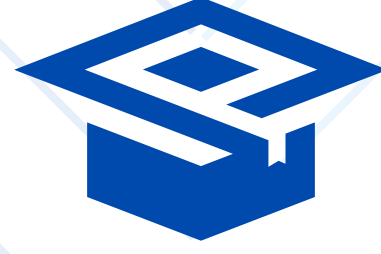


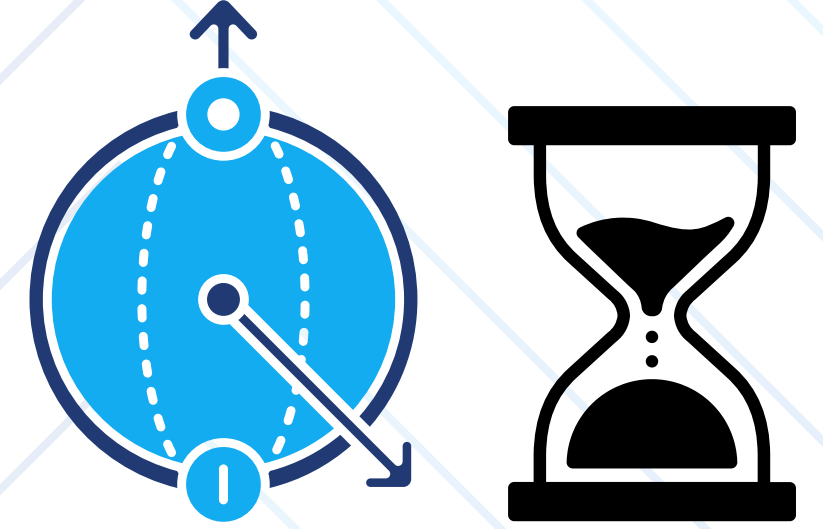
16–18 Mayıs 2025



Trakya Üniversitesi

WILLOW KUANTUM ÇİPİ VE KUANTUM SONRASI GÜVENLİĞİ: GELECEK TEHDİT ANALİZİ VE GÜVENLİK REHBERİ

Mehmet ALTINKILIÇ
Gökhan TUNCAY



**Bugün şifrelediğimiz
veriler, 10 yıl sonra da
güvende olacak mı?**

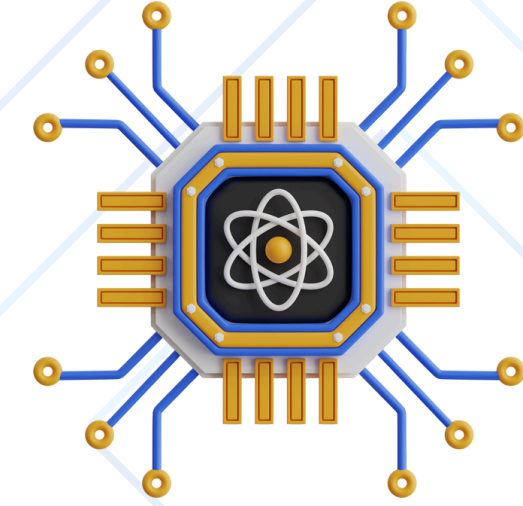
01

KLASİK VS KUANTUM BİLGİSAYARLAR



Klasik bilgisayarlar, tüm işlemleri bit adı verilen küçük bilgi parçalarıyla yapar. Bu bitler ya 0 ya da 1 olabilir. Bu yöntemle günlük hayattaki birçok problemi çözüyoruz. Ancak büyük ve karmaşık sorunları çözmek uzun zaman alabiliyor.

VS



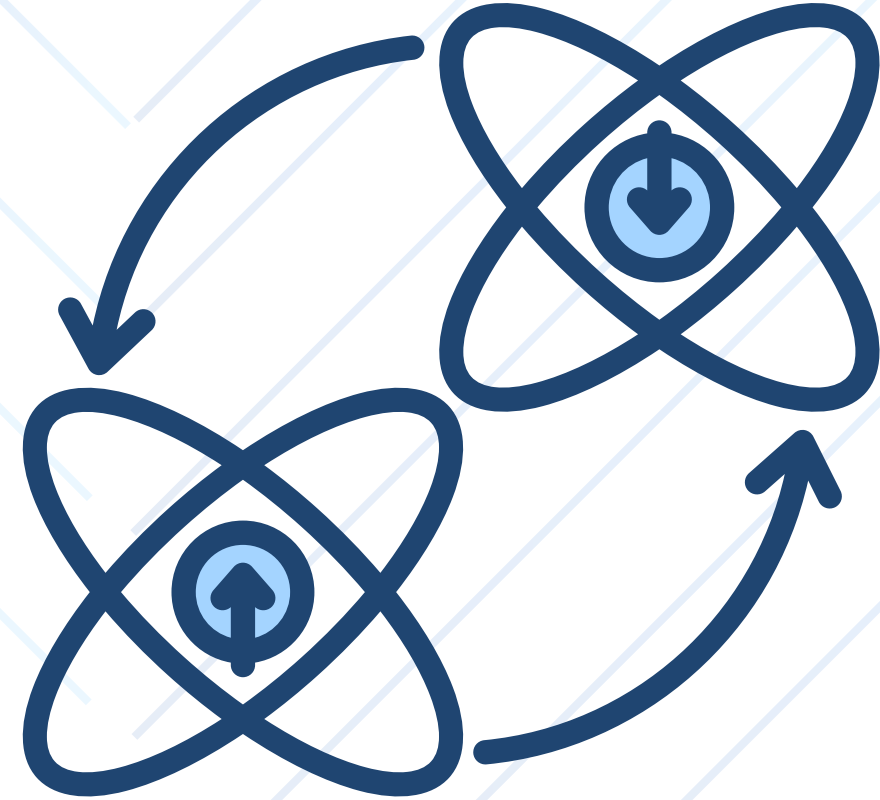
Kuantum bilgisayarlar ise bilgiyi kubitler ile işler. Kubitler aynı anda hem 0 hem de 1 olabilirler. Bu özellikleri sayesinde kuantum bilgisayarlar, karmaşık hesaplamaları çok daha hızlı yapabilir ve klasik bilgisayarların çözemediği problemleri çözebilirler.

KUBİT NASIL ÇALIŞIR?

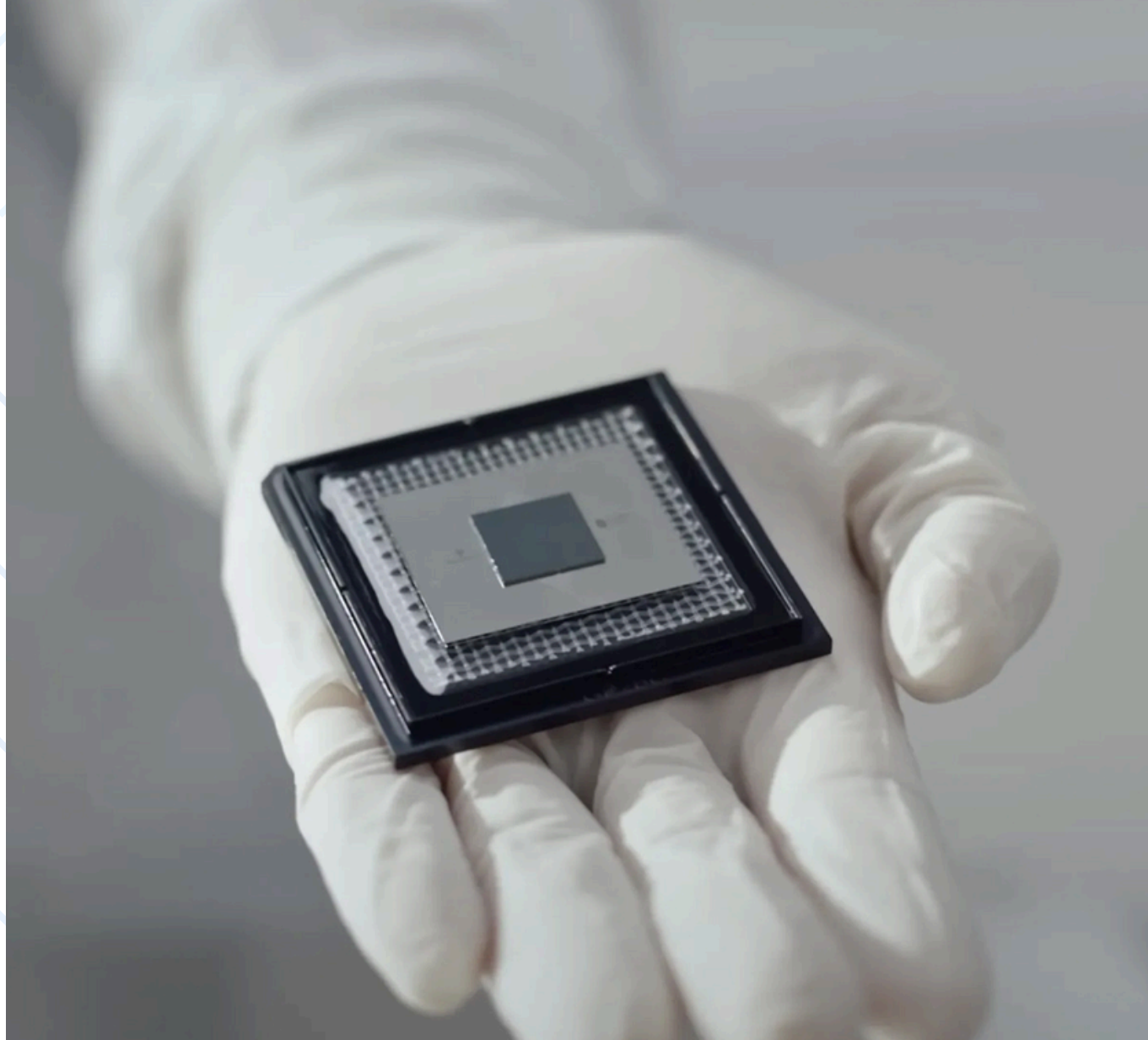


Kubit, kuantum fiziği sayesinde aynı anda hem 0 hem de 1 durumunda olabilir. Bu özelliğe “süperpozisyon” denir.

Kubit’ler birbirine bağlanabilir. Bu özel duruma “dolanıklık” denir. Dolanık iki kubit arasında mesafe fark etmeksizin bir etkileşim olur. Birinde yapılan değişiklik; diğerini anında etkiler.



WILLOW KUANTUM ÇİPİ VE ÖNEMİ



Willow, Google'ın geliştirdiği yeni nesil bir kuantum çipi. İçinde 105 kubit bulunuyor. Ancak onu diğerlerinden farklı ve özel yapan şey yalnızca kubit sayısının artmış olması değil. Willow, hata düzeltme konusunda önceki çiplere göre çok daha başarılı. Daha önce geliştirilen kuantum çiplerde hata oranı oldukça yüksekti ve bu da güvenilir sonuçlar almayı zorlaştırıyordu. Willow sayesinde ilk defa mantıksal hata oranı fiziksel hata oranının altına indi. Böylece kuantum bilgisayarlar gerçek hayattaki karmaşık problemleri çözmeye bir adım daha yaklaştı.

HATA DÜZELTME NEDEN ÖNEMLİ?



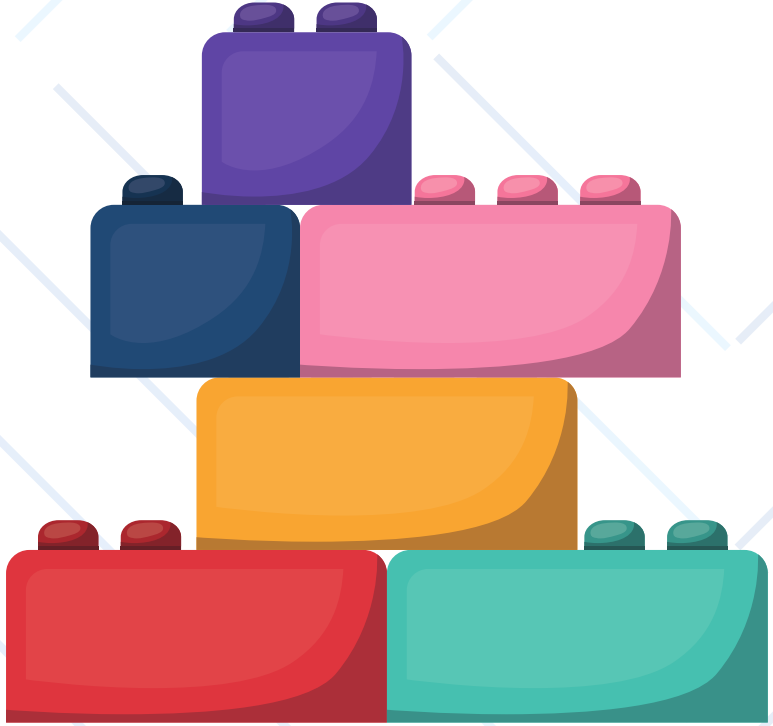
Mantıksal hata oranı, fiziksel hata oranının altına indi.



Artık daha uzun ve karmaşık işlemler mümkün.



TOPOLOJİK KUBİTLER: MICROSOFT'UN KARARLI KUANTUM YAKLAŞIMI

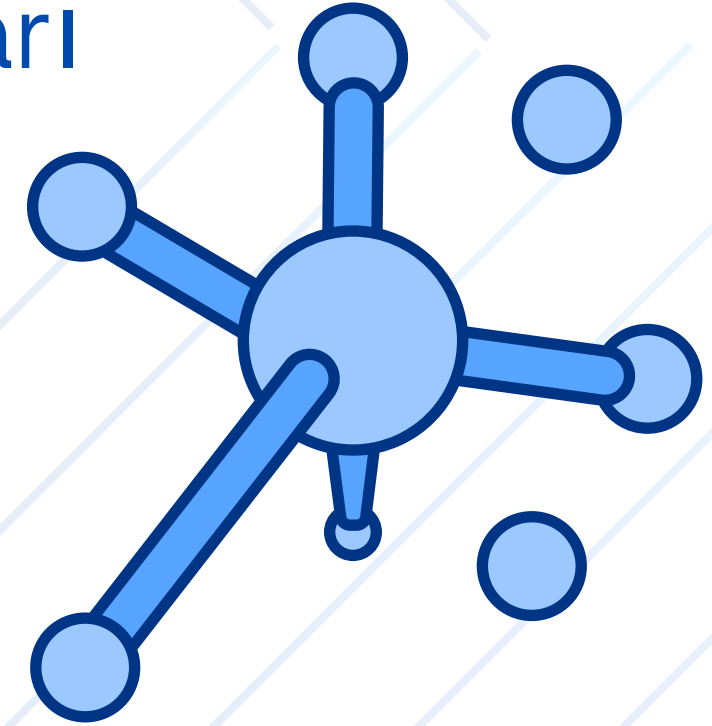


Topolojik Yaklaşım

Bilgiyi fiziksel konum yerine geometrik yapıda (lego tarzı) saklar. Bu nedenle daha stabil ve dayanıklıdır.

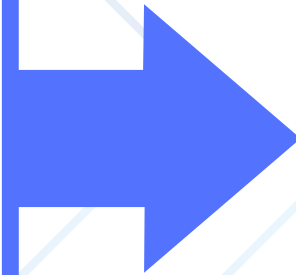
Majorana Fermiyonları

Topolojik kubitleri oluşturan; kendi anti-parçacığı olan egzotik parçacıklardır. Hataları önler, kararlılığı artırır.



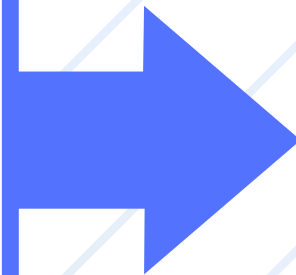
KUANTUM BİLGİSAYARLAR ŞİFRELERİ NASIL KIRAR?

Shor Algoritması

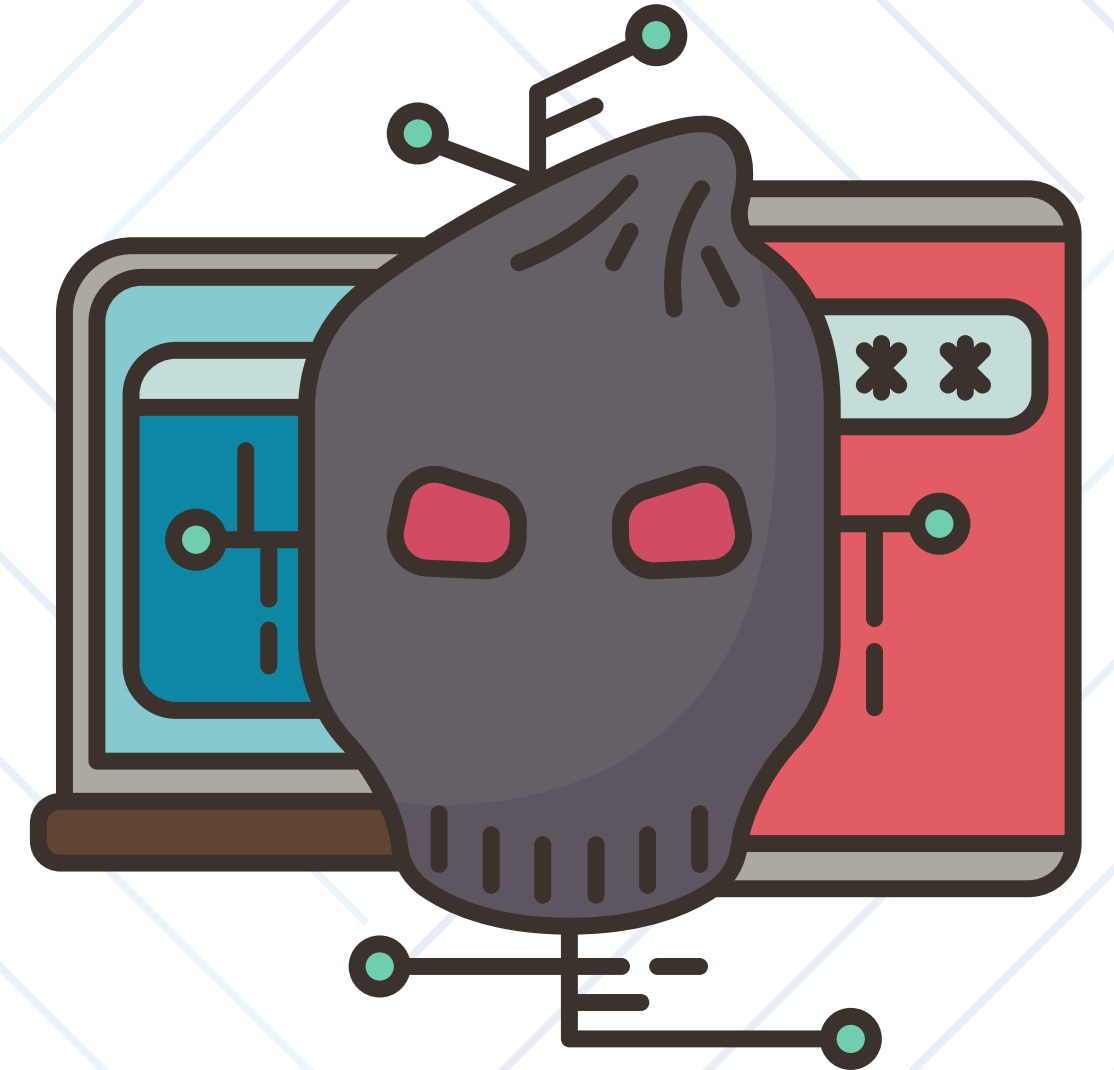


RSA / ECC gibi
algoritmaların
güvenliğini tamamen
ortadan kaldırır.

Grover Algoritması



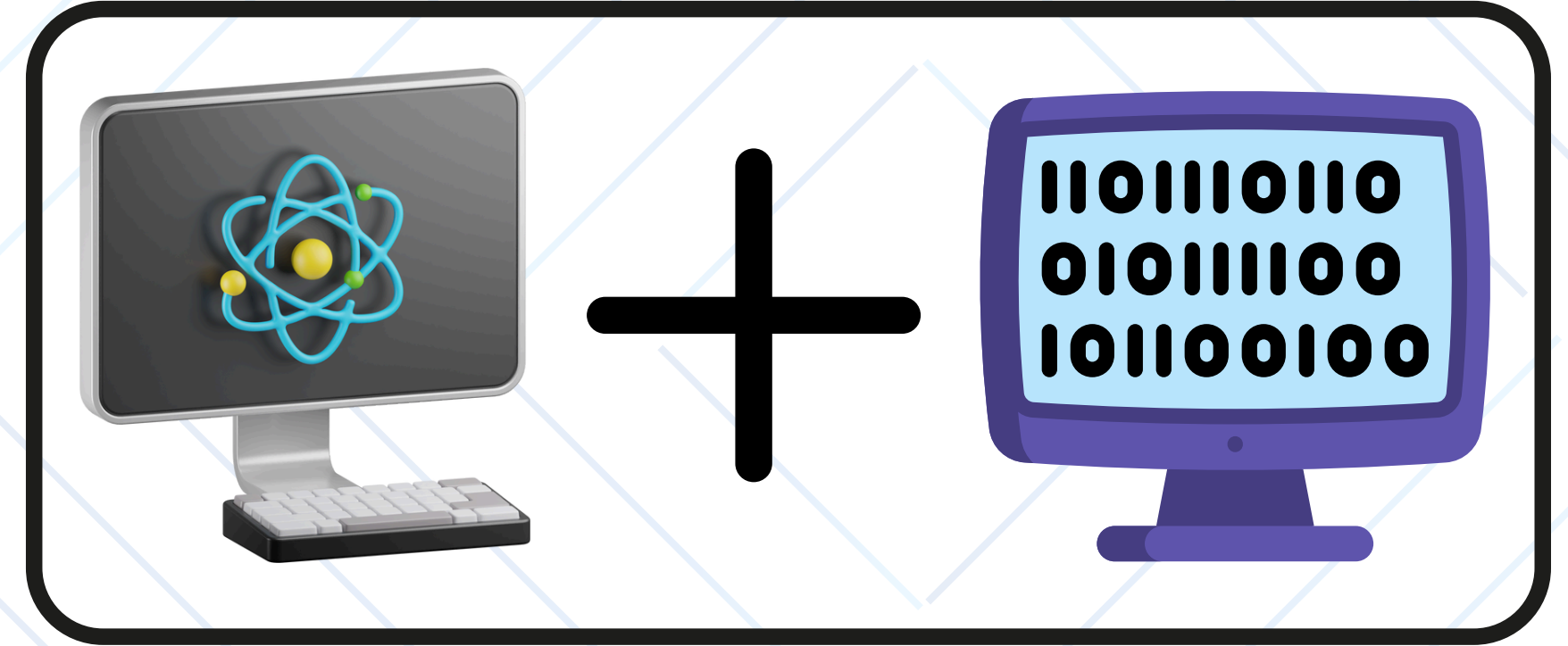
AES güvenliğini anahtar
uzunluğu/2 düzeyine
indirir.



VQAA NEDİR?

Variational Quantum Algorithmic
Attacks

Varyasyonel Kuantum Algoritmik
Saldırılar



Hibrit saldırı: Klasik +
Kuantum birleşimi

Daha az kubit ile etkin saldırılar

WILLOW'UN ŞİFRE KIRMA KAPASİTESİ



AES-128 ile şifrelenen bilgilerin klasik bilgisayarla kırılması neredeyse imkânsız kabul edilirken;

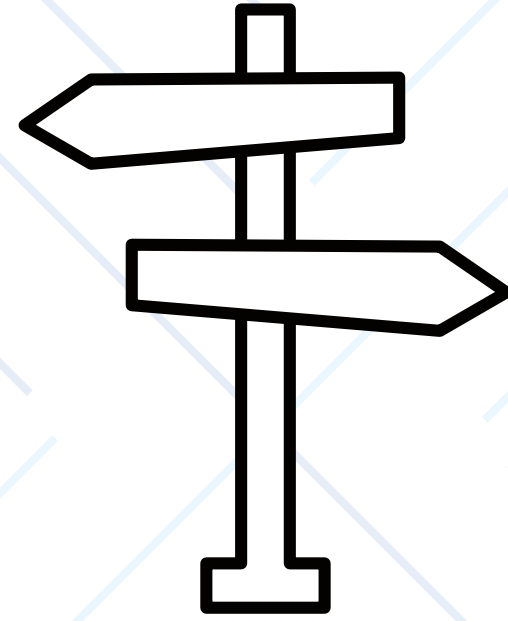


Willow kuantum çipi, paralel Grover algoritmasıyla bu süreyi yaklaşık 1.5 yıla indiriyor.

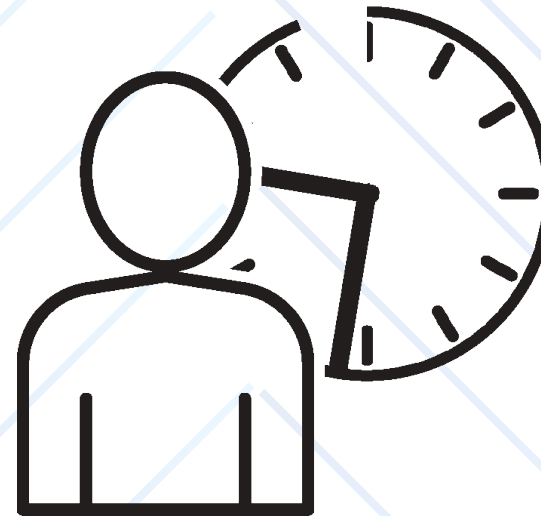
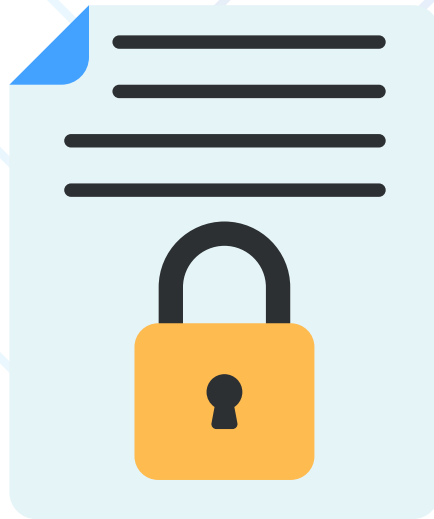


“STORE NOW, DECRYPT LATER” TEHDİDİ

Bugün verilerimiz güvende,
peki yarın?



Gizli sandığımız bilgiler, zamanı
geldiğinde ifşa olabilir.



10

POST-KUANTUM KRİPTOGRAFI (PQC)



KYBER: Kuantuma dayanıklı anahtar değişim algoritması.

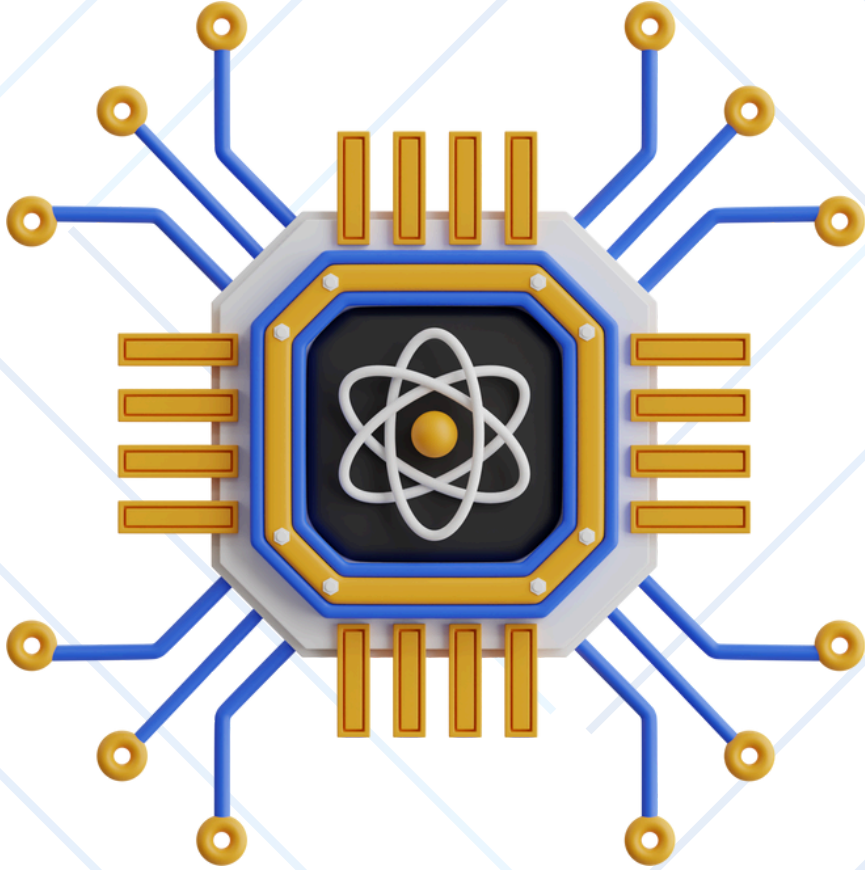


DILITHIUM: Sayısal imzalar için hızlı ve güvenli algoritma.



SPHINCS+: Uzun vadeli arşivler için hash tabanlı imza sistemi.

HİBRİT KRİPTOGRAFI – GEÇİŞ SÜRECİ

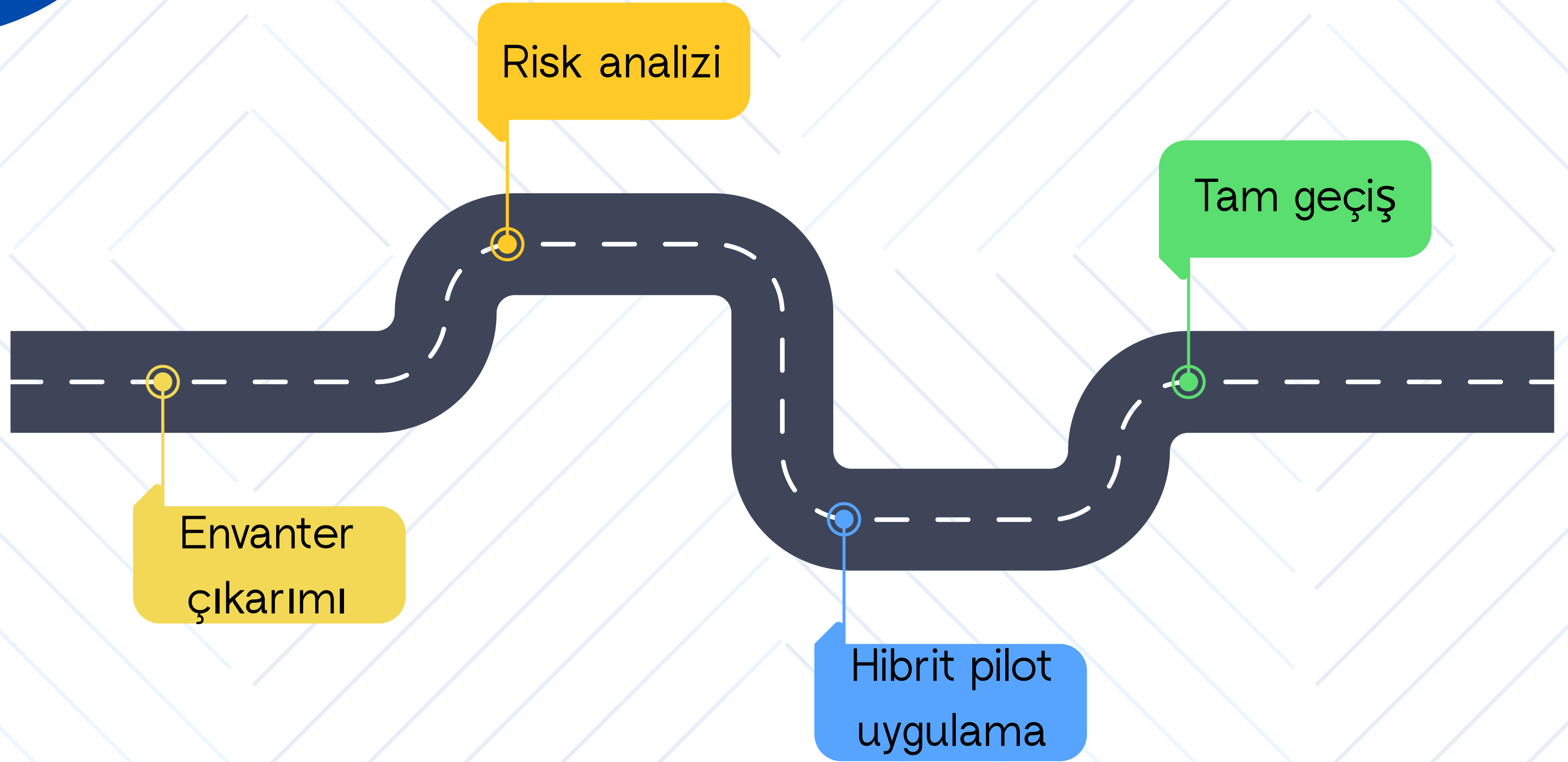


Klasik ve post-kuantum algoritmalar birlikte kullanılmalı.

Örnek olarak **X25519 + Kyber** kombinasyonu ile geleceğe karşı koruma sağlanır.



NIST YOL HARİTASI VE GEÇİŞ REHBERİ



NELER YAPILMALI?



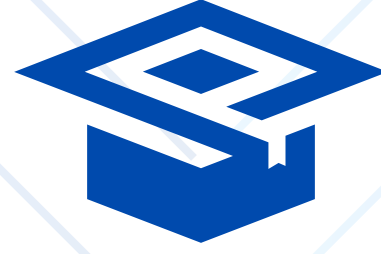
AES-256 kullanımı: Kuantum tehditlerine karşı daha güçlü bir simetrik şifreleme sağlar.



Hibrit TLS protokolü: Klasik ve kuantuma dayanıklı algoritmalar birlikte kullanılır.



SPHINCS+ tercih edilmesi: Uzun vadeli veri gizliliğini korumak için kuantuma dirençlidir.



Trakya Üniversitesi

**İLGİNİZ İÇİN TEŞEKKÜR EDERİZ.
SORULARINIZI ALABİLİRİZ.**