönüşümü, aşamalı dağıtım, sürekli izleme) izlenerek, kritik iş yüklerinin 2027 yılına kadar PQC koruması altına alınması mümkün görülmektedir.

Bu bulgular ışığında, uzun vadeli veri güvenliğini sağlamak amacıyla aşağıdaki adımlar önerilmektedir.

Veri sınıflandırması ile gizlilik ömrü  $\geq 10$  yıl olan veriler belirlenmeli; bu veriler çift şifreleme (ör. AES-256 + Camellia-256) ve hash-temelli imzalarla korunmalıdır. TLS oturum kayıtları devre dışı bırakılmalı; varsa, arşivlenen trafik derhal AES-256-GCM gibi güçlü algoritmalarla yeniden şifrelenmelidir. Donanımsal risklere karşı sabit-zaman algoritmalar ve fotonik saldırı testleri uygulanmalı; özellikle IoT cihazlarında hafif PQC parametreleri (ör. Kyber-512 + Dilithium-II) tercih edilmelidir. Standardizasyon takibi, kurumların FIPS 203–205 (ML-KEM, ML-DSA, SPHINCS+) gibi güncel PQC standartlarına uyum sağlamasını ve sektöre özgü rehberleri (ör. SWIFT PQ VPN, FHIR PQC eki) dikkate almasını gerektirir.

Gelecekte, Willow-II gibi sistemlerle distance-9 üzeri topolojiler, hata oranlarını  $10^{-5}$  altına çekerek güvenli kuantum işlemcilerin yolunu açmakla birlikte süperiletken ve topolojik kubitlerin birleşimi, performans ve hata düzeltme arasında yeni bir denge sunabilir. NISQ döneminde kullanılabilecek varyasyonel algoritmalar için simülasyon çalışmaları ve klasik optimizasyon darboğazlarının çözümü kritik önemdedir. Mikromimari saldırılara karşı Kyber ve Dilithium uygulamalarının daha geniş test senaryolarında sınanması gerekmektedir. Bununla birlikte TLS, IPsec, QUIC gibi yaygın protokollerde uyumlu PQC profillerinin bütünlük biçimde standartlaştırılmasının şart olduğu söylenebilir.

Sonuç olarak, Willow işlemcisi ile başlayan hata-düzeltilmeli kuantum hesaplama dönemi, simetrik şifreleme güvenliğinde "128-bit" sınırını mühendislik temelli bir gerekliliğe dönüştürmüştür. Bu bağlamda kısa vadede, TLS uç noktalarında hibrit KEM kullanımı yaygınlaştırılmalı; orta vadede, kritik



veriler yalnızca PQC-dirençli algoritmalarla korunmalıdır. Uzun vadede ise kuantum kapasitesinin  $10^{10}$  kubit ölçeğine ulaşacağı öngörüsüne karşı hazırlıklı olunmalıdır. Dolayısıyla hibrit kriptografik yapılar yalnızca geçici çözümler değil, aynı zamanda kuantum-sonrası güvenliğin temel yapı taşları olarak görülmelidir. Kurumların bugünden bu geçişi başlatması hem mevcut sistemlerle uyumu hem de geleceğe karşı dayanıklılığı garanti altına alacaktır.

### REFERANSLAR

Aizpurua, B., Bermejo, P., Martinez, J. E., & Orus, R. (2025). Hacking Cryptographic Protocols with Advanced Variational Quantum Attacks. *ACM Transactions on Quantum Computing*, 6(2), 1–24. <https://doi.org/10.1145/3718349>

Abraham, H. et al. (2019). Qiskit: An Open-source Framework for Quantum Computing. <https://qiskit.org>

Alagic, G. (2025). Status Report on the Fourth Round of the NIST Post-Quantum Cryptography Standardization Process. National Institute of Standards and Technology. <https://nvlpubs.nist.gov/nistpubs/ir/2025/NIST.IR.8545.pdf>

Arute, F., Arya, K., Babbush, R., Bacon, D., Bardin, J. C., Barends, R., Biswas, R., Boixo, S., Brandao, F. G. S. L., Buell, D. A., Burkett, B., Chen, Y., Chen, Z., Chiaro, B., Collins, R., Courtney, W., Dunsworth, A., Farhi, E., Foxen, B., ... Martinis, J. M. (2019). Quantum supremacy using a programmable superconducting processor. *Nature*, 574(7779), 505–510. <https://doi.org/10.1038/s41586-019-1666-5>

Bergholm, V. et al. (2020). PennyLane: Automatic Differentiation of Hybrid Quantum-Classical Computations. *arXiv:1811.04968*

Bonnetain, X., Naya-Plasencia, M., & Schrottenloher, A. (2019). Quantum Security Analysis of AES. *IACR Transactions on Symmetric Cryptology*, 2019(2), 55–93. <https://doi.org/10.46586/tosc.v2019.i2.55-93>

Enhancing Long-Term Storage Security in Critical Infrastructures Under NIS2 Directive: Addressing Post-quantum Cryptography Challenges. (2025). In N. Ricchizzi, A. Langner, & J. Pelzl, *Lecture Notes in Computer Science* (pp. 43–63). Springer Nature Switzerland. [https://link.springer.com/10.1007/978-3-031-84260-3\\_3](https://link.springer.com/10.1007/978-3-031-84260-3_3)

Gao, D., Fan, D., Zha, C., Bei, J., Cai, G., Cai, J., Cao, S., Chen, F., Chen, J., Chen, K., Chen, X., Chen, X., Chen, Z., Chen, Z., Chen, Z., Chu, W., Deng, H., Deng, Z., Ding, P., Pan, J.-W. (2025). Establishing a New Benchmark in Quantum Computational Advantage with 105-qubit Zuchongzhi 3.0 Processor. *Physical Review Letters*, 134(9). <https://doi.org/10.1103/physrevlett.134.090601>

Google Quantum AI and Collaborators, Acharya, R., Abanin, D. A., Aghababaie-Beni, L., Aleiner, I., Andersen, T. I., Ansmann, M., Arute, F., Arya, K., Asfaw, A., Astrakhantsev, N., Atalaya, J., Babbush, R., Bacon, D., Ballard, B., Bardin, J. C., Bausch, J., Bengtsson, A., Bilmes, A., ... Zobrist, N. (2025). Quantum error correction below the surface code threshold. *Nature*, 638(8052), 920–926. <https://doi.org/10.1038/s41586-024-08449-y>

Grover, L. K. (1996). A fast quantum mechanical algorithm for database search. *Proceedings of the Twenty-Eighth Annual ACM Symposium on Theory of Computing - STOC '96*, 212–219. <https://doi.org/10.1145/237814.237866>

Langley, A., et al. Experimenting with Post-Quantum Cryptography (2019), Google & Cloudflare. <https://www.imperialviolet.org/2018/12/12/cecpq2.html> ←

Mandal, S., Anand, R., Rahman, M., Sarkar, S., & Isobe, T. (2024). Implementing Grover's on AES-based AEAD schemes. *Scientific Reports*, 14(1). <https://doi.org/10.1038/s41598-024-69188-8>

Microsoft Azure Quantum, Aghaee, M., Alcaraz Ramirez, A., Alam, Z., Ali, R., Andrzejczuk, M., Antipov, A., Astafev, M., Barzegar, A., Bauer, B., Becker, J., Bhaskar, U. K., Bocharov, A., Boddapati, S., Bohn, D., Bommer, J., Bourdet, L., Bousquet, A., Boutin, S., ... Zilke, J. (2025). Interferometric

## 12. INTERNATIONAL EUROPEAN CONGRESS ON ADVANCED STUDIES IN BASIC SCIENCES



single-shot parity measurement in InAs–Al hybrid devices. *Nature*, 638(8051), 651–655. <https://doi.org/10.1038/s41586-024-08445-2>

National Institute of Standards and Technology. (2025, April 22). Post-Quantum Cryptography | CSRC. National Institute of Standards and Technology (NIST). <https://csrc.nist.gov/projects/post-quantum-cryptography>

Paquin, C., Stebila, D., & Tamvada, S. (2021). Post-Quantum TLS Without Handshake Signatures. In *Proceedings of the 2021 ACM SIGSAC Conference on Computer and Communications Security (CCS)*. DOI: 10.1145/3460120.3485364 ↵

Regenscheid, A. (2024). Transition to Post-Quantum Cryptography Standards. National Institute of Standards and Technology. <https://nvlpubs.nist.gov/nistpubs/ir/2024/NIST.IR.8547.ipd.pdf>

SaberiKamarposhti, M., Ng, K.-W., Chua, F.-F., Abdullah, J., Yadollahi, M., Moradi, M., & Ahmadpour, S. (2024). Post-quantum healthcare: A roadmap for cybersecurity resilience in medical data. *Heliyon*, 10(10), e31406. <https://doi.org/10.1016/j.heliyon.2024.e31406>

Schwabe, P., Stebila, D., & Wiggers, T. (2020). Post-Quantum TLS Without Handshake Signatures. *Proceedings of the 2020 ACM SIGSAC Conference on Computer and Communications Security*, 1461–1480. <https://doi.org/10.1145/3372297.3423350>

Sosnowski, M., Wiedner, F., Hauser, E., Steger, L., Schoinianakis, D., Gallenmüller, S., & Carle, G. (2023). The Performance of Post-Quantum TLS 1.3. *Companion of the 19th International Conference on Emerging Networking EXperiments and Technologies*, 19–27. <https://doi.org/10.1145/3624354.3630585>

Wang, Z., Wei, S., Long, G.-L., & Hanzo, L. (2022). Variational quantum attacks threaten advanced encryption standard based symmetric cryptography. *Science China Information Sciences*, 65(10), 200503. <https://doi.org/10.1007/s11432-022-3511-5>



# 12. INTERNATIONAL EUROPEAN CONGRESS ON ADVANCED STUDIES IN BASIC SCIENCES

May 16-18, 2025, Albania  
University Metropolitan Tirana

## İlgili makama;

12. ULUSLARARASI AVRUPA TEMEL BİLİMLERDE İLERİ ARAŞTIRMALAR KONGESİ 16-18 Mayıs 2025 tarihleri arasında Tiran Metropolitan Üniversitesi'nde 21 farklı ülkenin akademisyen/araştırmacılarının katılımıyla gerçekleşmiştir. Kongre kapsamında sunumu yapılan 212 bildirinin 104 adeti Türkiye'den katılımcılar tarafından; 1081 bildiri ise 21 ülkeden katılımcılar tarafından sunulmuştur. Kongre 16 Ocak 2020 Akademik Teşvik Ödeneği Yönetmeliğine getirilen “*Tebliğlerin sunulduğu yurt içinde veya yurt dışındaki etkinliğin uluslararası olarak nitelendirilebilmesi için Türkiye dışında en az beş farklı ülkeden sözlü tebliğ sunan konuşmacının katılım sağlaması ve tebliğlerin yarıdan fazlasının Türkiye dışından katılımcılar tarafından sunulması esastır.*” değişikliğine uygun düzenlenmiştir.

Bilgilerinize arz edilir,

Saygılarımla,

**Prof. Dr. Nikolla Civici**  
Rector of University Metropolitan Tirana  
Honorary President of Congress



UNIVERSITY METROPOLITAN TIRANA  
FACULTY OF ENGINEERING AND ARCHITECTURE  
Str. "Sotir Kolea", Qyteti Studenti, Tirana, Albania

## TO WHOM IT MAY CONCERN

It has been deemed appropriate for the researchers named below to be assigned to "INTERNATIONAL EUROPEAN CONFERENCE ON INTERDISCIPLINARY SCIENTIFIC RESEARCH" organizing committee.

1. Msc. Donika Plakolli – UMT, Albania - Head of Organizing Committee
2. Prof. Dr. Agim Selenica – UMT, Albania
3. Assoc. Prof. Dr. Anna Yunitsyna – UMT, Albania
4. Dr. Sonila Daiu – UMT, Albania
5. MSc. Fatlinda Struga – UMT, Albania
6. Dr. Ernest Shtepani – UMT, Albania

"INTERNATIONAL EUROPEAN CONFERENCE ON INTERDISCIPLINARY SCIENTIFIC RESEARCH" is scheduled at May 16-18, 2025, at the premises of University Metropolitan Tirana.

Best regards,

Prof. Dr. Nikolla Civici  
Rector of UMT

Tirana, June 14, 2024

