**Karadeniz Fen Bilimleri Dergisi**
The Black Sea Journal of Sciences
DOI: 10.31466/kfbd.1695525
ISSN (Online): 2564-7377
https://dergipark.org.tr/tr/pub/kfbd

Araştırma Makalesi / Research Article

# Kuantum Sonrası Kriptografi Alanında Türkiye'de Lisansüstü Eğitim ve Akademik Çalışmalar Üzerine Sistematik Bibliyometrik Analiz

# Systematic Bibliometric Analysis on Graduate Education and Academic Studies in Post-Quantum Cryptography in Türkiye

Kübra SEYHAN[1]*, Sedat AKLEYLEK[2], Ahmet Faruk DURSUN[3]

## Öz

Bu çalışmada, kuantum sonrası kriptografi alanında Türkiye'deki akademik araştırmaların güncel durumu ele alınarak nitelikli araştırmacı yetiştirilmesi odağında neler yapıldığının gösterilmesi amaçlanmıştır. Bu hedef doğrultusunda kuantum sonrası kriptografi (post-quantum cryptography - PQC) tanımı yapılarak uluslararası kuruluşlar tarafından duyurulan gereksinimler, PQC'de yaygın kullanılan kriptosistem aileleri ve bazı açık problemler ele alınmıştır. Türkiye'de PQC alanında nitelikli araştırmacıların ortaya çıkma süreci ve yapılan akademik çalışmalara bir bakış sunabilmek için bibliyometrik analizler yapılmıştır. İlk analiz için ulusal tez merkezi üzerinden sunulan verilere erişim amacıyla sistematik bir araştırma yöntemi oluşturularak 42 anahtar kelime üzerinden ilgili tezler belirlenmiştir. Oluşturulan kriterleri karşılayan ve Türkiye'de bu alanla ilişkili olduğu tespit edilen açık erişimli 47 lisansüstü tez özelinde sınıflandırma, nitelik (PQC açısından katkı, yazılan dil, yüksek lisans doktora dağılımı vb.) inceleme, yıllar içindeki gelişim, üniversite/enstitü/anabilim dalı özelinde dağılım, cinsiyet ve danışman değerlendirmeleri noktasında analizler gerçekleştirilmiştir. İkinci analiz için Türkiye adresli araştırmacıların bu alanda yaptığı güncel akademik çalışmalara (makale/bildiri/kitap/kitap bölümü/derleme) erişimde Scopus veritabanı üzerinden elde edilen veriler kullanılmıştır. İki farklı analiz ile sunulan bilgiler kriptografinin güncel konularından biri olan PQC alanında Türkiye'deki güncel durumun bir resmini sunmakla birlikte kariyer planlaması yapan araştırmacılar için hem yol haritası olma hem de kaynaklara erişim noktasında bir rehber niteliğindedir.

**Anahtar Kelimeler:** Kuantum sonrası kriptografi, Bibliyometrik analiz, Sistematik analiz, Bilgi güvenliği, Siber güvenlik, Kuantum sonrası güvenli kriptosistemler.

## Abstract

This study aims to provide a snapshot of the current status of academic research in Turkey in the field of PQC and the processes focused on training qualified researchers. The PQC concept, post-quantum secure cryptosystem families, the requirements of international organizations for a candidate proposal, and some open problems are discussed. To provide an overview of the education process of qualified researchers in the field of post-quantum cryptography in Türkiye and academic studies, bibliometric analyses are conducted. Firstly, a systematic research method is defined to access data via the national thesis center, and 42 keywords are used to determine relevant theses. 47 relevant and open-access graduate theses that meet the criteria are analyzed by including the nature of the theses, their development over the years, and their distribution in terms of university/institute/department, gender, and supervisor. In the second analysis, a systematic bibliometric analysis is conducted in the Scopus database to access current academic studies (articles/proceedings/books/book chapters/reviews) conducted by researchers from Türkiye in the field of PQC. In summary, these analyses provide a picture of PQC's current status and serve as both a roadmap and a guide for researchers planning their careers regarding access to resources.

**Keywords:** Post-quantum cryptography, Bibliometric analysis, Systematic analysis, Information security, Cyber security, Post quantum secure cryptosystems.

[1,3]Ondokuz Mayıs Üniversitesi, Bilgisayar Mühendisliği Bölümü, Samsun, Türkiye
[2]Tartu Üniversitesi, Bilgisayar Bilimleri Enstitüsü, Tartu, Estonya
[2]İstinye Üniversitesi, Bilgisayar Mühendisliği Bölümü, İstanbul, Türkiye

***Sorumlu Yazar/Corresponding Author:** kubra.seyhan@bil.omu.edu.tr

**Geliş/Received:** 08.05.2025 **Kabul/Accepted:** 09.02.2026 **Yayın/Published:** 04.03.2026

Seyhan K., Akleylek S., Dursun A. F., (2026). Kuantum Sonrası Kriptografi Alanında Türkiye'de Lisansüstü Eğitim ve Akademik Çalışmalar Üzerine Sistematik Bibliyometrik Analiz. *Karadeniz Fen Bilimleri Dergisi*, 16(1), 240-270. https://doi.org/10.31466/kfbd.1695525

## 1. Giriş

Haberleşme güvenliğinin sağlanmasında kullanılan simetrik ve açık anahtarlı kriptosistemler belirlenen standartlar ve oluşturulan protokollerle farklı uygulama alanlarında değişik formlarda aktif olarak kullanılmaktadır. İlkel kriptosistemlerin oluşturulması, 1976 yılında açık anahtarlı kriptosistem temellerinin atılması, 1970'li yıllarda Veri Şifreleme Standardı (DES) algoritmasının oluşturulması, 2000'li yıllarda simetrik kriptosistem standardı olarak Gelişmiş Şifreleme Standardı (AES)'in belirlenmesi vb. süreçler güvenli haberleşmeye olanak sağlayan kriptografik ilke sınıflarının günümüzde kullanılabilir hale gelmesindeki bazı önemli zaman dilimlerini tanımlamaktadır (Paar ve Pelzl, 2010). Benzer bir gelişmede 1990'lı yılların başında Shor (Shor, 1999) ve Grover (Grover, 1996) algoritmalarının önerilmesi ile kuantum bilgisayarların geliştirildiği dünyada geleneksel kriptosistemlerin güvenliğinin değişeceğinin gösterilmesi ile ortaya çıkmıştır. Grover algoritması ile $n$ girdili sıralanmamış veri bulunan bir veritabanından klasik bilgisayar hesaplama gücü ile $n/2$ aramada bulunan verinin kuantum bilgisayarlar ile $\sqrt{n}$ arama ile elde edilebileceği gösterilmiştir. Daha genel bir ifade ile kuantum bilgisayar dünyasında simetrik kriptosistemlerde anahtar güvenliğinin Grover algoritması ile yarıya düşeceğinin gösterilmesi ile tanımlanabilmektedir. Bu değişimin sayısal değerlerle gösterilmesi ve kuantum sonrası etkinin değerlendirilebilmesi için (Gheorghiu ve Mosca, 2019) çalışması ile gerçekleştirilen sonuçlar Tablo 1'de sunularak simetrik şifre standardı olarak kullanılan AES için üç farklı güvenlik seviyesinin kuantum sonrası güvenlik seviyelerindeki değişim ele alınmıştır.

**Tablo 1.** AES'in kırılması için gerekli kuantum kaynak tahminleri (Gheorghiu ve Mosca, 2019).

| **Simetrik**- | AES-128 | AES-192 | AES-256 |
|---|---|---|---|
| Paralel Kuantum Arama Sayısı | $\sim 2^{80}$ | $\sim 2^{140}$ | $\sim 2^{215}$ |
| Kuantum Güvenlik Seviyesi | 106 | 139 | 172 |
| Süre | 1 yıl | 1 yıl | 1yıl |
| - Kapı başına fiziksel hata oranı $10^{-4}$ için elde edilen sonuçlar. | | | |

Tablo 1'de verilen sonuçlar yorumlandığında 128-bit güvenlik sunan simetrik AES-128 algoritması Grover algoritması ile yaklaşık 1 yılda gerçekleştirilecek $2^{80}$ paralel kuantum arama sayısı 106-bit güvenlik sağlayabilecek hale gelecektir. Güvenlik seviyesini yaklaşık olarak yarıya indiren bu etkinin anahtar boyutunun iki katına çıkarılması ile ortadan kaldırılabileceği bilinmektedir. Açık anahtarlı kriptosistemler ise güvenliklerini oluşturan tamsayı çarpanlara ayırma ve ayrık logaritma problemlerini uygun parametre seçim durumlarında polinom zamanda çözebilen algoritma bilinmediğinden güvenli iletişimin bir parçası olarak birçok internet güvenliği protokolünde ve güvenli iletişim ihtiyacı olan senaryoda aktif olarak kullanılmaktadır (Chi ve ark., 2015). Shor algoritması ile herhangi bir boyuttaki sayıyı büyük ölçekli kuantum bilgisayar hesaplama gücü

kullanılarak polinom zamanda çarpanlarına ayırabilme ve ayrık logaritmaları hesaplayabilme özelliği gösterdiğinden açık anahtarlı kriptosistemler için kuantum bilgisayarlar dünyasında yeni bir çağ başlamıştır (Ekerå, 2019; Seyhan ve Akleylek, 2022). Ölçeği büyük kuantum bilgisayarların inşa edilmesi üzerine yapılan çalışmalar beraberinde kuantum bilgisayarlar varlığında açık anahtarlı kriptosistemlerin güvenliğinin nasıl etkileneceği ve ne gibi önlemler alınması gerektiği sorusunu ortaya çıkarmıştır. Tablo 1'de sunulan sonuçlara benzer şekilde açık anahtarlı kriptosistemlerin kuantum bilgisayar çağında nasıl etkileneceğinin gösterilmesi için ise Tablo 2'de anahtar paylaşımı ve elektronik imza açısından yaygın olarak kullanılan Rivest-Shamir-Adleman (RSA) kriptosisteminin üç farklı güvenlik seviyesi ele alınmıştır.

**Tablo 2.** RSA'nın kırılması için gerekli kuantum kaynak tahminleri (Gheorghiu ve Mosca, 2019).

| **Açık Anahtarlı**$^{+}$ | RSA-3072 | RSA-7680 | RSA-15360 |
|---|---|---|---|
| Kübit Sayısı | $6.41 \times 10^{8}$ | $7.70 \times 10^{10}$ | $4.85 \times 10^{12}$ |
| Süre | 24 saat | 24 saat | 24 saat |

+ Kapı başına fiziksel hata oranı $10^{-3}$ için elde edilen sonuçlar.

Tablo 2'de gösterildiği üzere 128-bit güvenlik sunan açık anahtarlı RSA-3072 algoritması $6.41 \times 10^{8}$ kübit (kuantum bilgisayarlarda bilginin temsil edilme formu) sayısı içeren kuantum bilgisayar ile yaklaşık olarak 24 saatte kırılabileceği bilinmektedir. Her ne kadar beklenen ölçekte bir kuantum bilgisayar henüz inşa edilmese de yapılan çalışmalar yakın gelecekte bu teknolojilerin elde edilebileceğini göstermektedir. Bu durum ise kuantum hesaplama gücünün ortaya çıktığı dünyada özellikle açık anahtarlı kriptosistemlerin güvenliğinin sağlanması üzerine çalışmalar yapılmasını zorunlu kılmış ve kuantum sonrası kriptografi kavramının doğmasına neden oluşturmuştur (Dam ve ark., 2023). Endüstri ve akademi çalışmaları için yeni bir alan oluşturan bu gelişme için uluslararası birçok kurum ve kuruluş araştırma, geliştirme ve standartlaştırma süreçlerinin başlatılması ile ilgili çalışmalar yapmıştır. Özellikle Amerika Birleşik Devletleri merkezli Ulusal Standartlar ve Teknoloji Enstitüsü (NIST), Uluslararası Standartlar Örgütü, İnternet Mühendisliği Görev Gücü ve Avrupa Telekomünikasyon Standartları Enstitüsü tarafından yönetilen standartlaşma çabaları bu anlamda önemli rol oynamıştır (Joseph ve ark., 2022). Bu açıdan en büyük etki NIST tarafından dünya genelinde başlatılan standartlaşma sürecinde (NIST, 2017) kuantum bilgisayar hesaplama gücünün ortaya çıkacağı çağ için açık anahtarlı kriptografi standart veya standartlarının (dijital imza ve açık anahtarlı şifreleme ve anahtar oluşturma) belirlenmesi ile ortaya çıkmıştır. Bu süreçte verimlilik ve uygulanabilirlik endişelerinden dolayı geleneksel kriptosistemlerde tercih edilmeyen ancak kuantum sonrası güvenli olduğu düşünülen kod, kafes, özet, çok değişkenli polinom sistemleri ve izojeni-tabanlı kriptosistem ailelerinde yer alan algoritmalar ile öneriler sunulmuş ve tüm süreçte güvenlik, maliyet, performans, algoritma ve uygulama

karakteristikleri gibi bileşenler açısından değerlendirmeler yapılmıştır (Kasapbaşı, 2019; Alagic, ve diğerleri, 2022). Standartlaşma sürecinde yer alan qTESLA, FrodoKEM ve Newhope isimli üç adayda Türkiye adresli araştırmacılar da yer almıştır. 13 Ağustos 2024 tarihinde standart algoritmaların duyurulması (NIST, 2024) ile tamamlanan standartlaşma sürecinde kafes-tabanlı CRYSTALS-KYBER algoritması FIPS 203 ile Modül-Kafes Tabanlı Anahtar-Kapsülleme Mekanizması Standardı olarak belirlenmiştir. Dijital imza standartları olarak ise; kafes-tabanlı CRYSTALS-Dilithium FIPS 204 ile Modül-Kafes Tabanlı Dijital İmza Standardı, kafes-tabanlı FALCON (FIPS süreci henüz tamamlanmadı) ve özet-tabanlı SPHINCS+ algoritması FIPS 205 ile Durumsuz Karma Tabanlı Dijital İmza Standardı olarak belirlenmiştir (NIST, 2024). NIST standartlaşma süreci dördüncü turu devam ederken kuantum sonrası kriptografi sürecinde kısa imza ve hızlı doğrulama içeren imzalama şemalarının belirlenmesi amacıyla 2022 yılında yeni bir çağrı duyurmuştur (NIST, 2022). Bu çağrıda genel amaçlı kuantum sonrası güvenli imza şemalarının oluşturulması hedeflenmiştir. Ana amaç kuantum sonrası güvenli imza şemalarında kafes varsayımlarından farklı varsayımların içerilmesi veya kafes varsayımı takip edilecekse de performans olarak standart kafes-tabanlı imza şemalarından önemli ölçüde daha iyi performans göstermesi istenmiştir. Bu süreçte ikinci tura geçmeye hak kazanan 14 imzalama şeması 24 Ekim 2024 tarihinde kod-tabanlı CROSS ve LESS, izojeni-tabanlı SQIsign, kafes-tabanlı HAWK, çok-taraflı hesaplama-tabanlı Mirath, MQOM, PERK, RYDE ve SDitH, çok değişkenli MAYO, QR-UOV, SNOVA ve UOV ve simetrik-tabanlı FAEST olarak duyurulmuştur (NIST, 2025). Her ne kadar standart algoritmaların belirlenmesi üzerine çalışmalar yapılsa da bilinen bir gerçek kriptografide geçişlerin zaman almasıdır. Özellikle kuantum sonrası güvenli algoritmaların genel olarak mevcut algoritmalara kıyasla kötü performans sergilemesi, standartlaşma ve sonrası süreçlerinde adaptasyon, entegrasyon ve uygulama alanlarında yapılacak çalışmaların birçok niteliğinin olması bu alanda sürecin çok daha yeni başladığını ve devam etmesi gerektiğini tanımlamaktadır (Joseph ve ark., 2022). Kuantum sonrası güvenli algoritmaların farklı uygulama alanları ve kullanım senaryoları özelinde uygulanması ve değerlendirilmesi, sistem performansını ve uyumluluğunu korurken ortaya çıkan kuantum hesaplama tehditlerine karşı teknik ve operasyonel zorlukların ele alınması, geleneksel kriptosistemleri içeren hibrit kriptografik çözümlerin tasarlanması, mevcut sistemlerle birlikte çalışılabilirliğin sağlanması ve yeni standartlara uyumluluk sürecinin takip edilmesi gibi durumlar ele alınması gereken süreçlerden sadece birkaçını tanımlamaktadır (CISA, 2024; Hasan ve ark., 2024). Dolayısıyla farklı tasarım bileşenleri ve mimarileri içeren kuantum bilgisayarlar sonrası güvenli açık anahtarlı kriptosistem tasarımı ve uygulaması (şifreleme, anahtar değişimi, kimlik doğrulama, anahtar paketleme, dijital/elektronik imza vb.), literatürde önerilen yaklaşımların verimli ve uygulamalı senaryolarının oluşturulması, aritmetik olarak iyileştirmelerin tasarlanması ve/veya aritmetik yöntemlerin adaptasyonu, verimli donanım uygulamalarının gerçeklenmesi, kaynak açısından kısıtlı

veya kısıtlı olmayan haberleşme modelleri için kuantum sonrası güvenlik analizi vb. gibi araştırma alanları ve açık problemler kuantum sonrası güvenliği hem endüstrinin hem de akademinin ilgilendiği önemli bir alan haline getirmiştir.

### 1.1. Motivasyon

Shor algoritmasının önerilmesi ve büyük ölçekli kuantum bilgisayar geliştirme odağında yapılan çalışmaların hız kazanması ile ortaya çıkan kuantum sonrası kriptografi kavramı gelecekte güvenli haberleşmenin oluşturulması açısından oldukça önemlidir. Özellikle NIST tarafından başlatılan standartlaşma süreci bu alanda yapılan çalışmaların hızlanmasına ve önem kazanmasına sebep olmuştur. Teorik ve uygulamalı çeşitli zorlukları bulunan kuantum sonrası kriptografi alanında Türkiye'deki araştırmacıların ne gibi çalışmalar yaptığı ve nitelikli araştırmacıların hangi alanlarda nasıl yetiştirildiğinin belirlenmesi kuantum bilgisayarlar çağında Türkiye'de güvenliğin sağlanması noktasındaki bilinci ve hazırlığı tanımlamak açısından oldukça önemlidir. Bu açıdan daha önceden farklı çalışma konuları odağında yapılan bibliyometrik analiz incelemelerinin (Pekşen ve Barman, 2024; Küpçüoğlu ve ark., 2024) katkısı ve etkinliği temel motivasyonu ile kuantum sonrası kriptografi alanındaki ilk bibliyometrik analizi çalışmasının yapılması amaçlanmıştır. Bu amaç doğrultusunda bibliyometrik analize konu olacak tez ve literatür çalışmalarının kapsamlı olarak ele alınıp planlı, tekrar edilebilir ve şeffaf bir şekilde belirlenmesi için sistematik bir inceleme gerçekleştirilmiştir. Sistematik literatür taramasında takip edilen anahtar kelimeler oluşturma, veritabanı taraması için anahtar kelimeleri içeren sorguların tanımlanması, seçme ve eleme kriterlerinin belirlenmesi süreçleri takip edilerek Türkiye'de kuantum sonrası kriptografi alanında yapılan tez çalışmaları ve literatüre yönelik bibliyometrik analize konu olacak çalışmaların elde edilmesi amaçlanmıştır. Sistematik arama ve sorgulama ile elde edilen lisansüstü çalışmalar ve akademik çalışmalara yönelik bu bibliyometrik analiz çalışması ile nitelikli araştırmacıların yetiştirilmesi sürecinde odak noktasını oluşturan çalışmaların niteliği, hangi üniversitelerde ve anabilim dallarında kayda değer çalışmaların yapıldığı vb. gibi bileşenler ile hem bu alanda çalışma yapmak isteyen araştırmacılara rehber olmak hem de Türkiye'de bu alanda nelerin yapıldığının gösterilmesi motivasyonu baz alınmıştır. Bu bibliyometrik analiz ile sunulan sonuçlar güncel bir çalışma alanı olan kuantum sonrası kriptografi alanında uzmanlaşmak isteyen araştırmacıların bu alanda öncü konu başlıkları, gereksinimler, açık problemler ve Türkiye'de bu alanda ne gibi tezler yapıldığına dair analizler elde edebilecektir. Gerçekleştirilen bibliyometrik analizin bir alt bileşeni olarak Türkiye adresli araştırmacıların yaptığı akademik çalışmalar incelenerek kuantum sonrası kriptografi alanında ne gibi çalışmalar ve hangi odak noktaları ile bu çalışmalara erişilebileceğine dair bir yol haritası niteliğindedir.

### 1.2. Organizasyon

Bu çalışmanın kalanı şu şekilde organize edilmiştir. Kuantum Sonrası Kriptografi bölümünde kuantum sonrası kriptografi tanımı ve güvenli kriptosistem aileleri tanımlanarak bu alanda ifade edilen bazı gereksinimler ve açık problemler verilmiştir. Araştırma Yöntemi başlığında analiz kapsamında Yükseköğretim Kurulu (YÖK) tez ve Scopus veri tabanlarından sayısal verilerin elde edilmesinde takip edilen araştırma yöntemleri detaylandırılmıştır. Bibliyometrik Analiz bölümünde her bir araştırma yöntemi sonucu elde edilen veriler ile Türkiye'de kuantum sonrası kriptografi alanında yapılan tez ve akademik çalışmalara ait bibliyometrik analiz sonuçları sunulmuştur. Son bölümde ise sonuç ve genel değerlendirmeler ele alınmıştır.

## 2. Kuantum Sonrası Kriptografi

Kuantum bilgisayar geliştirme odağında yapılan çalışmalar ve Shor algoritması ile ortaya çıkan etki klasik kriptografinin yanı sıra kuantum kriptografi ve kuantum sonrası kriptografi kavramlarının ortaya çıkmasına neden olmuştur. Bu iki kavram her ne kadar aynıymış gibi düşünülse de kuantum bilgisayarlar sonrası dünyada güvenliği sağlamak için temel aldıkları odak noktalar farklı olduğundan kuantum sonrası kriptografinin kuantum kriptografi ile karıştırılmaması gerekmektedir. Bu çalışmada Türkiye'de kuantum sonrası kriptografi alanı özelinde analizler sunulacağı için bu kavramların nasıl birbirinden farklılaştığı verilen tanımlar ile detaylandırılacaktır.

*Tanım 1. Kuantum Kriptografi* (NIST, 2024): Yeni ve güvenli kriptosistemlerin oluşturulması için kuantum mekaniğinin sezgiye aykırı özelliklerini kullanarak temelini 20. yüzyılda ortaya çıkan kuantum fiziğine dayandıran kriptografi alt çalışma alanıdır. Verilerin kuantum tehditlere karşı korunmasında hesaplamalı zor matematiksel problemler yerine kuantum mekaniğinin özelliklerini kullanmaktadır.

*Tanım 2. Kuantum Sonrası Kriptografi* (NIST, 2017; NIST, 2024): Klasik kriptografinin bir evrimi olarak kriptosistem tasarımında kuantum bilgisayarlar varlığında bile çözülemez olduğuna inanılan hesaplamalı olarak zor matematiksel problemleri temel alan kriptografi olarak tanımlanır.

Tanım 1 ve Tanım 2 ele alındığında her iki kriptografi alt dalı da kuantum hesaplama gücü ile ortaya çıkacak etkinin ortadan kaldırılmasını hedeflese de bunu gerçekleştirirken temel aldığı bileşenler (kuantum mekaniği özellikleri, hesaplamalı zor matematiksel problemler) ile farklılık göstermektedir. Başka bir deyişle, kuantum kriptografisinde iletişim güvenliğini garanti altına alırken mesajların şifrelenmesi veya şifrelerinin çözülmesinde kuantum düzeyde maddenin öngörülemez doğasını temel alırken kuantum sonrası kriptografi de kuantum ataklara karşı dayanıklı olduğu bilinen ve hesaplamalı olarak çözülmesi zor olan matematiksel problemlere dayalı kriptosistemler

tasarlanmaktadır. Kuantum kriptografide en bilinen örnek kuantum anahtar dağıtımı (quantum key distribution) iken kuantum sonrası kriptografi için ise güvenli kriptosistem ailelerinde yer alan zor problemlere dayalı tasarlanan kriptosistemlerdir. Dolayısıyla, kuantum sonrası kriptografi, kuantum kriptografi anlamına gelmemektedir. Kuantum sonrası kriptografi kavramı çok daha geniş bir kapsama sahiptir. Bu analizde kuantum sonrası kriptografi odağında Türkiye'de yapılan çalışmalar analiz edileceği için Bölüm 2.1'de büyük ölçekli kuantum bilgisayarlar varlığında bile hesaplamalı olarak zor olduğu yıllardır bilinen ancak verimlilik ve kullanılabilirlik problemleri nedeniyle tercih edilmeyen kriptosistem aileleri tanıtılmaktadır.

### 2.1. Kuantum Bilgisayarlar Sonrası Güvenli Kriptosistem Aileleri

Bu bölümde büyük ölçekli kuantum bilgisayarların oluşturulduğu dünyada güvenli olabilecek başka bir deyişle ayrık logaritma veya çarpanlara ayırma problemlerinin yerini alabilecek kuantum bilgisayar hesaplama gücüne karşı güvenli olduğu bilinen hesaplamalı olarak zor problemleri içerdiği bilinen kafes, kod, özet, izojeni ve çok değişkenli polinom sistemlerine dayanan kriptosistem aileleri ele alınmıştır.

#### 2.1.1. Kafes Tabanlı Kriptosistem Ailesi

Ajtai fonksiyonu (Ajtai, 1996) ve eş zamanlı olarak NTRU şifreleme sisteminde (Hoffstein ve ark., 1999) kriptografik amaçlarda kafes yapısının kullanılması ile önem kazanan kriptosistem ailesidir. Özellikle kuantum saldırılara karşı varsayılan güvenlik, algoritmik verimlilik, basitlik ve paralelleştirilebilirlik, en kötü durum zorluğuna dayanan güçlü güvenlik kanıtları, çok yönlü ve güçlü kriptografik nesne yapısı sunabilme gibi özelliklere sahip olması kafes tabanlı kriptosistemleri ön plana çıkaran özellikler olarak bilinmektedir (Akleylek ve Seyhan, 2019; Peikert, 2016). Özellikle en kısa vektör problemi (shortest vector problem) gibi kafeslerdeki en kısa sıfır olmayan vektörü bulma odağında kararsız polinom zaman (nondeterministic polynomial-NP)-zorluğa sahip ve belirli seçim sınırları altında kuantum bilgisayarlar varlığında bile çözülemeyeceği bilinen problemler içermesi kuantum bilgisayarlar sonrası güvenli açık anahtarlı kriptosistem tasarımı için kafes-tabanlı kriptografik ilkeleri ön plana çıkarmıştır (Li ve ark., 2023). Bu üstünlük ise NIST'in standartlaşma sürecinde hem sayısal olarak hem de standart olarak seçilen kafes tabanlı CRYSTALS-Kyber, CRYSTALS-Dilithium ve FALCON algoritmaları ile bir anlamda tescil kazanmıştır. NIST'in imzalama şemaları için duyurduğu çağrıda ise kafes-tabanlı HAWK imzalama şeması ikinci tura geçmeye hak kazanmıştır (NIST, 2022).

### 2.1.2. Kod Tabanlı Kriptosistem Ailesi

Geleneksel olarak hata düzeltme kodlarının mesajlar güvenilir olmayan bir kanal üzerinden iletilirken bit hatalarını tespit etmek ve düzeltmek için kullanıldığı bilinmektedir. Kod tabanlı açık anahtar şifrelemede temel fikri ise iletim sırasında bir mesajın içeriğini gizlemek için hata düzeltme kodlarının kullanılması ile tanımlanmaktadır. Kod tabanlı kriptografinin temel güvenlik varsayımı, rastgele doğrusal bir kodun kodunu çözmenin zorluğudur (Niederhagen ve Waidner, 2017). Bu ailenin ilk kriptosistemi 1978'de Robert J. McEliece (Alagic ve ark., 2022) tarafından önerilen açık anahtar için bir üreteç matrisi ve özel anahtarı için Goppa kodu kullanan McEliece kriptosistemidir. Önerildiği zamandan beri kırılamadığı için McEliece hata düzeltme kodlarına dayalı birçok şifreleme ve imzalama şemasının tasarlanmasına olanak sağlamıştır. Oldukça hızlı olan çoğu kod tabanlı kriptografik sistem çok büyük anahtar boyutlarına sahip olmaktan muzdariptir. Daha yeni versiyon kriptosistemler, anahtar boyutlarını azaltma girişiminde kodlara daha fazla yapı getirmiştir, ancak eklenen yapı aynı zamanda bazı önerilere yönelik başarılı saldırılara da yol açmıştır. Kod tabanlı imzalar için bazı önerilerde çok büyük anahtar boyutları pahasına kısa imzalar sunsa da kod tabanlı kriptografi şifreleme şemalarıyla daha fazla başarı elde etmiştir (NIST, 2017; Akleylek ve Seyhan, 2021). Ağustos 2024'te NIST standartlaşma süreci tamamlanıp seçilen algoritmalar belirlendikten sonra NIST, standart kafes-tabanlı CRYSTALS–KYBER'a alternatif anahtar-kapsülleme mekanizması belirlemek için dördüncü tur değerlendirmesi için kod-tabanlı BIKE, Classic McEliece, HQC ve izojeni-tabanlı SIKE algoritmalarını seçmiştir. 11 Mart 2025 tarihli duyuruda kod-tabanlı HQC algoritması kuantum sonrası dünyada alternatif anahtar-kapsülleme mekanizması olarak seçilmiştir (NIST, 2025). NIST'in kısa imza ve hızlı doğrulama özelliklerini içeren imzalama şemalarının belirlenmesi için başlattığı çağrıda kod-tabanlı CROSS ve LESS imzalama şemaları ikinci tura geçmeye hak kazanmıştır (NIST, 2022).

### 2.1.3. Özet Tabanlı Kriptosistem Ailesi

Özet fonksiyonlar, keyfi uzunluktaki bit dizilerini nispeten kısa ve sabit uzunlukta özet değerlere eşleyen tek yönlü fonksiyonlardır. Çakışmalara karşı dayanıklılık, ters görüntü direnci ve ikinci ters görüntü direnci özellikleri ile tanımlanan kriptografik özet fonksiyonlar, kuantum algoritmalardan Grover algoritmasının ters görüntü ve çakışmaları hesaplamada hızlandırma sağlaması ile kuantum bilgisayarlar dünyasından etkilenirken Shor'un polinom zamanlı kuantum algoritmasından etkilenmediğinden özet fonksiyonlar kuantum sonrası güvenli açık anahtarlı kriptosistem tasarımı için iyi adaylardır. Tanım gereği bir özet fonksiyonunun tersini hesaplamak hesaplama açısından mümkün olmadığından, bu fonksiyonları kullanarak açık anahtar şifreleme

şemalarının nasıl oluşturulacağı bilinmese de yapı taşları olarak yalnızca özet fonksiyonları kullanılarak imza şemaları tasarlamak mümkün olmuştur (Niederhagen ve Waidner, 2017). Özet tabanlı imzalama şemaları herhangi bir güvenli özet fonksiyonları ile kullanılabilmeleri nedeniyle esnektir. Dolayısıyla, güvenli özet fonksiyonunda bir kusur keşfedilirse, özet tabanlı bir imza şemasının etkili kalmak için yalnızca yeni ve güvenli bir özet fonksiyonuna geçmesi gerekir. En iyi bilinen özet-tabanlı imzalama şeması 1979 yılında önerilen tek kullanımlık Lamport şemasıdır (Akleylek ve Seyhan, 2019). Takip eden yıllarda verimlilik açısından iyileştirilmiş birçok imzalama şeması önerilse de imzalama ve doğrulama zamanlamalarının karşılaştırılabilir olması açısından iyileştirilmeler yapılması üzerine çalışmalar yapılmış ve birçok özet-tabanlı şema önerilmiştir (Campagna ve ark., 2015). NIST standartlaşma süreci sonunda elektronik imza kategorisinde standart olarak seçilen SPHINCS+ özet-tabanlı kriptosistem ailesinde yer almaktadır.

### 2.1.4. Çok Değişkenli Polinom Sistemlerine Dayalı Kriptosistem Ailesi

1980'li yıllarda çok değişkenli polinom sistemleri temel alınarak kriptosistem tasarlama fikri ile sonlu cisimler üzerinde ikinci dereceden çok değişkenli denklem sistemlerine çözüm bulmanın belirli parametre seçim kısıtlarında çözümsüz veya zor olması gerçeği baz alınarak ortaya çıkmıştır. Genel anlamda yapılan işlemlerin sonlu bir cisim üzerinde yapılması ve şifre çözme aşamasında doğrusal sistem çözme odaklı işlemler yapılması çok değişkenli polinom sistemlerine dayalı şifreleme şemalarını verimli hale getirmiştir (Chen ve ark., 2016). Verimlilik sebebi ile birçok şifreleme şeması önerilse de bunların güvenliği ile ilgili problemler ortaya çıkmıştır (Ding ve ark., 2014). Dolayısıyla tarihsel olarak bakıldığında çok değişkenli polinom sistemleri kullanılarak imzalama şemalarının tasarlanmasında daha başarılı olduğu gözlemlenmiştir (Dubois ve ark., 2007). Bu açıdan iyi bilinen ve yaygın olarak kullanılan çok değişkenli polinom-sistemi tabanlı imza şemaları dengesiz yağ-sirke (Unbalanced Oil-Vinegar-UOV) (Patarin, 1996) ve en çok bilinen örneklerden birisi Rainbow (Ding ve Schmidt, 2005)'dur. Rainbow imzalama şemasının mevcut parametreler için güvensiz olduğu gösterilmiştir. Verimli uygulanabilirlik ile hız, hesaplama açısından düşük işlem maliyeti ve küçük imza boyutu sunma gibi avantajların yanı sıra büyük açık anahtar boyutu ve verimsiz şifre çözme süreçleri gibi bazı olumsuz özellikleri de olduğu bilinen kriptosistem sınıfıdır (Akleylek ve Seyhan, 2021). NIST standartlaşma süreci sonrasında elektronik imza algoritmaları için genel amaçlı kısa imza ve hızlı doğrulama içeren çağrıda çok değişkenli polinom sistemleri temel alınarak önerilen MAYO, QR-UOV, SNOVA ve UOV şemalar ikinci tura geçmeye hak kazanmıştır.

### 2.1.5. İzojeni Tabanlı Kriptosistem Ailesi

2000'li yılların başı ile önem kazanan temelleri 1980'li yıllarda Miller ve Koblitz'in eliptik eğriler kullanarak Diffie-Hellman anahtar değişimini (Miller, 1985; Koblitz, 1987) kriptografinin eski bir dalı olan eliptik eğri kriptografisine (elliptic curve cryptography-ECC) dayandıran kriptosistem ailesidir. Sonlu bir cisim üzerinde tanımlanmış iki eliptik eğri arasında bir izojeni bulmanın zorluğu ile tanımlanan bu kriptosistemler küçük anahtar ve imza boyutu sunabilme özellikleri ile verimli çözümler oluşturma potansiyeline sahiptir (Corte-Real Santos ve ark., 2024). Bu özelliklere ek Schoof algoritması ile büyük asal mertebeden eliptik eğrileri bulmaya yönelik çözüm günümüz açık anahtarlı kriptografinin temeli olarak ECC'nin değerlendirilmesine sebep olmuştur. Özellikle eliptik eğrilerde tanımlı ayrık logaritma problemi tabanlı birçok açık anahtarlı kriptosistem verimlilik özellikleri ile ön plana çıkmıştır (Chen ve ark., 2016). Her ne kadar Shor algoritmasının eliptik eğriler üzerinde tanımlı ayrık logaritma problemini çözebileceği bilinse de süpersingüler eğrilerdeki izojeni problemini çözebilecek kuantum bir algoritmanın bilinmemesi bu kriptosistem ailesini kuantum sonrası için alternatif bir aday haline getirmiştir (Chen ve ark., 2024). Özet fonksiyon, elektronik imza, şifreleme odağında birçok eliptik eğri tabanlı kriptosistem önerilse de verimlilik ve uygulanabilirlik açısından anahtar değişim protokollerinin tasarımı bu kriptosistem ailesinde ön plana çıkmıştır. NIST standartlaşma sürecinde dördüncü turda değerlendirilmeye hak kazanan anahtar-kapsülleme algoritması izojeni-tabanlı SIKE algoritmasının güvensiz olduğu gösterilmiştir. NIST'in imzalama şemaları için başlattığı ek çağrıda (NIST, 2022) izojeni-tabanlı SQIsign algoritması ikinci tura geçmeye hak kazanan algoritmalar arasında yer almıştır.

### 2.1.6. Simetrik Sistemler Tabanlı İmzalama Şemaları

Kuantum sonrası güvenli imza şeması tasarımında güvenliğini sayı teorisinde yer alan zor problemlere dayanmak yerine simetrik ilkelere ait bileşenlere dayandıran kriptosistem sınıfıdır (Campagna ve ark., 2015). Simetrik bileşen olarak blok şifreler ve özet fonksiyonların kullanımı ile kuantum sonrası güvenli imza algoritması tasarımında küçük anahtarlar, orta düzeyde imza boyutu ve orta düzeyde imzalama ve doğrulama süresi elde edilebilmesine olanak sağlamıştır (Chase ve ark., 2017). Diğer kriptosistem ailelerinden ayrılmasına olanak sağlayan en önemli özelliği sayı teorisi veya yapılandırılmış zorluk varsayımları gerektirmeyen kuantum sonrası güvenlik sunmasıdır. NIST'in standardizasyon projesindeki ikinci tur aday imza algoritmalarından biri olan Picnic imza şeması bu yaklaşım temel alınarak önerilen algoritmaların başında yer almıştır. Ayrıca imzalama şemaları için başlatılan ek çağrıda ikinci tura geçmeye hak kazanan adaylardan FAEST bu kriptosistem ailesinde yer almaktadır.

### 2.2. PQC İçin NIST Gereksinimleri ve Bazı Açık Problemler

Bu bölümde kuantum sonrası kriptografide standartlaşma süreci ve literatürde yer alan bazı açık problemler tanıtılarak Türkiye'de yapılan çalışmaların bu anlamda oluşturduğu etkinin değerlendirilmesine yönelik yol haritasının çıkarılması planlanmıştır.

İlk çağrısı 2016 yılında yapılarak 30 Kasım 2017'ye kadar tekliflerin alınacağı ilan edilen NIST kuantum sonrası kriptografi standardizasyon süreci için başvuru koşulları ve değerlendirme kriterleri ilanında her bir aday teklifte yer alması gereken detaylar ve özellikler şu şekildedir (NIST, 2017; NIST, 2024).

- *Tam bir yazılı tasarım belgesi:* Algoritmaların uygulanması için gerekli tüm matematiksel işlemler, denklemler, tablolar ve diyagramlardan oluşan, algoritmaların eksiksiz bir yazılı tasarım belgesinin bulunması gerekmektedir.
- *Ayrıntılı bir performans analizi:* Windows veya Linux'ta çalışan ve derleyici destekleyen bir Intel x64 Referans Platformunda algoritmanın tahmini hesaplama verimliliği ve bellek gereksinimlerine ilişkin detaylı bilgi sunulması beklenmektedir.
- *Bilinen Cevap Testi (Known Answer Test) değerleri:* Gönderilen algoritmaların uygulanmasının doğruluğunu belirlemek için kullanılabilecek Bilinen Cevap Testi değerleri başka bir deyişle tek çıkış değerleri üreten bireysel giriş grupları sağlanmalıdır.
- *Beklenen güvenlik gücünün ayrıntılı bir açıklaması:* Destekleyici bir gerekçeyle birlikte kriptosistemin beklenen güvenlik gücüne ilişkin bir beyanı içermeli. NIST, genel kullanım için uyarlanabilir seçilmiş şifreli metin saldırısına ilişkin olarak "anlamsal olarak güvenli" şifreleme veya anahtar kapsüllemeyi etkinleştiren bir veya daha fazla şemayı standartlaştırmayı amaçlamışken elektronik imzalar için, uyarlanabilir seçilmiş bir mesaj saldırısına ilişkin olarak varoluşsal olarak taklit edilemez dijital imzaları etkinleştiren bir veya daha fazla şemanın standardizasyonunu hedeflemiştir.
- *Algoritmanın bilinen saldırılara göre analizi:* Önerilen şemaya yapılan bilinen kriptanalitik saldırıları özetleyen ve bu saldırıların karmaşıklığına ilişkin tahminler sağlayan teknik açıklamaların sunulması gerekmektedir.
- *Avantajlar ve sınırlamaların beyanı:* Teklif algoritmanın klasik ve kuantum saldırılarına karşı güvenliğinin değerlendirilmesinin yanı sıra ekstra işlevsellikler, performans değişimleri ve olağandışı güvenlik açıkları gibi olağandışı özelliklerinin olumlu ve olumsuz olarak değerlendirilmesinin sunulması beklenmektedir.

NIST'in standartlaşma süreci için belirlediği bu gereksinimler hem araştırmacılar hem de endüstri açısından kuantum sonrası güvenli açık anahtarlı kriptosistem tasarımı için bir rehber olmuştur. Bu durum ise kuantum sonrası kriptografi kavramını anlama, gereksinimleri belirleme,

potansiyel adaylar üzerinden çözüm önerileri oluşturma, var olan sistemleri kullanılabilir hale getirme ve iyileştirme, farklı uygulama alanları için yazılım ve donanım uygulaması gerçekleştirme odağında birçok çalışma ve girişimin gerçekleştirildiği ve gerçekleştirilmekte olduğu bilinmektedir. Bu açıdan literatüre bakıldığında spesifik birçok açık problemin tanımlandığı ve üzerinde çalışmalar yapıldığı bilinmektedir. Literatürde tanımlanan açık problemlerden bazıları şu şekilde listelenebilir:

- Kuantum bilgisayarlar sonrası güvenli açık anahtarlı şifreleme, anahtar değişimi, elektronik imza, kimlik doğrulama şemaları için protokol tasarımı (Li ve ark., 2023),
- İyi çalışılmış ve/veya standartlaştırılmış algoritmaların endüstrinin de ihtiyaç duyduğu mevcut yazılımlarla, donanımlarla ve arayüzlerle uyumlu, verimli ve uygulanabilir hale getirilmesi (Niederhagen ve Waidner, 2017; Fernández-Caramés, 2019),
- Kuantum sonrası teorik olarak güvenli olduğu gösterilen algoritmaların ve/veya kriptosistemlerin yazılım ve donanım uygulamalarının testi, uygulama odaklı saldırılar karşısında analizi (Niederhagen ve Waidner, 2017),
- Kuantum sonrası güvenli algoritmaların doğru bir şekilde uygulanmasında tasarım ve uygulamada ortaya çıkabilecek hataların önüne geçilebilmesi için her seferinde sıfırdan uygulamak yerine kriptografik kütüphaneler oluşturmak (Hekkala ve ark., 2023),
- Yüksek bilgi işlem, depolama, bellek ve iletişim gereksinimlerine sahip PQC algoritmalarının geleneksel kriptosistemler ile göreceli olarak kıyaslanabilir performans sunabilecek optimizasyonlar verilmesi (Seyhan ve ark., 2022; Bavdekar ve ark., 2022),
- Kuantum bilgisayarlar için zor olan yeni, küçük masraf ve hesaplama gereksinimine ihtiyaç duyan matematik problemlerin, kriptografik ilkelerin bulunması, uyarlanması ve tasarlanması ile yeni kuantum sonrası güvenli kriptosistem tasarımı (Bavdekar ve ark., 2022),
- Daha küçük anahtar boyutu gereksinimi duyan kaynak kısıtlı cihazların güvenliği özelinde enerji verimli (özetle hafif siklet) kriptosistem, İnternet protokolleri tasarlanması ve uygulanması (Fernández-Caramés, 2019; Kumar ve ark., 2022).

Özetlenen NIST gereksinimleri ve açık problemler baz alınarak farklı uygulama alanları, kullanım senaryoları, kısıtlamalar, özelleşmeler, standartlaşmalar özelinde birçok akademik çalışmanın yapılmasının yanı sıra endüstri girişimleri, farklı standartlaşma süreçlerinin olduğu bilinmektedir. Bu çalışma ile sunulan analizde Türkiye'de kuantum sonrası kriptografi alanında uzmanlık kazanmak amacıyla lisansüstü eğitim döneminde yapılan çalışmalara, hedeflenilen açık problemlere, yaklaşımlara ve yöntemlere ışık tutulması amaçlanmıştır. Ayrıca Türkiye adresli araştırmacıların kuantum sonrası kriptografi ile ilgili yaptığı yayınlara ilişkin sayısal bilgiler sunularak bu alanda Türkiye'deki mevcut durum ve gelişme sürecinin analiz edilmesi hedeflenmiştir. Hem lisansüstü eğitimde çalışılan konular hem de Türkiye adresli akademik çalışmaların günceline erişebilmek için araştırma yöntemleri oluşturulmuştur.

## 3. Araştırma Yöntemi

Bu çalışma ile gerçekleştirilen bibliyometrik analizde kuantum sonrası kriptografi alanında Türkiye'de yapılan tezlerin analiz edilmesi ve yapılan akademik çalışmaların ile bu alanda gelişen, nitelik kazanan ve uzmanlaşılan konular, süreçler ve yaklaşımlar hakkında bilgi sunulması amaçlanmıştır. Analiz YÖK tez merkezinde bulunan tezler ve Türkiye adresli bu alanda yapılan akademik çalışmaların incelenmesi odağında gerçekleştirilmiştir.

### 3.1. YÖK Tez Merkezi Verilerine Erişim İçin Araştırma Yöntemi

Türkiye'de kuantum bilgisayarlar sonrası kriptografi alanında yapılan lisansüstü tez çalışmalarını elde edebilmek için Ulusal Tez Merkezi (Yükseköğretim Kurulu Başkanlığı, 2025.) üzerinden yapılacak sistematik arama için Tanım 2'de detayları sunulan kuantum sonrası kriptografi ile ilgili iki farklı anahtar kelime havuzu oluşturulmuştur. Genel kavram havuzunda kuantum sonrası kriptografi alanı ile ilişkili olası genel kavramları içeren 9 İngilizce ve 13 Türkçe anahtar kelime içerecek şekilde oluşturulmuştur. Özelleşmiş kavram havuzunda ise kuantum sonrası güvenli kriptosistem aileleri ile ilgili 8 İngilizce ve 12 Türkçe anahtar kelimeyi içerecek şekilde oluşturulmuştur. Oluşturulan anahtar kelime havuzlarına Tablo 3'te anahtar kelime sütununda yer verilmiştir. Tüm bu anahtar kelimeler ile kuantum sonrası ile ilgili genel kavramları içeren tezlere ek kuantum bilgisayarlar varlığında güvenli olduğu bilinen zor problemlere sahip olan kriptosistem ailelerini temel alan tez çalışmaları da analize dahil edilerek hassasiyeti artırılmıştır. İlgili anahtar kelimelerin aynı tezde yer alması, matematik, fizik gibi alanlarla ilgili tezlerin kapsam dışında bırakılması, kuantum sonrası kriptografi ve kuantum kriptografi kavramlarının farklılığından oluşan kapsamın ele alınması gibi gereklilikler ile analiz için seçilecek tez çalışmalarının belirlenmesi amacıyla seçim kriterleri (SK) ve eleme kriterleri (EK) oluşturulmuştur.

- SK1: Anahtar kelimelerden en az biri, tez için YÖK tez merkezinde tezin tanımlanmasında kullanılan konu, dizin ve özet kısımlarından birinde geçmelidir.
- SK2: Tezlerde hem Türkçe hem de İngilizce özetler sunulduğu için anahtar kelime havuzlarında tekrar eden tez bulunmamalıdır.
- SK3: Aynı tez iki farklı kavram havuzunda tekrar etmemelidir.
- EK1: Tezin konusu kuantum sonrası kriptografi alanını içeren açık erişimli tezler ele alınmalıdır.
- EK2: Fizik, Matematik gibi alanlarda yapılmış kuantum hesaplama ile ilgili çalışmalar kuantum sonrası kriptografi ile doğrudan ilgili olmadığı için analize dahil edilmemelidir.

Belirlenen anahtar kelimeler kullanılarak YÖK tez merkezi aracılığıyla yapılan gelişmiş taramada (analize dahil edilecek tezler Mart 2025'e kadar yayınlanmış olan tezlerden seçilmiştir) bu SK ve EK'ların uygulanması sonucu elde edilen tezlere ait sayısal veriler Tablo 3'te sunulmuştur.

**Tablo 3.** YÖK tez merkezinden elde edilen sayısal sonuçlar.

| | | *Anahtar Kelime* | *SK1* | *T* | *SK2* | *SK3* | *EK1 +EK2* |
|---|---|---|---|---|---|---|---|
| **Genel Kavram Havuzu** | *İngilizce* | *post-quantum* | 42 | 198 | 76 | **135** | **50** |
| | | *post quantum* | 42 | | | | |
| | | *post-quantum cryptography* | 20 | | | | |
| | | *post quantum cryptography* | 20 | | | | |
| | | *quantum secure* | 9 | | | | |
| | | *quantum-secure* | 9 | | | | |
| | | *quantum resistant* | 8 | | | | |
| | | *quantum-resistant* | 8 | | | | |
| | | *quantum cryptography* | 40 | | | | |
| | *Türkçe* | *kuantum sonrası kriptografi* | 15 | 68 | | | |
| | | *kuantum-sonrası kriptografi* | 15 | | | | |
| | | *kuantum-ertesi* | 1 | | | | |
| | | *kuantum ertesi* | 1 | | | | |
| | | *kuantum güvenli* | 6 | | | | |
| | | *kuantum kriptografisi* | 2 | | | | |
| | | *kuantum kriptografi* | 18 | | | | |
| | | *post-kuantum* | 7 | | | | |
| | | *kuantum bilgisayarlar ertesi kriptografi* | 0 | | | | |
| | | *kuantum bilgisayarlar sonrası kriptografi* | 0 | | | | |
| | | *kuantum bilgisayarlar sonrası güvenilir* | 1 | | | | |
| | | *kuantum ertesi kriptografi* | 1 | | | | |
| | | *kuantum-ertesi kriptografi* | 1 | | | | |
| **Özel Kavram Havuzu** | *Türkçe* | *kafes tabanlı kriptografi* | 13 | 87 | 98 | | |
| | | *kafes tabanlı* | 39 | | | | |
| | | *latis tabanlı* | 2 | | | | |
| | | *latisler üzerinde kriptoloji* | 1 | | | | |
| | | *kod tabanlı kriptografi* | 1 | | | | |
| | | *kod tabanlı* | 22 | | | | |
| | | *özet tabanlı* | 2 | | | | |
| | | *özet tabanlı kriptografi* | 0 | | | | |
| | | *çok değişkenli polinom sistemleri* | 4 | | | | |
| | | *çok değişkenli polinom sistemleri tabanlı kriptografi* | 0 | | | | |
| | | *izojeni tabanlı kriptografi* | 1 | | | | |
| | | *izojeni tabanlı* | 2 | | | | |
| | *İngilizce* | *lattice-based cryptography* | 12 | 78 | | | |
| | | *lattice-based* | 47 | | | | |
| | | *hash-based cryptography* | 0 | | | | |
| | | *hash-based* | 17 | | | | |
| | | *multivariate based cryptography* | 0 | | | | |
| | | *multivariate based* | 2 | | | | |
| | | *isogeny-based cryptography* | 0 | | | | |
| | | *isogeny-based* | 0 | | | | |
| **T: Toplam** | | | | | | | |

Tablo 3'te sunulan sayısal verilerin nasıl elde edildiğine yönelik açıklamalar şu şekildedir:

- Öncelikli olarak YÖK tez merkezi gelişmiş tarama seçeneğinde Tablo 3 anahtar kelimeler sütununda yer alan anahtar kelimeler tek tek sorgulanmış ve bu anahtar kelimeleri içeren tezlerin sayısı SK1 sütununda verilmiştir. Örneğin; "post-quantum" anahtar kelimesini YÖK tez merkezinde yayınlanan tezlerin konu, dizin, anahtar kelimeler kısmında içeren toplam 42 tez bulunmuştur.
- Daha sonra hem genel hem de özel anahtar kelime havuzları kendi içerisinde tez no değerleri (YÖK tez tarafından her bir teze özgü verilen kimlik değeri) aynı olan tezler arasından tekrar etmeyen tezler bulunmuştur. SK2 sütununda verildiği üzere genel kavram havuzunda bulunan 22 anahtar kelimeden herhangi birini içeren ve tekrar etmeyen toplam 76 tez bulunmuştur. Özel kavram havuzunda sunulan anahtar kelimelerden herhangi birini içeren ve tekrar etmeyen toplam tez sayısı ise 98 olarak belirlenmiştir.
- Bir sonraki adım olarak tezlerin hem genel kavram hem de özel kavram havuzunda yer alan anahtar kelimeleri aynı anda içerebileceği bilindiğinden 76+98=174 tez arasından tez no'ları incelenerek tekrar etmeyen tez sayısı 135 olarak (SK3 sütununda sunulduğu üzere) belirlenmiştir.
- Son olarak incelemeye konu olacak 135 tezin İngilizce ve Türkçe tez adları ve özetleri, tezin gerçekleştirildiği üniversite, enstitü ve anabilim dalı bilgileri, türü (yüksek lisans veya doktora), dili ve yıl bilgileri elde edilmiştir. Ancak her ne kadar bu kavramları içerse bile Tanım 2'de açıklanan kuantum sonrası kriptografi kavramı ile ilişkili olmayacak tezlerin de bulunabileceği bilinmektedir. Bu anlamda analizde ele alınacak tezlerin belirlenmesi için tez özetleri ve tezler ile ilişkili bilgiler üzerinde EK1 ve EK2 uygulanarak kuantum sonrası kriptografi ile ilgili Türkiye'de yazılan tez sayısı 47+3 (erişim kısıtı)=50 olarak belirlenmiştir.

Sistematik inceleme ile bibliyometrik analize konu olan tezlere ilişkin tez no değerleri Ekler bölümüne sunulan Tablo 7 ile verilmiştir. Belirlenen tezlerin bibliyometrik analizine ilişkin incelemeler ise Tezlerin Bibliyometrik Analiz'i alt başlığında sunulmuştur.

*Not.* Bu analizde odak noktası kuantum sonrası kriptografi olduğu için Tanım 1 ile verilen kuantum kriptografi alanında yapılan anahtar dağıtım protokolü odağındaki çalışmalar ve kriptografik ilke olarak kuantum sonrası güvenli kriptosistem ailelerinde yer alan ilkeleri kullanma odağı ile gerçekleştirilen ana amacı homomorfik şifreleme açısından katkı sunan tezler değerlendirmeye dahil edilmemiştir. Ayrıca ilgili araştırma yöntemi ile elde edilen ancak açık erişime kapalı olan 3 tez bu analize dahil edilememiştir.

### 3.2. Scopus Verilerine Erişim İçin Araştırma Yöntemi

Türkiye'de kuantum sonrası kriptografi alanında yapılan akademik çalışmalara bir bakış sunabilmek için iyi bilinen veritabanlarından yazarların bulunduğu ülke açısından filtreleme özelliği sunan Scopus veritabanı (Scopus, 2025) seçilmiştir. Gelişmiş arama seçeneği ile Türkiye adresli yazarların kuantum sonrası kriptografi ile ilgili yaptığı akademik çalışmalara erişmek için Tablo 3'te sunulan genel ve özel kavramlar havuzunun Scopus özelinde güncellenmiş hali Tablo 4'te verilmiştir. Tablo 4 oluşturulurken Scopus ile sadece Türkiye adresli yazarlar tarafından İngilizce yazılmış akademik çalışmalar elde edilebileceği için Tablo 3'teki Türkçe anahtar kelimeler çıkarılmış ve mantıksal veya (OR) seçeneği ile kontrol edilebilecek anahtar kelimeler tek sorgu nosu ile eşleştirilmiştir. Scopus'tan ilgili akademik çalışmaların elde edilmesi için oluşturulan SK ve EK'lar ise şu şekildedir.

- SK4: Tablo 4'teki anahtar kelimelerden en az biri, Scopus'ta yayınlanan çalışmaların başlık, özet ve anahtar kelimelerinden en az birinde geçmelidir.
- SK5: Akademik çalışmanın konusu kuantum sonrası kriptografi alanını içermelidir.
- EK3: Oluşturulan anahtar kelime kavram havuzlarında tekrar eden akademik çalışmalar bulunmamalıdır.

**Tablo 4.** Scopus için güncellenen anahtar kelime havuzları.

| | Sorgu No | Anahtar Kelimeler |
|---|---|---|
| **Genel Kavram Havuzu** | **S1** | post quantum, post-quantum |
| | **S2** | post quantum cryptography, post-quantum cryptography |
| | **S3** | quantum secure, quantum-secure |
| | **S4** | quantum resistant, quantum-resistant |
| | **S5** | quantum cryptography, quantum-cryptography |
| **Özel Kavram Havuzu** | **S6** | lattice based cryptography, lattice-based cryptography |
| | **S7** | lattice cryptography |
| | **S8** | hash based cryptography, hash-based cryptography |
| | **S9** | hash cryptography |
| | **S10** | multivariate based cryptography, multivariate-based cryptography |
| | **S11** | multivariate cryptography |
| | **S12** | isogeny based cryptography, isogeny-based cryptography |
| | **S13** | isogeny cryptography |
| | **S14** | code based cryptography, code-based cryptography |
| | **S15** | code cryptography |

Scopus'ta gelişmiş taramada kullanılan sorgular ve SK4, SK5 ve EK3'ün uygulanması ile elde edilen sayısal sonuçlar Tablo 5 ve Tablo 6'da verilmiştir.

Genel kavram havuzu için Tablo 4'te verilen anahtar kelimeler gelişmiş arama ile SK4 uygulanarak (Tablo 5'te sunulan) 189+95+81+81+171=617 ve özel kavram havuzu için (Tablo 6'da

sunulan) 83+88+4+66+6+7+1+2+64=321 kuantum sonrası kriptografi ile ilgili akademik çalışmanın Türkiye adresli araştırmacılar tarafından yayınlandığı tespit edilmiştir. Bu çalışmalardan doğrudan kuantum sonrası kriptografi ile ilgili olmayanların filtrelenmesi için SK5 uygulanarak genel kavram havuzu ile alakalı 385 özel kavram havuzu ile alakalı 181 çalışmanın yayınlandığı belirlenmiştir. Her iki havuz özelinde ayrı ayrı aynı çalışmanın sayılara dahil edilmemesi için EK3 uygulandığında Scopus'ta taranan yayın sayısı genel kavram havuzundaki anahtar kelimeleri içerenler için 155 iken özel kavram havuzu için ise 76+5+6+2+7= 96 olarak belirlenmiştir. Türkiye adresli yazarlar tarafından oluşturulan kuantum sonrası kriptografi ile ilgili Scopus'ta taranan akademik çalışmalara yönelik bibliyometrik analiz ise Scopus Verileri Özelinde Bibliyometrik Analiz bölümünde detaylandırılmıştır.

**Tablo 5.** Genel kavram havuzunda yer alan anahtar kelimeler ile Scopus veritabanından ile elde edilen sayısal sonuçlar.

| | Sorgu ID | Scopus Sorgu | SK4 | SK5 | EK3 |
|---|---|---|---|---|---|
| Genel Kavram Havuzu | S1 | ( TITLE-ABS-KEY ( post AND quantum ) OR TITLE-ABS-KEY ( post-quantum ) ) AND ( LIMIT-TO ( AFFILCOUNTRY , "Turkey" ) ) | 189 | 96 | **155** |
| | S2 | ( TITLE-ABS-KEY ( post AND quantum AND cryptography ) OR TITLE-ABS-KEY ( post-quantum AND cryptography ) ) AND ( LIMIT-TO ( AFFILCOUNTRY , "Turkey" ) ) | 95 | 90 | |
| | S3 | (TITLE-ABS-KEY ( quantum AND secure ) OR TITLE-ABS-KEY ( quantum-secure ) ) AND ( LIMIT-TO ( AFFILCOUNTRY , "Turkey" ) ) | 81 | 58 | |
| | S4 | ( TITLE-ABS-KEY ( quantum AND resistant ) OR TITLE-ABS-KEY ( quantum-resistant ) ) AND ( LIMIT-TO ( AFFILCOUNTRY , "Turkey" ) ) | 81 | 25 | |
| | S5 | ( TITLE-ABS-KEY ( quantum AND cryptography ) OR TITLE-ABS-KEY ( quantum-cryptography ) ) AND ( LIMIT-TO ( AFFILCOUNTRY , "Turkey" ) ) | 171 | 116 | |

**Tablo 6.** Özel kavram havuzunda yer alan anahtar kelimeler ile Scopus veritabanından ile elde edilen sayısal sonuçlar.

| | | | | | |
|---|---|---|---|---|---|
| Özel Kavram Havuzu | S6 | ( TITLE-ABS-KEY ( lattice AND based AND cryptography ) OR TITLE-ABS-KEY ( lattice-based AND cryptography ) ) AND ( LIMIT-TO ( AFFILCOUNTRY , "Turkey" ) ) | 83 | 72 | **76** |
| | S7 | TITLE-ABS-KEY ( lattice AND cryptography ) AND ( LIMIT-TO ( AFFILCOUNTRY , "Turkey" ) ) | 88 | 75 | |
| | S8 | (TITLE-ABS-KEY ( hash-based AND cryptography ) AND TITLE-ABS-KEY ( hash AND based AND cryptography )) AND ( LIMIT-TO ( AFFILCOUNTRY , "Turkey" ) | 4 | 4 | **5** |
| | S9 | TITLE-ABS-KEY ( hash AND cryptography ) AND ( LIMIT-TO ( AFFILCOUNTRY , "Turkey" ) ) | 66 | 4 | |
| | S10 | (TITLE-ABS-KEY ( multivariate AND based AND cryptography ) OR TITLE-ABS-KEY ( multivariate-based AND cryptography )) AND ( LIMIT-TO ( AFFILCOUNTRY , "Turkey" ) ) | 6 | 6 | **6** |
| | S11 | TITLE-ABS-KEY ( multivariate AND cryptography ) AND ( LIMIT-TO ( AFFILCOUNTRY , "Turkey" ) ) | 7 | 6 | |
| | S12 | ( TITLE-ABS-KEY ( isogeny AND based AND cryptography ) OR TITLE-ABS-KEY ( isogeny-based AND cryptography ) ) AND ( LIMIT-TO ( AFFILCOUNTRY , "Turkey" ) ) | 1 | 1 | **2** |
| | S13 | TITLE-ABS-KEY ( isogeny AND cryptography ) AND ( LIMIT-TO ( AFFILCOUNTRY , "Turkey" ) ) | 2 | 2 | |
| | S14 | (TITLE-ABS-KEY ( code AND based AND cryptography ) OR TITLE-ABS-KEY ( code-based AND cryptography )) AND ( LIMIT-TO ( AFFILCOUNTRY , "Turkey" ) ) | 64 | 4 | **7** |

## 4. Bibliyometrik Analiz

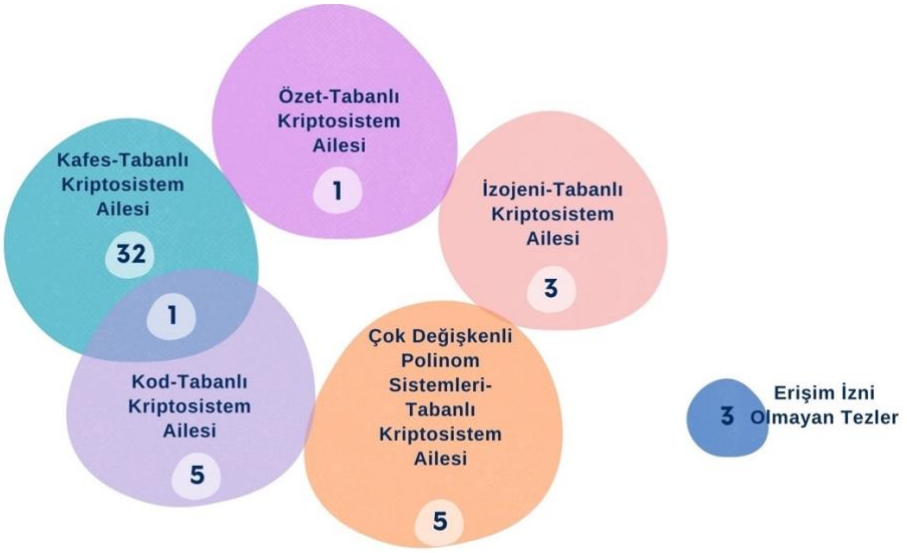
Bu bölümde açıklanan araştırma yöntemleri baz alınarak belirlenen kuantum sonrası kriptografi alanında Türkiye'deki araştırmacılar tarafından gerçekleştirilen lisansüstü çalışmalar ve akademik

çalışmalara yönelik elde edilen sonuçlar üzerinden gerçekleştirilen bibliyometrik analiz sonuçları sunulmaktadır.

### 4.1. Tezlerin Bibliyometrik Analiz

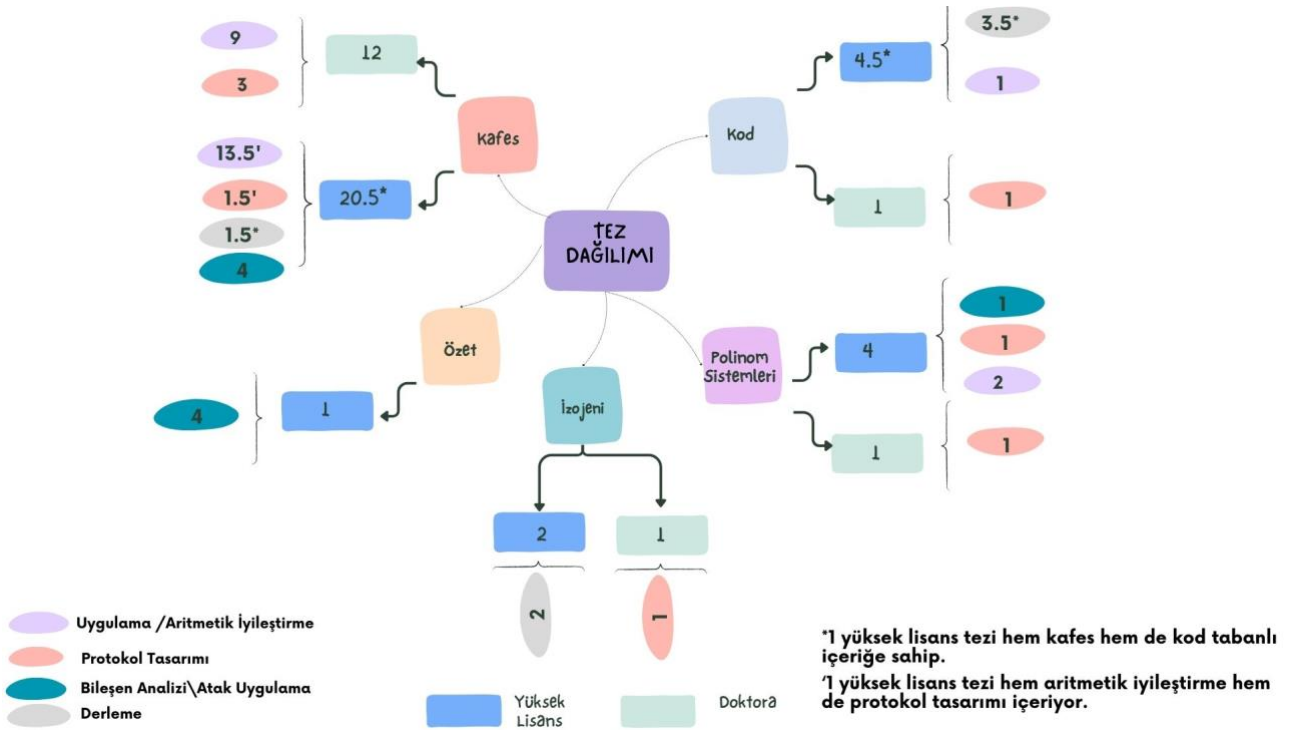
Kuantum Bilgisayarlar Sonrası Güvenli Kriptosistem Aileleri alt başlığında özetlendiği üzere kuantum sonrası kriptografi alanında protokol tasarım gereksinimleri, bileşenleri, uygulama senaryosu, kullanım durumları vb. açısından birçok açık problem üzerinde çalışmalar yapılmıştır. Bibliyometrik analiz açıklanan araştırma yöntemi ile belirlenen açık erişimli 47 tez üzerinden yapılmıştır. Bu tezlerin temel özellikleri ve detayları özetlenen kuantum bilgisayarlar sonrası güvenli kriptosistem ailelerine dağılımı Şekil 1'de sunulmuştur. Şekil 1'de sunulan sayısal dağılıma göre Türkiye'de lisansüstü eğitim aşamasında kuantum sonrası kriptografi alanında en fazla çalışılan kuantum sonrası güvenli kriptosistem ailesi kafes-tabanlı sistemler olmuştur. Bunu takiben sayısal olarak en fazla kod ve çok değişkenli polinom sistemlerine dayalı lisansüstü tezler takip etmiştir.

Yapılan lisansüstü tezlerin niteliği ve kuantum sonrası kriptografi açısından sunduğu katkının belirlenebilmesi bibliyometrik analizde kullanılmak üzere 4 farklı katkı metriği belirlenmiştir. Protokol tasarımı, bileşen analizi/atak uygulama, yazılım veya donanım uygulaması geliştirme/aritmetik iyileştirme içerme ve derleme çalışması olup olmaması açısından belirlenen tezler üzerinde analiz gerçekleştirilmiştir. Seçilen 47 tezin kuantum sonrası güvenli kriptosistem aileleri özelinde bu alanda belirlenen katkı metriklerine dağılımı ise Şekil 2'de sunulmuştur. Ayrıca bu dağılımda hangi tezlerin yer aldığına ait detaylandırma Ek'te sunulan Tablo 7 ile verilmiştir.



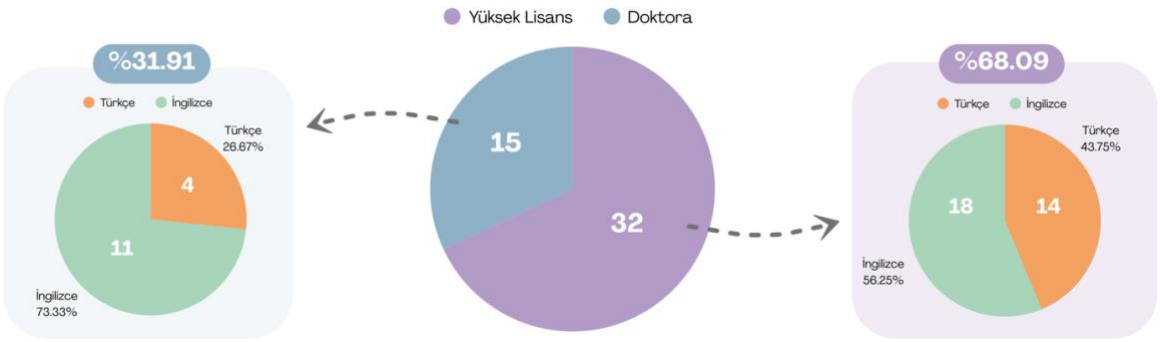

**Şekil 1.** Tezlerin kuantum sonrası güvenli kriptosistem aileleri özelinde dağılımı.

Şekil 2'de sunulan analiz Türkiye'de kuantum sonrası kriptografi alanında en fazla kafes-tabanlı kriptosistemlerin Uygulama ve Aritmetik iyileştirme odağında çalışıldığını göstermektedir. Dağılım oluşturulurken bir kafes-tabanlı yüksek lisans tezi (Şekil 2'de ‘ ile vurgulanan) hem protokol tasarımı hem de aritmetik iyileştirme açısından katkı sunduğu için 0.5-0.5 olarak ilgili dağılıma dahil edilmiştir. Ayrıca bir yüksek lisans tezi (Şekil 2'de * ile vurgulanan) hem kafes tabanlı hem de kod tabanlı yaklaşımı içeren bir derleme çalışması olduğu için ilgili dağılıma 0.5-0.5 olarak eklenmiştir. Genel sonuçlara bakıldığında toplam tez sayısının yaklaşık %18'ini oluşturan protokol tasarımı (algoritma akışı, doğruluk analizi, güvenlik analizi vb.) açısından yapılan katkının kuantum sonrası güvenli açık anahtarlı kriptosistem tasarımı açısından en önemli bileşenlerden biri olduğu bilinmektedir. Bileşen analizi, atak uygulama, yazılım/donanım uygulaması geliştirme, aritmetik iyileştirme ve derleme odağında yapılan tezlerin kuantum sonrası kriptografi alanında kriptosistem tasarımında bileşen bazlı katkı sunduğu ve farklı uygulama alanlarında da kullanım senaryoları olduğu bilinmektedir.




**Şekil 2.** Tezlerin katkı metrikleri ve kuantum sonrası güvenli kriptosistem aileleri özelinde sayısal dağılımı.

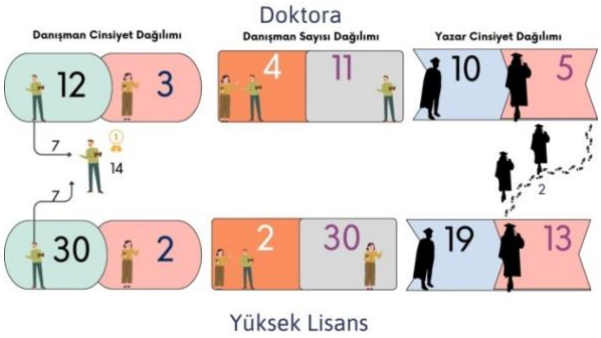
Belirlenen tezlerin yazıldığı diller ve lisansüstü eğitimin hangi aşamasında yapıldığına dair analizler ise Şekil 3'te sunulmuştur.




**Şekil 3.** Tezlerin lisansüstü eğitim aşaması ve yazıldığı dil açısından dağılımı.

Açık erişimli 47 tezden 32 tanesi yüksek lisans (18 İngilizce, 14 Türkçe) çalışması iken 15 tanesi (11 İngilizce, 4 Türkçe) doktora çalışması olarak gerçekleştirildiği gözlemlenmiştir. Bu alanda yapılan iki doktora tezi ana bilim dalı Türkçe eğitim vermesine rağmen İngilizce olarak hazırlandığı gözlemlenmiştir.

İlgili tezlerin danışman sayısı, cinsiyeti ve nitelikli araştırmacılara ait cinsiyet incelenmesi sonuçları ise Şekil 4'te sunulmuştur.

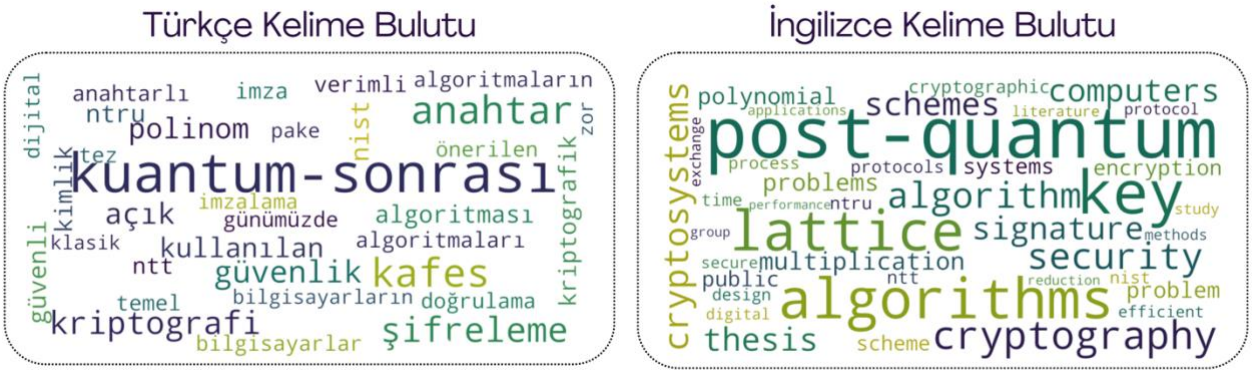



**Şekil 4.** Tezlerin danışman sayısı, cinsiyeti ve araştırmacıların cinsiyet açısından incelenmesi sonuçları.

Şekil 4'te de sunulduğu üzere yüksek lisans seviyesinde gerçekleştirilen tezlerden 30 doktora seviyesinde 12 tez erkek danışmanlar tarafından tamamlanmışken kadın danışman dağılımı sırasıyla 3 ve 2 olmuştur. Tüm aşamalarda tezlerde birinci ve ikinci danışman olarak yer alan Ondokuz Mayıs Üniversitesi adresli bir danışman bu alanda 14 tez ile en fazla tez bitirten danışman olarak ön plana çıkmıştır. Doktora aşamasındaki 4 tez yüksek lisans aşamasında ise 2 tez iki danışmanlı olarak tamamlanmışken kalan tezler tek danışmanlı olmuştur. Tezleri gerçekleştiren araştırmacıların cinsiyet dağılımı gösteriyor ki doktora aşamasında kadın-erkek dağılımı 5'e 10 iken yüksek lisansta bu oran 13'e 19 olmuştur. Seçilen 47 tezde hem yüksek lisansı hem de doktorası bu alanda olan iki kadın araştırmacı olduğu gözlemlenmiştir.

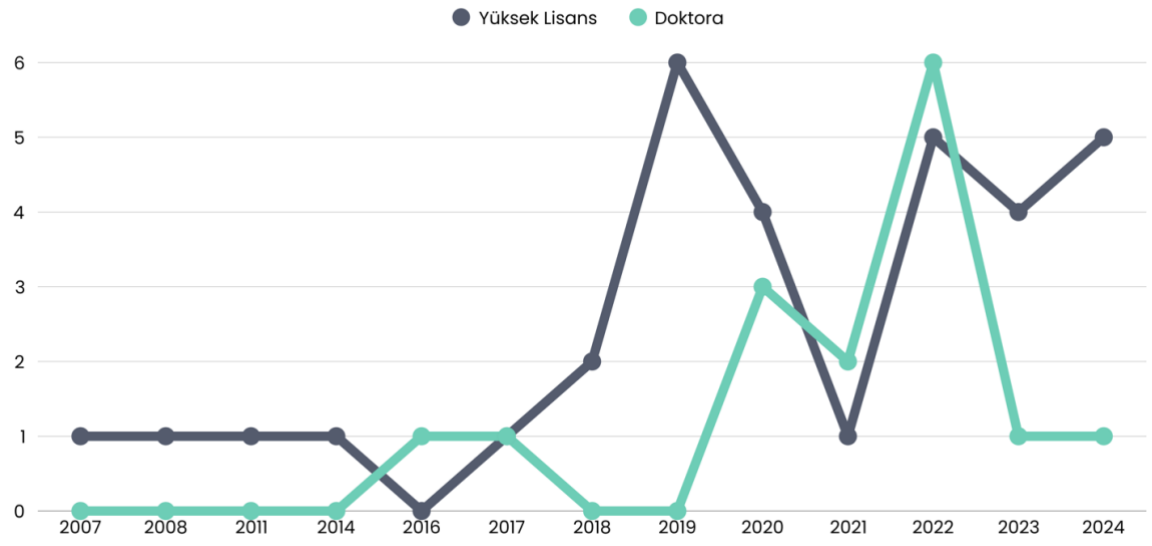
Seçilen tezlerin İngilizce ve Türkçe özetleri ele alınarak en az 20 kez kullanılan (frekansı 20 olan) kavramsal kelimeler ile oluşturulan anahtar kelime bulutları ise Şekil 5'te sunulmuştur. Türkçe

özetlerde en fazla kullanılan kelimeler sırasıyla kuantum-sonrası, kafes, anahtar ve şifreleme gibi kelimeler iken İngilizce özetlerde ise post-quantum, key, algorithms ve lattice gibi kelimeler sıklıkla kullanılmıştır.



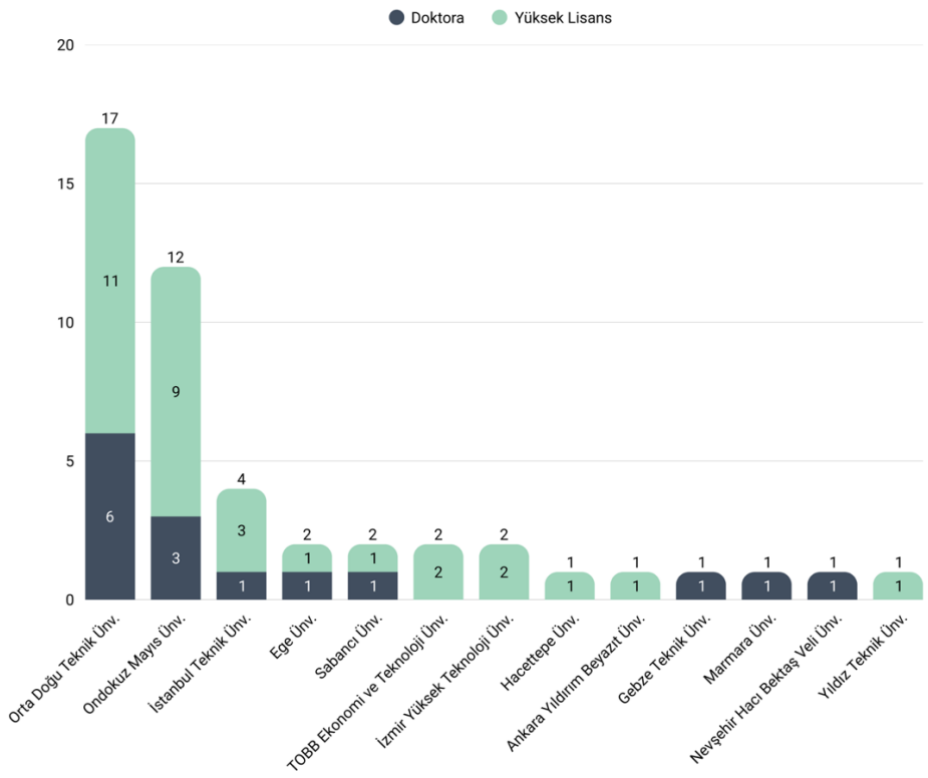

**Şekil 5.** Lisansüstü tezlerden dil bazlı kelime bulutları.

Kuantum sonrası kriptografi alanında yapılan lisansüstü tezlerin yıl bazında dağılımı ise Şekil 6'da verilmiştir. Bu alanda ilk yüksek lisans çalışması ise 2007 yılında tamamlanmışken ilk doktora çalışması 2016 yılında sonlandırılmıştır. Yüksek lisans açısından en fazla tez 2019 yılında tamamlanmışken Doktora aşamasında en fazla tez 2022 yılında tamamlanmıştır. Sonuçlara göre kuantum sonrası kriptografi alanında yapılan çalışmalar son altı yılda yoğunlaşmaktadır.



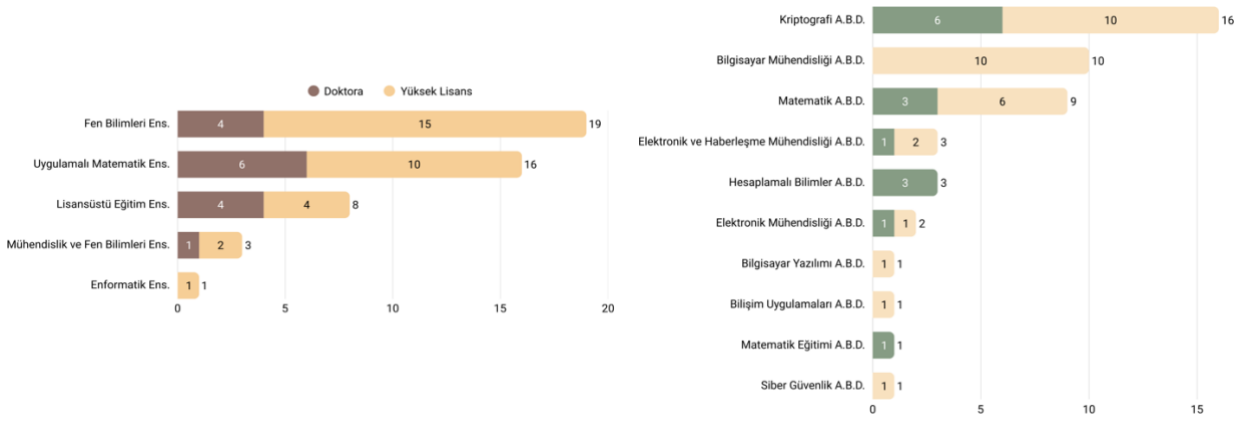

**Şekil 6.** Lisansüstü tezlerin tamamlandığı yıl bazında dağılımı.

Kuantum sonrası kriptografi alanında yapılan tezlerin gerçekleştirilen üniversiteler (Ünv) açısından dağılımı ise Şekil 7'de sunulmuştur. Bu dağılıma bakıldığında kuantum sonrası kriptografi alanında Orta Doğu Teknik Üniversitesi ve Ondokuz Mayıs Üniversite'lerinin ön plana çıktığı söylenebilmektedir.




**Şekil 7.** Lisansüstü tezlerin üniversite bazında dağılımı.

Bu tezlerin ilgili üniversitelerde gerçekleştirildiği enstitüler (Ens) ve anabilim dalları (A.B.D.) açısından dağılımı ise Şekil 8'de sunulmuştur.




**Şekil 8.** Lisansüstü tezlerin gerçekleştirildiği ana bilim dalları ve enstitü dağılımı.

Kuantum sonrası kriptografi alanında yapılan doktora tezlerinde Uygulamalı Matematik, Lisansüstü Eğitim ve Fen Bilimleri enstitüleri ön plana çıkarken yüksek lisansta Fen Bilimleri ve Uygulamalı Matematik Enstitüleri öncülük etmiştir. Anabilim Dalları açısından yapılan karşılaştırmada doktora da Kriptografi, Matematik ve Hesaplamalı Bilimler A.B.D.'leri ön plana çıkarken, yüksek lisansta Kriptografi, Bilgisayar Mühendisliği ve Matematik A.B.D.'lerinde bu alanın daha çok çalışıldığı tespit edilmiştir.

Bu analizde kuantum sonrası kriptografi alanında yapılan katkının değerlendirilmesi için belirlenen dört farklı katkı metriği açısından ilgili üniversitelere dağılımı ise Şekil 9'da verilmiştir.

Şekil 9 ile sunulan analizde ayrıca tezlerin danışmanlık durumları incelenerek iki danışmanlı tezler için ayrı bir analiz yapılmıştır. Protokol tasarımı açısından iki tez Orta Doğu Teknik-Ondokuz Mayıs ve Gebze Teknik-Diğer kurumlarında iki danışmanlı olarak yürütüldüğü için 0.5-0.5 olarak paylaştırılmıştır. Uygulama/Aritmetik İyileştirme açısından gerçekleştirilen üç tez, Ondokuz Mayıs-Ege ve Ondokuz Mayıs-Orta Doğu ve Ege-Diğer çalışmaları ile gerçekleştirildiğinden 0.5-0.5 olarak dağıtılmıştır. Derleme metriğinde bir tez ise Orta Doğu Teknik-Diğer eşleşmesinde yer alan danışmanlar ile gerçekleştirildiğinden 0.5-0.5 olarak paylaştırılmıştır. Genel olarak bakıldığında kuantum sonrası kriptografi açısından protokol tasarımı metriğinde en fazla lisansüstü tezin Ondokuz Mayıs Üniversitesinde, uygulama/aritmetik iyileştirme, bileşen analizi/atak uygulama ve derleme metriklerin de ise Orta Doğu Teknik Üniversitesi ön plana çıktığı belirlenmiştir.

| | Protokol Tasarımı | Uygulama Aritmetik İyileştirme | Bileşen Analiz/Atak Uygulama | Derleme | Toplam |
|---|---|---|---|---|---|
| Ankara Yıldırım Beyazıt Ünv. | 0 | 0 | 0 | 1 | 1 |
| Ege Ünv. | 0 | 1 + 0.5 | 0 | 1 | 2.5 |
| Gebze Teknik Ünv. | 0.5 | 0 | 0 | 0 | 0.5 |
| Hacettepe Ünv. | 0 | 0 | 0 | 1 | 1 |
| İstanbul Teknik Ünv. | 0 | 3 | 0 | 1 | 4 |
| İzmir Yüksek Teknoloji Ens. | 0 | 1 | 1 | 0 | 2 |
| Marmara Ünv. | 1 | 0 | 0 | 0 | 1 |
| Nevşehir Hacı Bektaş Veli Ünv. | 1 | 0 | 0 | 0 | 1 |
| Ondokuz Mayıs Ünv. | 6+0.5 | 6+0.5+0.5 | 0 | 0 | 13.5 |
| Orta Doğu Teknik Ünv. | 0+0.5 | 7+0.5+0.5 | 4 | 2+0.5 | 15 |
| Sabancı Ünv. | 0 | 2 | 0 | 0 | 2 |
| TOBB Ekonomi ve Teknoloji Ünv. | 0 | 1 | 0 | 1 | 2 |
| Yıldız Teknik Ünv. | 0 | 0 | 1 | 0 | 1 |
| Diğer | 0.5 | 0.5 | 0 | 0.5 | 1.5 |

**Şekil 9.** Katkı metrikleri açısından üniversite-bazlı dağılımı.

### 4.2. Scopus Verileri Özelinde Bibliyometrik Analiz

Scopus Verilerine Erişim İçin Araştırma Yöntemi alt başlığında özetlendiği üzere kuantum sonrası kriptografi alanında Türkiye adresli araştırmacıların yaptığı çalışmalara ve güncel literatüre bir bakış sunulabilmesi amacıyla Tablo 4'te verilen genel kavram havuzu için 5 sorgu (S1, S2, S3, S4, S5) ve özel kavram havuzu için 10 (S6, S7, S8, S9, S10, S11, S12, S13, S14, S15) sorgu kullanılarak Scopus'ta araştırma yapılmıştır. Araştırmada akademik çalışmaların niteliği Makale, Bildiri, Kitap, Kitap Bölümü ve Derleme çalışması olup olmama durumlarına göre sınıflandırma yapılmıştır. Özel kavram havuzu için belirlenen sorgular ikili grup oluşturduğu için (S6-S7, S8-S9, S10-S11, S12-S13, S14-S15) bu ikili gruplar özelinde tekrar etmeyen çalışmalar ile genel dağılım belirlenmiştir. Hem Scopus'ta tüm yıllarda hem de güncel literatüre bir bakış sunabilmek için son 6 yıl özelinde elde edilen sonuçlar Şekil 10'da sunulmuştur. Tanımlanan Scopus sorguları gelişmiş arama seçeneği üzerinden sorgulanarak her bir sorgu veya sorgu çifti için tüm yıllar taranan akademik çalışmalar export özelliği kullanılarak csv formatında tüm künye bilgileri içerecek şekilde indirilmiştir. Her iki havuz için ayrı ayrı olarak elde edilen tüm csv dosyaları aynı çalışma tekrar içermeyecek şekilde tek iki farklı csv dosyası ($S_{i=\{1,2,3,4,5\}}$: Tüm yıllar tekrar etmeyen 155 çalışma-$S_{i=\{6,8,10,12,14\}} - S_{i=\{7,9,11,13,15\}}$: Tüm yıllar tekrar etmeyen 76 çalışma) altında toparlanmıştır. Tarih filtrelemesi ile son 6 yıla ilişkin verileri de içerecek şekilde yayınlanan çalışmalar ayrıca makale, bildiri, kitap, kitap bölümü ve derleme türleri açısından filtrelenerek Tablo 10'daki sonuçlar elde edilmiştir. Erişilen literatüre ilişkin oluşturulan csv dosyaları (Seyhan ve ark, 2025) referansı üzerinden erişilebilmektedir. Örneğin,

- Tablo 10'da sunulan 2018-2025 yılları arasında yayınlanan 86 makale Tablo 4'te sunulan genel kavram havuzunda yer alan 10 farklı anahtar kelimeden herhangi birini içeren ve Türkiye adresli araştırmacılar tarafından gerçekleştirilen çalışmaları ifade etmektedir.
- Tablo 10'da sunulan 2018-2025 yılları arasında yayınlanan ve Tablo 4'te verilen 3 anahtar kelimeden (S6-S7 sorgu no ile eşleşen) herhangi birini içeren Türkiye adresli araştırmacılar tarafından gerçekleştirilen bildiri çalışmalarının sayısıdır.

Şekil 10'da sunulan sonuçlar değerlendirildiğinde genel kavram havuzu için belirlenen anahtar kelimeler ile çalışmaların son 6 yılda yoğunlaşıldığı söylenebilmektedir. Özel kavram havuzu için belirlenen anahtar kelimeler özelinde yapılan incelemeler ise Türkiye adresli araştırmacıların kuantum sonrası kriptografi alanında kafes tabanlı kriptosistemler odağında daha fazla çalışma yaptığını göstermektedir. Son 6 yıl için elde edilen sayısal sonuçlar göstermektedir ki akademik çalışma olarak Türkiye adresli araştırmacılar önceliği makale yazımına vermiştir. Bunu takiben de ulusal ve/veya uluslararası konferanslarda yayınlanan bildirilerin yer aldığı söylenebilmektedir.

| Sorgular | S1, S2, S3, S4, S5 | | S6, S7 | S8, S9 | S10, S11 | S12, S13 | S14, S15 | S6, S7 | S8, S9 | S10, S11 | S12, S13 | S14, S15 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Zaman Aralığı | Tüm Yıllar | 2018-2025 | Tüm Yıllar | | | | | 2018-2025 | | | | |
| Tekrar Etmeyen | **155** | 143 | **76** | 5 | 6 | 2 | 7 | **64** | 4 | 5 | 1 | 6 |
| Makale | **89** | 86 | **41** | 1 | 4 | 0 | 3 | **39** | 1 | 4 | 0 | 3 |
| Bildiri | **60** | 51 | **32** | 4 | 2 | 2 | 4 | **24** | 3 | 1 | 1 | 3 |
| Kitap | **2** | 2 | **0** | 0 | 0 | 0 | 0 | **0** | 0 | 0 | 0 | 0 |
| Kitap Bölümü | **2** | 2 | **2** | 0 | 0 | 0 | 0 | **0** | 0 | 0 | 0 | 0 |
| Derleme | **2** | 2 | **1** | 0 | 0 | 0 | 0 | **1** | 0 | 0 | 0 | 0 |

**Şekil 10.** Scopus'ta taranan akademik çalışmalara ilişkin sayısal dağılım.

## 5. Genel Değerlendirme ve Sonuçlar

Gerçekleştirilen bibliyometrik analizler ile Türkiye'de kuantum sonrası kriptografi alanında yapılan lisansüstü ve akademik çalışmaların güncel durumu ve odak noktaları ifade edilmiştir. Lisansüstü çalışmaların bibliyometrik analizi için oluşturulan arama yönteminde yayımlanan tez çalışmalarına erişimde ulusal tez merkezinde tarama yapmak için toplam 42 anahtar kelimeyi içeren genel (9 İngilizce-13 Türkçe) ve özel (8 İngilizce-12 Türkçe) kavram havuzları oluşturulmuştur. Yapılan gelişmiş taramada kuantum sonrası kriptografi ile ilgili tezlere erişmek için üç seçim (SK1, SK2, SK3) ve iki eleme (EK1, EK2) kriteri uygulanarak açık erişimli ve tekrarsız toplam 47 tez olduğu belirlenmiştir. Eleme aşamasında Tanım 2 temel alınarak kuantum sonrası kriptografi alanında çeşitli katkılar sunan tezler değerlendirmeye alınmıştır. Bu aşamada anahtar kelime eşleşmesi olsa bile doğrudan kuantum sonrası kriptografik protokol tasarımı/iyileştirme/uygulama geliştirme amacı olmadığı bilinen homomorfik şifreleme ile alakalı tezler elemeye tabi tutulmuştur. Her ne kadar kafes-tabanlı ilkeleri temel alarak oluşturulsa da doğrudan kuantum sonrası kriptografi ile eşleşme olmaması nedeniyle bu indirgeme yapılmıştır. Ayrıca Tanım 1 kuantum kriptografi kavramı ile alakalı olan kuantum anahtar dağıtımı açısından katkı hedefi bulunan tezler de bu analizin odak noktasında olmadığı için çıkarılmıştır. 47 tez üzerinden yapılan bibliyometrik analizde;

- Tezlerin ait olduğu kriptosistem ailesi bakımından sınıflandırma ile Türkiye'de en fazla kafes-tabanlı kriptosistem özelinde tez yazıldığı tespit edilmiştir.
- Tezler ile kuantum sonrası kriptografi alanında yapılan katkısının sınıflandırılması için protokol tasarımı, uygulama ve aritmetik iyileştirme, bileşen analizi/atak uygulama ve

derleme çalışması olma metrikleri belirlenmiştir. Bu metrikler ile yapılan analiz yüksek lisans ve doktora aşamalarında en fazla kafes-tabanlı kriptosistem ailesi odağında uygulama ve aritmetik iyileştirme üzerine çalışıldığını göstermiştir.

- 47 tezin gerçekleştirildiği lisansüstü aşaması ve yazıldığı dil açısından yapılan analize göre %31.9'luk kısmı oluşturan doktora tezlerinin (15 tane) %73.3'ü İngilizce yazılmışken % 26.7'sinin Türkçe dilinde yazıldığı %68.1'lik kısmı oluşturan yüksek lisans tezlerinin (32) ise %56.3'ü İngilizce yazılmışken %43.7'si Türkçe'dir. Yazılan doktora tezlerinden iki tanesi ilgili anabilim dalında eğitim Türkçe iken İngilizce dilinde yazıldığı gözlemlenmiştir.
- Kuantum sonrası kriptografi alanında gerçekleştirilen açık erişimli tezlerden ilk yüksek lisans çalışması 2007 yılında tamamlanmışken doktora çalışmasının 2016 yılında tamamlandığı belirlenmiştir. En fazla tezin yayınlandığı yıl ise 2022 yılı (6 doktora-5 yüksek lisans) olmuştur.
- Danışman sayısı açısından tezler incelendiğinde yüksek lisans aşamasında 2 doktora aşamasında 4 tez iki danışmanlı olarak gerçekleştirilmiştir. Yüksek lisans aşamasında kalan 11 ve doktora aşamasında kalan 32 tez ise tek danışmanlı olarak yürütülmüştür. İlgili tarihlerde Ondokuz Mayıs Üniversitesi'nde çalışan bir araştırmacı 14 tezde birinci ve ikinci danışman olarak bu alanda en fazla tez bitirten araştırmacı olarak öncü olmuştur.
- Yapılan tezler yazar bakımından incelendiğinde sadece Ondokuz Mayıs Üniversitesi'nde yürütülen iki tezde yer alan kadın araştırmacıların hem yüksek lisansını hem de doktorasını kuantum sonrası kriptografi alanında tamamladığı gözlemlenmiştir.
- Tezlerin gerçekleştirildiği üniversitelerde Orta Doğu Teknik ve Ondokuz Mayıs Üniversiteleri ön plana çıkarken en fazla lisansüstü tez Fen Bilimleri, Uygulamalı Matematik Enstitülerinde ve Kriptografi A.B.D.'nda yapılmıştır.
- Üniversitelerde yapılan tez çalışmalarının kuantum sonrası kriptografi açısından katkıları belirlenen metrikler ile değerlendirildiğinde protokol tasarımı metriğinde Ondokuz Mayıs Üniversitesi, kalan metriklerde Orta Doğu Teknik Üniversitesi ön plana çıkmıştır.
- 47 tezin gerçekleştirilmesinde danışmanların cinsiyet açısından dağılımı değerlendirildiğinde toplamda 42 tezin erkek danışmanlar 5 tezin kadın danışmanlar tarafından yürütüldüğü tespit edilmiştir. Yazarlar açısından kadın-erkek oranı ise 18'e 29'dur.

Kuantum sonrası kriptografi alanında Türkiye adresli araştırmacıların yaptığı akademik çalışmaların güncel durumuna ilişkin bir değerlendirme yapabilmek amacıyla ülke bazlı filtreleme özelliği sunan Scopus veritabanı seçilmiştir. Bu veritabanı üzerinde yayınlanan akademik çalışmaların tespit edilmesi için tez analizi için belirlenen 42 Türkçe ve İngilizce anahtar kelime Scopus ile sorgulama ile uyumlu 20 sorguya indirgenmiştir. Belirlenen sorgular ile (Tablo 5-Tablo 6) Scopus veritabanı

üzerinde yapılan gelişmiş taramada kullanılmak üzere iki seçim (SK4, SK5) ve bir eleme (EK3) kriteri belirlenerek uygulanmıştır.

- Tablo 4'te sunulan genel kavram havuzunda yer alan anahtar kelimelerden en az birini içeren ve tekrar eden çalışma bulunmayan akademik çalışma sayısı tüm yıllarda 155 iken son altı yılda 143 olduğu gözlemlenmiştir.
- Özel kavram havuzu için yapılan analize göre tüm yıllarda kafes-tabanlı 76, özet-tabanlı 5, çok-değişkenli polinom sistemleri-tabanlı 6, izojeni-tabanlı 2 ve kod-tabanlı 7 akademik çalışma yayınlanmıştır. Bunlardan kafe-tabanlıların 64'ü, özet-tabanlıların 4'ü, çok-değişkenli polinom sistemleri-tabanlıların 5'i, izojeni-tabanlıların 1'i ve kod-tabanlıların 6'sı son altı yılda yayımlanmıştır.
- Tüm yıllarda ve son altı yılda yayımlanan akademik çalışmaların (makale, bildiri, kitap, kitap bölümü, derleme çalışması) kafes-tabanlı kriptosistem ailesine ait bileşenler baz alınarak yapıldığı görülmektedir. Kafes-tabanlı kriptosistemleri takiben en fazla yayının kod-tabanlı kriptosistemler özelinde yapıldığı analiz edilmiştir.

Sonuç olarak, bu çalışma kapsamında yapılan analiz ile Türkiye'de kuantum sonrası kriptografi alanında yapılan çalışmaların ve katkı sunulan alanların incelenmesi ile güncel duruma bir bakış sunulması hedeflenmiştir. Kuantum kriptografi ve kuantum sonrası kriptografi ayrımları tanımlanarak kuantum sonrası kriptografi alanında çalışmaların temel odak noktasını oluşturan belirli şartlar altında güvenli olduğu bilinen kriptosistem ailelerinin genel özellikleri ve tanımlamaları sunulmuştur. Ayrıca kuantum sonrası kriptografi açısından öncü kuruluş NIST'in gereksinimleri ve bazı açık problemler ifade edilerek Türkiye'de yapılan çalışmaların bu anlamdaki katkılarının anlaşılması hedeflenmiştir. Bibliyometrik analiz için araştırma yöntemi sistematik ve iki alt bileşenli (lisansüstü tezler-Scopus Türkiye adresli akademik çalışmalar) olarak belirlenmiştir. Oluşturulan araştırma yöntemleri takip edilerek hem lisansüstü tezler hem de akademik çalışmalar sistematik olarak elde edilmiştir. Bu analiz ile sunulan sonuçlar hem kuantum sonrası kriptografi alanında çalışmalar yapmak isteyen araştırmacılara Türkiye'de hem lisansüstü eğitim hem de akademik çalışmalar açısından yön gösterici olacağı düşünülmektedir. Hangi üniversitelerde hangi alt başlıkların nasıl çalışıldığı ile ilgili sunulan sonuçlar ve sınıflandırmada kullanılan tezler bu alanda çalışmalar yapacak araştırmacılar için yol haritası niteliğindedir. Son altı yılda Türkiye'de yapılan çalışmaların artması bu alana olan ilginin gelecekte de artarak devam edeceğini gösterir niteliktedir.

## 6. Ekler

Bölüm 4.1. tezlerin bibliyometrik analizi başlığında incelemeye konu olan tezlere ilişkin tez no değerleri Tablo 7 ile sunulmuştur. (Yükseköğretim Kurulu Başkanlığı, 2025) sayfası üzerinde detaylı arama kısmında tez no bölgesine Tablo 7 ile sunulan değerler yazılarak ilgili tezlere erişilebilmektedir. Ayrıca, bu çalışma kapsamında incelenen tüm tezler (Seyhan ve ark, 2025) klasöründe sunulmuştur.

**Tablo 7.** Analiz için seçilen tez no ve sınıflandırma metrikleri.

| | **Tez No** |
|---|---|
| **Kafes** | **768762, 818606, 864196, 449254, 365575, 830051, 687073, 844884, 775978, 846982, 864131, 783401, 716889, 760471, 680357, 610767, 750001, 850996, 815076, 635010, 648938, 708796, 729853, 611898, 479739, 510472, 830670, 651657, 612231, 232902, 202161, 296883, 757042** |
| **Kod** | **783401, 577019, 547154, 663788, 593158, 899159** |
| **Özet** | **595406** |
| **Polinom Sistemleri** | **558831, 750871, 612263, 519598, 468178** |
| **İzojeni-Tabanlı** | **755858, 731342, 595471** |
| **Erişim Kısıtı** | **895752, 142933, 849122** |
| **protokol tasarımı** | |
| **bileşen analizi/atak uygulama** | |
| **yazılım veya donanım uygulaması geliştirme/aritmetik iyileştirme içerme** | |
| **derleme** | |

## Teşekkürler

Makalenin son haline getirilmesine katkı sunun değerli hakemlere teşekkür ederiz.

## Yazarların Katkısı

Tüm yazarlar çalışmaya eşit katkıda bulunmuştur.

## Çıkar Çatışması Beyanı

Yazarlar arasında herhangi bir çıkar çatışması bulunmamaktadır.

## Araştırma ve Yayın Etiği Beyanı

Yapılan çalışmada araştırma ve yayın etiğine uyulmuştur.

## Kaynaklar


Ajtai, M. (1996, Temmuz). Generating hard instances of lattice problems. *Proceedings of the twenty-eighth annual ACM symposium on Theory of computing* , s. 99-108.

Akleylek, S., & Seyhan, K. (2019). Kuantum Bilgisayarlar Sonrası Güvenilir Kafes Tabanlı Kriptosistem Temellerine Giris. *Siber Güvenlik ve Savunma: Farkındalık ve Caydırıcılık.* içinde

Akleylek, S., & Seyhan, K. (2021). Kuantum Bilgisayar Çağında Kriptosistemlere Bir Bakış. E. K. Sedat Akleylek içinde, *Siber Güvenlik ve Savunma: Blokzincir ve Kriptoloji* (s. 239-275). Ankara: Nobel Akademik Yayıncılık.

Alagic, G., Apon, D., Cooper, D., Dang, Q., Dang, T., Kelsey, J., . . . Smith-Tone, D. (2022). Status report on the third round of the NIST post-quantum cryptography standardization process.

Bavdekar, R., Chopde, E. J., Bhatia, A., Tiwari, K., Daniel, S. J., & Atul. (2022). Post Quantum Cryptography: Techniques, Challenges, Standardization, and Directions for Future Research. *arXiv preprint arXiv:2202.02826*.

Campagna, M., Chen, L., Dagdelen, Ö., Ding, J., Fernick, J. K., Gisin, N., . . . St. (2015). Quantum safe cryptography and security: An introduction, benefits, enablers and challengers. Technical report. . *ETSI (European Telecommunications Standards Institute)*.

Chase, M., Derler, D., Goldfeder, S., Orlandi, C., Ramacher, S., Rechberger, C., . . . Zaverucha, G. (2017). Post-Quantum Zero-Knowledge and Signatures from Symmetric-Key Primitives. *Proceedings of the 2017 acm sigsac conference on computer and communications security*, s. 1825-1842.

Chen, L., Jordan, S., Liu, Y.-K., Moody, D., Peralta, R., Perlner, R., & Smith-Tone, D. (2016). Report on Post-Quantum Cryptography. Gaithersburg, MD, USA.

Chi, D. P., Choi, J. W., Kim, J. S., & Kim, T. (2015). Lattice Based Cryptography for Beginners. *Cryptology ePrint Archive*.

CISA. (2024). Strategy for Migrating to Automated Post-Quantum Cryptography Discovery and Inventory Tools.

Corte-Real Santos, M., Eriksen, J. K., Meyer, M., & Rodríguez-Henríquez, F. (2024). Finding Practical Parameters for Isogeny-based Cryptography. *Cryptology ePrint Archive*.

Dam, D.-T., Tran, T.-H., Hoang, V.-P., Pham, C.-K., & Hoang, T.-T. (2023). A Survey of Post-Quantum Cryptography: Start of a New Race. *Cryptography*, s. 7(3), 40.

Ding, J., & Schmidt, D. (2005). Cryptanalysis of HFEv and Internal Perturbation of HFE. *Public Key Cryptography-PKC 2005: 8th International Workshop on Theory and Practice in Public Key Cryptography, Les Diablerets* (s. 288-301). Switzerland: Springer Berlin Heidelberg.

Ding, J., Petzoldt, A., & Wang, L.-c. (2014). The Cubic Simple Matrix Encryption Scheme. *Post-Quantum Cryptography: 6th International Workshop, PQCrypto 2014, Waterloo, ON, Canada*, s. 76-87.

Dubois, V., Fouque, P.-A., Shamir, A., & Stern, J. (2007). Practical cryptanalysis of SFLASH. *Annual International Cryptology Conference.* (s. 1-12). Berlin: Heidelberg: Springer Berlin Heidelberg.

Ekerå, M. (2019). Revisiting Shor's quantum algorithm for computing general discrete logarithms. *arXiv preprint arXiv:1905.09084*.

Fernández-Caramés, T. M. (2019). From pre-quantum to post-quantum IoT security: A survey on quantum-resistant cryptosystems for the Internet of Things. *IEEE Internet of Things Journal, 7(7)*, s. 6457-6480.

Gheorghiu, V., & Mosca, M. (2019). Benchmarking the quantum cryptanalysis of symmetric, public-key and hash-based cryptographic schemes. *arXiv preprint arXiv:1902.02332*.

Grover, L. K. (1996, Temmuz). A fast quantum mechanical algorithm for database search. *Proceedings of the twenty-eighth annual ACM symposium on Theory of computing*, s. 212-219.

Hasan, K. F., Simpson, L., Rezazadeh Baee, M. A., Islam, C., Rahman, Z., Armstrong, W., . . . McKague, M. (2024). A Framework for Migrating to Post-Quantum Cryptography: Security Dependency Analysis and Case Studies. *IEEE Access, 12*, s. 23427-23450.

Hekkala, J., Muurman, M., Halunen, K., & Vallivaara, V. (2023). Implementing post-quantum cryptography for developers. ). *SN Computer Science, 4(4)*, s. 365.

Hoffstein, J., Lieman, D., Pipher, J., & Silverman, J. H. (1999). NTRU: A public key cryptosystem. *NTRU Cryptosystems, Inc.*

Joseph, D., Misoczki, R., Manzano, M., Tricot, J., Pinuaga, F. D., Lacombe, O., . . . Hansen, R. (2022). Transitioning organizations to post-quantum cryptography. *Nature, 605(7909)*, s. 237-243.

Kasapbaşı, M. C. (2019). A New Chaotic Image Steganography Technique Based on Huffman Compression of Turkish Texts and Fractal Encryption With Post-Quantum Security. *IEEE Access*, 148495-148510.

Koblitz, N. (1987). Elliptic curve cryptosystems., (s. 203-209).

Kumar, A., Ottaviani, C., Gill, S. S., & Buyya, R. (2022). Securing the future internet of things with post-quantum cryptography. *Security and Privacy, 5(2)*.

Küpçüoğlu, E., Alakaş, H. M., & Eren, T. (2024). Blok Zincir Üzerine Yazılan Yüksek Lisans ve Doktora Tezlerinin Bibliyometrik Analizi. *Bilişim Teknolojileri Dergisi, 17(4)*, s. 281-293.

Li, S., Chen, Y., Chen, L., Liao, J., Kuang, C., Li, K., . . . Xiong, N. (2023). Post-Quantum Security: Opportunities and Challenges. *Sensors, 23(21)*, s. 8744.

Miller, V. S. (1985). Use of Elliptic Curves in Cryptography. *Conference on the theory and application of cryptographic techniques* (s. 417-426). Berlin: Springer Berlin Heidelberg.

Niederhagen, R., & Waidner, M. (2017, Ağustos 18). Practical Post-Quantum Cryptography. *Fraunhofer SIT*.

NIST. (2017, Ocak 03). *Post-Quantum Cryptography Standardization Project*. Nisan 23, 2025 tarihinde https://csrc.nist.gov/pqc-standardization adresinden alındı

NIST. (2022, Eylül 6). Request for Additional Digital Signature Schemes for the Post-Quantum Cryptography Standardization Process: https://csrc.nist.gov/Projects/pqc-dig-sig/round-2-additional-signatures adresinden alındı

NIST. (2024, Ağustos 13). *Announcing Approval of Three Federal Information Processing Standards (FIPS) for Post-Quantum Cryptography*. Nisan 23, 2025 tarihinde https://csrc.nist.gov/news/2024/postquantum-cryptography-fips-approved adresinden alındı

NIST. (2024, Ağustos 13). *What Is Post-Quantum Cryptography?* Nisan 23, 2025 tarihinde https://www.nist.gov/cybersecurity/what-post-quantum-cryptography adresinden alındı

NIST. (2025, Mart 11). *NIST Selects HQC as Fifth Algorithm for Post-Quantum Encryption*. https://www.nist.gov/news-events/news/2025/03/nist-selects-hqc-fifth-algorithm-post-quantum-encryption adresinden alındı

Paar, C., & Pelzl, J. (2010). *Understanding cryptography (Vol 1).* Berlin Heidelberg: Springer-Verlag.

Patarin, J. (1996). Hidden Fields Equations (HFE) and Isomorphisms of Polynomials (IP): Two New Families of Asymmetric Algorithms. *nternational conference on the theory and applications of cryptographic techniques (pp. 33-48)* (s. 33-48). Berlin: Heidelberg: Springer Berlin Heidelberg.

Peikert, C. (2016). A decade of lattice cryptography. *Foundations and trends® in theoretical computer science, 10(4)*, s. 283-424.

Pekşen, G. D., & Barman, T. (2024). MOTION CAPTURE TEKNOLOJİLERİ ÜZERİNE BİBLİYOMETRİK BİR ARAŞTIRMA. *Kahramanmaras Sutcu Imam University Journal of Engineering Sciences, 27(3)*, s. 1102-1116.

Scopus. (2025). *Scopus - Document search*. Nisan 23, 2025 tarihinde https://www.scopus.com/search/form.uri?display=basic&zone=header&origin=searchbasic#basic adresinden alındı

Seyhan, K., & Akleylek, S. (2022). Post-Quantum Cryptography: A Snapshot of Standardization Efforts. *Cybersecurity for Critical Infrastructure Protection via Reflection of Industrial Control Systems*, s. 90-99.

Seyhan, K., Akleylek, S., & Dursun, A. F. (2025, Mart). *Scopus Verileri*. http://drive.google.com/drive/folders/1Bx6WWzpXHuzyCm3DeZqRUewpZ5SJIz38 adresinden alındı

Seyhan, K., Nguyen, T. N., Akleylek, S., & Cengiz, K. (2022). Lattice-based cryptosystems for the security of resource-constrained IoT devices in post-quantum world: a survey. *Cluster Computing, 25(3)*, s. 1729-1748.

Shor, P. W. (1999). Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer. *SIAM review*, s. 303-332.

Yükseköğretim Kurulu Başkanlığı. (2025). *Ulusal Tez Merkezi | Anasayfa*. Nisan 23, 2025 tarihinde Ulusal Tez Merkezi: https://tez.yok.gov.tr/UlusalTezMerkezi/ adresinden alındı