Haliç Üniversitesi Fen Bilimleri Dergisi 2025, 8/1: 41-79
DOI: 10.46373/hafebid.1610167

ISSN: 2618-6241
e-ISSN: 2667-5757

Post-Kuantum Kriptografi Anahtar Değişim Mekanizması ile Kaotik Akış Şifreleme Algoritması

Vildan KALKAVAN[1]*, Mustafa Cem KASAPBAŞI[2]

[1]İstanbul Ticaret Üniversitesi, Bilgisayar Mühendisliği, İstanbul, Türkiye
Orcid: 0009-0003-3247-6337, (https://orcid.org/0009-0003-3247-6337)
[2]İstanbul Ticaret Üniversitesi, Bilgisayar Mühendisliği, İstanbul, Türkiye
Orcid: 0000-0001-6444-6659, (https://orcid.org/0000-0001-6444-6659)

Geliş Tarihi: 30.12.2024
Kabul Tarihi: 28.01.2025

***Sorumlu Yazar e mail:** kalkavanvildan@gmail.com

Atıf/Citation: Kalkavan, V., Kasapbaşı, M. C., "Post-Kuantum Kriptografi Anahtar Değişim Mekanizması ile Kaotik Akış Şifreleme Algoritması", Haliç Üniversitesi Fen Bilimleri Dergisi 2025, 8/1: 41-79.

Araştırma Makalesi/ ***Research Article***

Öz

Bu çalışmada, Amerikan Ulusal Standartlar ve Teknoloji Enstitüsü (NIST) tarafından gerçekleştirilen kuantum sonrası kriptografi standartlaştırılması için açılan gönderimlerde de yer alan ve 3. gönderim turuna da katılan CRYSTALS-Kyber algoritması incelenmiş ve bir uygulama ile post-kuantum kriptografi standartlarına uygunluğunu ve performansını değerlendirilmesi yapılmıştır. [1] Algoritma, Hatalar ile Öğrenme (Learning With Errors - LWE) problemine dayanan matematiksel temeliyle, kuantum bilgisayarların tehditlerine karşı dayanıklılık göstermektedir. Uyarlanabilir Seçimli Açık Metin Saldırısına Karşı Güvenlik (IND-CPA: Adaptive Chosen Plaintext Attack) ve Uyarlanabilir Seçimli Şifreli Metin Saldırısına Karşı Güvenlik (IND-CCA2: Adaptive Chosen Ciphertext Attack) güvenlik seviyelerini başarıyla sağlaması, algoritmanın hem doğruluk hem de güvenlik açısından güçlü bir performans sergilediğini ortaya koymaktadır. Bu çalışmada, algoritmanın performans analizi ve güvenlik değerlendirmesi sürecine kaotik harita uygulaması da entegre edilmiştir. Kaotik harita, başlangıç koşullarına duyarlı ve öngörülemez matematiksel yapısıyla güçlü bir rastgelelik sağlayarak algoritmanın şifreleme süreçlerinde kullanılabilecek bir entropi kaynağı olarak değerlendirilmiştir. Kaotik haritalardan türetilen anahtarlar, CRYSTALS-Kyber algoritmasının şifreleme ve şifre çözme süreçlerinde test edilmiştir. Kyber, farklı güvenlik gereksinimlerine hitap eden üç parametre dizisi (Kyber512, Kyber768, Kyber1024) sunmaktadır. Kyber512 düşük kaynak tüketimi gerektiren IoT cihazları gibi uygulamalarda hızlı ve hafif bir çözüm sunar. Kyber768 dengeli bir güvenlik ve performans seviyesine sahiptir. Kyber1024

yüksek güvenlik gereksinimlerini karşılayan en güçlü seçenek olarak dikkat çeker. Test sonuçları, algoritmanın doğruluğunu ve verimliliğini ortaya koymuştur. Yapılan testlerde, Simetrik Anahtar (ss1) ve Asimetrik Anahtar (ss2) değerleri her testte eşleşmiş ve algoritmanın %100 doğruluğa sahip olduğu gösterilmiştir. Ayrıca, Kyber'in şifreleme ve şifre çözme süreçleri, diğer kafes tabanlı algoritmalara kıyasla dengeli bir performans sergilemiştir. Kyber algoritması, NIST'in post- kuantum kriptografi standartlaştırma sürecinde önemli bir aday olarak öne çıkmıştır. Finansal sistemler, IoT güvenliği ve bulut bilişim gibi uygulama alanlarında geniş bir kullanım potansiyeline sahiptir. Bununla birlikte, algoritmanın büyük anahtar boyutları nedeniyle, depolama ve işlem gücü gereksinimleri açısından daha optimize edilmiş sürümlerinin geliştirilmesi önerilmektedir. Sonuç olarak, CRYSTALS-Kyber algoritması, doğruluk, performans ve kaotik harita gibi yenilikçi yaklaşımlar sayesinde post-kuantum güvenlik ihtiyaçlarını karşılamada güçlü bir adaydır. Ancak, algoritmanın daha geniş çaplı testler, kaotik haritaların daha derinlemesine entegrasyonu ve optimizasyonlarla iyileştirilmesi, gelecekteki siber güvenlik gereksinimlerini karşılama kapasitesini artırabilir.

Anahtar Kelimeler: Akış Şifreleme, NIST, Post-Kuantum Kriptografi, Siber Güvenlik

Chaotic Stream Cipher Algorithm with Post-Quantum Cryptography Key Exchange Mechanism

Abstract

This study evaluates the CRYSTALS-Kyber algorithm, which has been included in the submissions opened by NIST for post-quantum cryptography standardization and participated in the 3rd submission round, along with an application to assess its compliance with post-quantum cryptography standards and its performance. [1] Based on the mathematical foundation of the Learning With Errors (LWE) problem, the algorithm demonstrates resilience against the threats posed by quantum computers. Its ability to successfully achieve IND-CPA and IND- CCA2 security levels highlights the algorithm's strong performance in terms of both accuracy and security. In this study, chaotic map application has also been integrated into the performance analysis and security evaluation process of the algorithm. Chaotic maps, with their mathematical structure sensitive to initial conditions and unpredictability, have been considered as a strong entropy source that can be used in the encryption processes of the algorithm. Keys derived from chaotic maps were tested in the encryption and decryption processes of the CRYSTALS-Kyber algorithm. Kyber offers three parameter sets (Kyber512, Kyber768, Kyber1024) catering to different security requirements. Kyber512 provides a fast and lightweight solution for applications such as IoT devices

with low resource consumption. Kyber768 achieves a balanced level of security and performance. Kyber1024 stands out as the most robust option, addressing high-security requirements. Test results reveal the algorithm's accuracy and efficiency. In the tests conducted, Symmetric Key (ss1) and Decapsulated Symmetric Key (ss2) values matched in every test, proving the algorithm's 100% accuracy. Furthermore, Kyber's encryption and decryption processes demonstrated balanced performance compared to other lattice-based algorithms. The Kyber algorithm has emerged as a significant candidate in NIST's post-quantum cryptography standardization process. It holds broad potential for use in applications such as financial systems, IoT security, and cloud computing. However, due to the algorithm's large key sizes, it is recommended to develop more optimized versions in terms of storage and computational requirements. In conclusion, the CRYSTALS-Kyber algorithm is a strong candidate for addressing post-quantum security needs in terms of accuracy, performance, and innovative approaches such as chaotic maps. However, further extensive testing, deeper integration of chaotic maps, and optimizations are suggested to enhance its capacity to meet future cybersecurity demands.

Keywords: Stream Cipher, NIST, Post-Quantum Cryptography, Cybersecurity

1. Giriş

Günümüzde teknolojinin hızlı gelişmesiyle birlikte, kuantum bilgisayarları gelecekte mevcut kriptografik sistemlerin güvenliğini tehdit eder hale gelmiştir. Şifreleme yapmak için kullanılan yöntemlerin bazılarının kuantum bilgisayarlar tarafından çözülmesi kolay olacaktır [2]. Geleneksel kriptografi algoritmaları, özellikle RSA, Diffie-Hellman ve Eliptik Eğri Kriptografisi (ECC) gibi sistemler, kuantum bilgisayarların kullanabileceği Shor algoritması gibi matematiksel çözümler karşısında savunmasızdır [3]. Bu durumda, post-kuantum kriptografi adı verilen ve kuantum bilgisayarların saldırılarına karşı dayanıklı yeni algoritmaların geliştirilmesini günümüzde gelecek siber saldırıların artmasına karşılık zorunlu hale gelmiştir.

Post-kuantum güvenlik yaklaşımlarında, akış şifreleme (stream cipher) yöntemleri dikkat çekici bir çözüm alanı sunmaktadır. Akış şifreleme algoritmaları, sürekli veri akışını şifreleme kabiliyeti sayesinde, özellikle IoT cihazları, ağ iletişimi ve büyük veri transferlerinde yaygın olarak kullanılmaktadır. Ancak, Shor ve Grover algoritmaları

gibi kuantum algoritmalarının simetrik şifreleme sistemlerine getirdiği potansiyel riskler, post-kuantum bilgisayarların bu algoritmaları çözme kolaylığından dolayı bu sistemlerin anahtar boyutlarının artırılmasını ve güvenlik seviyelerinin gözden geçirilmesini gerektirmektedir [4].

Bu bağlamda, NIST tarafından yürütülen post-kuantum kriptografi standartlaştırma süreci büyük önem taşımaktadır. NIST, kuantum bilgisayarların yaratacağı tehditlere karşı güvenli yeni nesil algoritmaların seçilmesi ve test edilmesi amacıyla çeşitli deneyler ve değerlendirmeler yürütmektedir. Yürüttüğü çalışmalarda 82 algoritma önerisi sunmaktadır [2]. Bu süreçte, kafes tabanlı kriptografi ve simetrik şifreleme gibi alanlar öne çıkmakta, güvenlik performansları detaylı olarak incelenmektedir.

Bu çalışma, CRYSTALS-Kyber algoritmasının performansını ve güvenlik seviyelerini analiz ederek, kuantum sonrası dönemde uygulanabilirliğini değerlendirmeyi amaçlamaktadır. Algoritmanın farklı parametre setlerinde yapılan testlerle doğruluğu, güvenilirliği ve pratik uygulamalardaki potansiyeli ortaya konmuştur. Ayrıca, gelecekteki güvenlik standartlarının belirlenmesinde Kyber'in oynayabileceği rol detaylı bir şekilde incelenmiştir.

2. Literatür Özeti

Shor kuantum bilgisayarların klasik bilgisayarlara kıyasla bazı zorlu problemleri çok daha hızlı çözebileceğini gösterirken bu bağlamda, makale özellikle iki zor problem üzerine odaklanmaktadır.

Tam sayıların çarpanlarına ayrılması (Factoring)**:** RSA gibi şifreleme yöntemleri bu zorlu problem üzerine kurulmaktadır.

Ayrık Logaritmalar: Bir başka zorlu matematiksel problem olan "Ayrık Logaritmalar" problemi de birçok kriptografik sistemin temelini oluşturmaktadır.

Shor, kuantum bilgisayarların bu iki problemi polinomal zamanda çözebileceğini gösteren algoritmalar geliştirmiştir. Kuantum

bilgisayarların klasik bilgisayarlara kıyasla hesaplama yeteneklerindeki farklılıklara değinilirken, kuantum mekaniğinin "süperpozisyon" ve "kuantum dolanıklığı" gibi özellikleri sayesinde, kuantum bilgisayarlar paralel hesaplama gücüne sahip olabilmektedir. Bu durum, klasik bilgisayarlarla çözülmesi zor veya imkânsız olan bazı problemlerin kuantum bilgisayarlarda daha hızlı çözülmesine imkân tanır. Bu da kuantum bilgisayarların gücünü göstermektedir. Shor, kuantum bilgisayarlarda hem tam sayıların çarpanlarına ayrılmasına hem de ayrık algoritmalar problemlerine yönelik polinomal zamanlı algoritmalar geliştirmiştir.

Çarpanlara Ayırma**:** RSA algoritması gibi şifreleme yöntemleri, büyük sayıların çarpanlara ayrılmasının zor olması varsayımına dayanmaktadır. Shor, kuantum bilgisayarların bu sayıları çarpanlarına ayırmak için polinomal zamanda işlem yapabileceğini göstermektedir. Bu da RSA gibi yöntemleri kırılabilir hale getirmektedir.

Ayrık Logaritmalar**:** Shor'un algoritması ayrıca ayrık algoritmalar problemlerini de polinomal zamanda çözebilmektedir. Bu da, Eliptik Eğri Kriptografisi (ECC) gibi sistemlerin güvenliğini tehdit etmektedir.

Ayrıca ilgili makale karmaşıklık teorisine de odaklanmakta ve kuantum bilgisayarların klasik bilgisayarlara göre hız avantajı sunduğunu açıklamaktadır. Bu bağlamda, kuantum hesaplamanın klasik hesaplamadaki karmaşıklık sınıfları olan P, NP gibi sınıflarla ilişkisini tartışmakta ve kuantum karmaşıklık sınıflarının tanımını yapmaktadır.

BQP (Sınırlandırılmış Hata Kuantum Polinomal Zaman)**:** Kuantum bilgisayarların çözebileceği problem sınıfları arasında tanımlanan BQP, klasik bilgisayarlarda çözülemeyen problemleri kuantum bilgisayarların çözebileceğini göstermektedir.

Shor, kuantum bilgisayarların hala teorik bir aşamada olduğunu ve bu algoritmaların pratiğe dökülmesinin zorluklarını tartışmaktadır. Kuantum bilgisayarların inşası, hem fiziksel hem de teknik zorluklar nedeniyle o dönemde gerçekleştirilememiştir. Ancak Shor, bu makale ile kuantum bilgisayar araştırmalarına önemli bir katkı sağlayarak, gelecekte bu tür bilgisayarların yapılabileceği umudunu taşımaktadır.

Shor'un algoritmaları, kuantum bilgisayarların kriptografi üzerindeki potansiyel etkilerini göstermektedir. Bu algoritmaların pratiğe dökülmesi halinde, mevcut şifreleme yöntemlerinin kırılabilir hale geleceği, dolayısıyla post-kuantum kriptografi gibi yeni güvenlik sistemlerinin geliştirilmesi gerektiği vurgulanmaktadır [5].

Kuantum bilgisayarların geleneksel kriptografiye getirdiği tehditleri dikkate almaktadır. Kuantum bilgisayarlar, günümüzde kullanılan şifreleme algoritmalarını (RSA, ECC, DH, DSA vb.) kolayca kırabilir algoritmalar olarak görmektedir. Ancak, kuantum bilgisayarlara karşı dayanıklı post-kuantum kriptografi algoritmaları geliştirilmektedir.

Makale, post-kuantum kriptografi için önerilen şemaların güvenliği, etkinliği ve geçiş süreci ile ilgili birçok zorluğu tartışmaktadır. Post-kuantum kriptografi, geleneksel cihazlarla uyumlu olacak şekilde tasarlanmıştır ve çeşitli matematiksel problemlere dayanmaktadır. Bu makale, post-kuantum şifreleme algoritmalarının akademik ve endüstriyel uygulamalarına genel bir bakış sunmaktadır.

Temel zorluklar arasında hangi şemalara güvenileceği, güvenlik parametrelerinin nasıl belirleneceği ve mevcut sistemlerin nasıl uyumlu hale getirileceği gibi konular yer almaktadır. Makale ayrıca kuantum bilgisayarların etkilerine karşı önlem almak için endüstri, hükümet ve kamuoyunun bilgilendirilmesi gerektiğini vurgulamaktadır [6].

Lov K. Grover'un 1996 yılında yayımladığı makale, kuantum bilgisayarların klasik bilgisayarlara kıyasla belirli problemlerde nasıl avantaj sağladığını gösteren temel çalışmalardan biri olarak görülmektedir. Bu makalede Grover, bir veri tabanında arama işleminin kuantum algoritmalarıyla nasıl hızlandırılabileceğini ele alırken klasik arama algoritmalarına göre polinomal bir hızlanma sağladığını söylemektedir.

Grover'un Algoritması**:** Grover, veritabanındaki n öğe arasında bir öğeyi bulmak için klasik bilgisayarlarda gerekli olan O(n) adım yerine, kuantum bilgisayarlarla bu işlemin O(√n) adımda yapılabileceğini göstermektedir. Bu, veri tabanı aramalarındaki hızlanmanın ciddi bir ölçüde artacağı anlamına gelmektedir.

Kuantum Paralelizmi**:** Kuantum süperpozisyon ve dolanıklık gibi kuantum mekaniği prensipleri sayesinde, kuantum bilgisayar aynı anda birden fazla olasılığı değerlendirebilir ve bu da arama işlemlerini klasik bilgisayarlara kıyasla çok daha verimli hale getirmektedir.

Algoritmanın Önemi**:** Grover'un algoritması, simetrik şifreleme gibi alanlarda şifre kırma süresini de hızlandırabilir, ancak bu tehdit, daha uzun anahtar boyutlarıyla bertaraf edilebilmektedir. Aynı zamanda bu algoritma, kuantum bilgi işleminde birçok pratik uygulamanın temelini oluşturmaktadır.

Grover'un algoritması, veri tabanı araması gibi belirli problemlerde kuantum bilgisayarların klasik bilgisayarlara göre nasıl üstün performans gösterebileceğini etkileyici bir şekilde sergilemektedir [7].

Kuantum bilgisayarlar sayıları çarpanlarına ayırma ve ayrık logaritmaları hesaplama gibi görevler için etkin algoritmalar sunarak bu tür problemlerin klasik bilgisayarlara kıyasla kuantum bilgisayarlarda çok daha hızlı çözülebileceğini göstermektedir. Makale, kuantum Fourier dönüşümünün ve periyodik yapıların belirlenmesinde kuantum bilgisayarların gücüne dayanan algoritmaların kullanımını incelemektedir. Ayrıca, bu yaklaşımların "gizli altgrup problemi" olarak bilinen daha geniş bir gruplama teorisine dayanan problemi nasıl çözdüğünü tartışmaktadır.

Shor'un algoritmalarının, büyük tam sayıların çarpanlarına ayrılması ve ayrık logaritmaların kuantum bilgisayarlar ile polinomal zamanda çözülebileceğini gösterirken, Kuantum Fourier Dönüşümü (QFT) periyodik yapıların belirlenmesi ve ayrık Fourier dönüşümünün kuantum bilgisayarlarla nasıl hızlandırılabileceği üzerine odaklanmaktadır. Gizli Altgrup Probleminde, periyodik yapıları genel bir gruplama teorisi bağlamında incelerken hem klasik hem de kuantum algoritmalar için genel çözümler sunmaktadır. Kuantum bilgisayarların çarpanlara ayırma ve ayrık logaritma hesaplaması gibi problemlerde klasik bilgisayarlara üstünlük sağladığı belirtilmektedir [8].

Makale, Kuantum bilgisayarların klasik şifreleme algoritmalarını tehdit ettiği bir geleceğe hazırlanmak amacıyla post-kuantum

kriptografinin önemini ele almaktadır. Özetle, kuantum bilgisayarların mevcut şifreleme sistemlerini (özellikle RSA ve Eliptik Eğri Kriptografisi - ECC) kırabileceği öngörülmektedir. Bu yüzden bu tehdide karşı dirençli yeni algoritmaların geliştirilmesi gerektiği vurgulanmaktadır.

Shor ve Grover algoritmaları gibi kuantum algoritmalarının, RSA, DSA, ve ECC gibi asimetrik şifreleme yöntemlerini kırabileceği tehdidini belirtilirken özellikle Shor'un algoritması büyük sayıların çarpanlarına ayrılması gibi matematiksel problemlerde kuantum bilgisayarların üstün performans gösterdiğini vurgulamaktadır. Kuantum bilgisayarlara karşı güvenli olduğu düşünülen alternatif kriptografik teknikler tartışılırken, bu teknikler arasında kafes tabanlı, kod tabanlı, hash tabanlı, ve çok değişkenli polinom tabanlı şifreleme algoritmaları yer almaktadır. Amerikan Ulusal Standartlar ve Teknoloji Enstitüsü (NIST) tarafından başlatılan post-kuantum kriptografisi standartlaştırma sürecine değinirken, yeni algoritmaların güvenliği ve performansı test edilmekte ve gelecekte kullanılması planlanan standartlar geliştirilmektedir.

Post-kuantum algoritmaların internet güvenliği, veri transferi ve IoT cihazları gibi alanlarda nasıl uygulanabileceği üzerinde durulmaktadır. Bu çözümlerin hem yüksek güvenlik sağlaması hem de pratik olarak kullanılabilir olması gerektiği belirtilmektedir. Post-kuantum kriptografi, kuantum bilgisayarların klasik şifreleme yöntemlerine yönelik tehditleri bertaraf etmek için geliştirilen alternatif yöntemlere odaklanmaktadır. Bernstein ve ekibi, mevcut şifreleme tekniklerinin zamanla güvenli olmayabileceğini ve yeni kuantum sonrası güvenlik standartlarının belirlenmesi gerektiğini vurgulamaktadır [9].

Kuantum bilgisayarların asimetrik kriptografi sistemleri üzerindeki potansiyel tehditlerini ele alan makale, özellikle Shor'un algoritması kullanılarak RSA (Rivest–Shamir–Adleman) ve ECC (Eliptik Eğri Kriptografisi) gibi yaygın şifreleme algoritmalarının kuantum bilgisayarlar tarafından kırılabileceğini incelemektedir.

Shor'un Algoritması**:** Kuantum bilgisayarlar, Shor'un algoritmasını kullanarak büyük sayıların çarpanlarına ayrılmasını çok hızlı bir şekilde gerçekleştirebilmektedir. Bu, RSA gibi büyük asal sayı faktörizasyonu gerektiren algoritmaları savunmasız hale getirmektedir. Aynı zamanda, ECC'de kullanılan ayrık logaritmalar da kuantum bilgisayarların çözebileceği matematiksel problemler arasında yer almaktadır.

Asimetrik Şifrelemenin Tehlikeye Girmesi**:** RSA ve ECC gibi geleneksel asimetrik şifreleme sistemleri, klasik bilgisayarların zorlukla çözebildiği matematiksel problemler üzerine kurulmuştur. Ancak, kuantum bilgisayarların bu problemlere hızlı çözümler getirebilme kapasitesi, bu sistemlerin güvenliğini tehdit etmektedir. Özellikle finansal işlemler, güvenli iletişim ve dijital imzalar gibi alanlarda kullanılan bu algoritmalar, kuantum dönemiyle birlikte ciddi bir risk altında bulunmaktadır.

Post-Kuantum Kriptografi**:** Makale, bu tehditlere karşı geliştirilen post-kuantum algoritmalarına da değinmektedir. Kafes tabanlı, hash tabanlı ve diğer kuantum dirençli algoritmalar, mevcut sistemlerin yerine geçmesi planlanan yeni yaklaşımlardır. Bu algoritmalar, kuantum bilgisayarların saldırılarına karşı dayanıklı olacak şekilde tasarlanmaktadır. Makale, asimetrik kriptografi sistemlerinin geleceğini ele alırken, kuantum bilgisayarların gelişimine karşı alınması gereken önlemler ve post-kuantum kriptografisinin önemini vurgulamaktadır [10].

Simetrik anahtar şifreleme, hem şifreleme hem de deşifreleme işlemleri için tek bir ortak anahtarın kullanıldığı bir yöntemdir. Makalede, çeşitli simetrik şifreleme algoritmaları (AES, DES, 3DES, Blowfish, RC4 vb.) ele alınmakta ve bu algoritmaların avantajları, dezavantajları ve uygulama alanları karşılaştırmalı olarak sunulmaktadır. Simetrik şifreleme yöntemleri, günümüzdeki veri güvenliği ihtiyaçlarına cevap vermek üzere tasarlanmıştır. Özellikle ağ güvenliği, veri gizliliği ve yetkisiz erişimi engellemek amacıyla kullanılmaktadır. Bu algoritmalar, büyük veri transferlerinde, finansal işlemlerde ve kişisel bilgilerin korunmasında etkin rol oynamaktadır. Makalede

bahsedilen AES ve Blowfish gibi algoritmalar, hız ve güvenlik açısından yüksek performans göstererek geniş çaplı veri şifreleme gereksinimlerini karşılamaktadır. AES, devlet düzeyinde güvenlik sağlarken, Blowfish daha düşük kaynaklı cihazlarda hızlı bir şekilde uygulanabilmektedir. Uygulandığı alanlar:

RC4 gibi algoritmalar, özellikle ağ protokollerinde (örn. SSL/TLS) kullanılır. Bu algoritmalar, sürekli veri akışını güvenli hale getirerek hızlı ve güvenilir şifreleme sağlar.

Finans ve Bankacılık Sistemleri**:** AES ve 3DES, finansal sistemlerde sıkça kullanılır. Bu sistemlerde veri güvenliği kritik olduğundan, güçlü şifreleme algoritmalarına ihtiyaç vardır.

Kişisel Verilerin Korunması**:** Simetrik şifreleme algoritmaları, kişisel verilerin güvenliğinin sağlanmasında da büyük rol oynar. Şirket içi gizli bilgiler, kullanıcı verileri ve diğer hassas bilgiler bu algoritmalarla korunur.

Güvenlik karşılaştırmaları yapıldığında, AES, özellikle güçlü güvenlik gerektiren ortamlarda yaygın olarak kullanılmaktadır. Hem 128-bit hem de 256-bit anahtar boyutları ile çeşitli güvenlik seviyeleri sağlamaktadır. Blowfish**,** daha esnek anahtar boyutlarına sahip olması nedeniyle, hem küçük ölçekli cihazlarda hem de yüksek hızlı veri şifreleme uygulamalarında yaygın olarak tercih edilmektedir. DES ve 3DES**,** artık modern güvenlik gereksinimlerini karşılayamamakla birlikte, daha önce kullanılan algoritmalar arasında yer almaktadır. 3DES, DES algoritmasını üç defa uygulayarak güvenliği artırmaya çalışsa da, işlem gücü gereksinimleri açısından verimsizdir ve yerini AES gibi daha güvenli algoritmalara bırakmıştır [11].

Çalışma, Simetrik şifreleme yöntemlerinin mevcut durumunu ele alarak bu algoritmaların güvenlik özelliklerini, karşılaştıkları zorlukları ve kuantum bilgisayarların oluşturduğu tehditlere karşı gelecekte nasıl korunabileceklerini tartışmaktadır.

Makale, DES, Uluslararası Veri Şifreleme Algoritması (IDEA: International Data Encryption Algorithm), RC5 ve AES gibi yaygın kullanılan simetrik şifreleme algoritmalarını incelemektedir. DES, eski

bir algoritma olduğu için modern güvenlik ihtiyaçlarını karşılayamamaktadır. Uluslararası Veri Şifreleme Algoritması (IDEA: International Data Encryption Algorithm) algoritması diferansiyel ve lineer saldırılara dayanıklı olmasına rağmen çarpışma ve anahtar-zamanlama saldırılarına karşı savunmasızdır. RC5, esnek anahtar uzunlukları ve verimliliğiyle dikkat çekerken, AES ise modern güvenlik standartlarında en güçlü algoritmalardan biri olarak öne çıkmaktadır. AES, 128, 192 ve 256 bitlik anahtar boyutları ve sabit blok boyutları ile yüksek düzeyde güvenlik sağlar. AES'in bayt dönüşümü, satır kaydırma, sütun karıştırma ve anahtar ekleme gibi yapısal işlemleri, şifreleme sürecinin güçlü ve güvenilir olmasını sağlayarak geniş bir kullanım alanı oluşturmaktadır.

Makale ayrıca kuantum bilgisayarların simetrik şifreleme üzerindeki etkilerini incelemektedir. Kuantum bilgisayarların Grover algoritması sayesinde anahtar arama sürelerini karekök hızında azaltabileceği belirtilmektedir. Bu durum, simetrik algoritmalar için bir tehdit oluştursa da, anahtar boyutlarının artırılmasıyla bu tehdit minimize edilebilmektedir. Örneğin, AES-128 yerine AES-256 kullanımı, kuantum saldırılarına karşı daha dirençli bir çözüm sunmaktadır.

Kuantum bilgisayarların oluşturduğu bu tehditler karşısında post-kuantum kriptografi çözümleri önerilmektedir. Yeni nesil kuantum dirençli teknikler, simetrik şifreleme algoritmalarının güvenliğini güçlendirmekte önemli bir rol oynayacaktır. Makale, post- kuantum araştırmalarının, simetrik şifreleme yöntemlerinin gelecekteki güvenlik altyapılarını nasıl destekleyeceğine dair önemli bilgiler sunmaktadır.

Sonuç olarak, bu makale, simetrik şifreleme algoritmalarının mevcut güvenlik durumunu analiz ederek, kuantum bilgisayarların oluşturduğu tehditlere karşı alınması gereken önlemleri vurgulamaktadır. AES gibi güçlü algoritmaların önemi bir kez daha öne çıkarken, anahtar boyutlarının artırılması ve kuantum sonrası kriptografi çözümlerinin geliştirilmesi, güvenliğin sürdürülebilirliği açısından kritik bir adım olarak ele alınmaktadır. Bu çalışma, simetrik şifreleme alanında çalışan araştırmacılar ve uygulayıcılar için değerli bir referans kaynağıdır [12].

Kafes tabanlı kriptografinin hem teorik hem de uygulamalı yönlerini basit ve anlaşılır bir şekilde açıklamayı hedeflemektedir. Yazarlar, özellikle Chris Peikert'in 2013'te verdiği Bonn derslerinden esinlenerek bu konuyu detaylandırmıştır. Notlar, hem temel kavramları hem de bu kavramların kriptografik uygulamalardaki yerini kapsamaktadır.

Kafes, çok boyutlu uzaylarda düzenli noktalar kümesi olarak tanımlanmaktadır. Kafes tabanlı kriptografi, kuantum bilgisayarlar karşısında dirençli olduğu bilinen Shortest Vector Problem (SVP) ve Hatalar ile Öğrenme (Learning With Errors - LWE) gibi matematiksel problemlere dayanmaktadır. Bu problemler, hem teorik olarak sağlam bir güvenlik temeli sunar hem de kuantum algoritmalarının bu yapıları çözmekte yetersiz kalması nedeniyle post-kuantum dönemde büyük bir avantaj sağlamaktadır.

Halka Tabanlı Hatalar ile Öğrenme (Ring-LWE) ve Kriptografik Uygulamaları çalışmanın ikinci bölümünde, Lyubashevsky, Peikert ve Regev'in "A Toolkit for Ring-LWE" adlı makalesine dayanmaktadır. Halka Tabanlı Hatalar ile Öğrenme (Ring-LWE), kafes tabanlı algoritmaların verimliliğini artırmak için kullanılan önemli bir optimizasyondur. Bu bölümde, halka yapıları ve bu yapılar üzerinden geliştirilen algoritmalar detaylandırılmıştır. Özellikle NTRUEncrypt gibi şifreleme sistemleri ve Dilithium gibi dijital imza algoritmalarının temelinde Halka Tabanlı Hatalar ile Öğrenme (Ring-LWE)'nin kullanıldığı vurgulanmıştır.

Çoklu Doğrusal Haritalar ve Güvenlik Analizleri ders notlarının üçüncü kısmı, Hu ve Jia'nın GGH haritası ile ilgili kriptografik analizlerini ve çoklu doğrusal haritaların kullanımını incelemektedir. Çoklu doğrusal haritalar, homomorfik şifreleme ve diğer ileri düzey kriptografik uygulamalar için kritik bir bileşendir [13].

3. Stream Cipher (Akış Şifreleme Algoritması)

Akış şifreleme (stream cipher), veriyi bit veya byte düzeyinde, sürekli bir akış halinde şifreleyen simetrik şifreleme yöntemidir. Bu

yöntem, özellikle donanım uygulamalarında ve gerçek zamanlı veri iletiminde yaygın olarak kullanılmaktadır. Akış şifreleme algoritmaları, genellikle yüksek hız ve düşük gecikme avantajları sunmaktadır.

3.1 Akış Şifreleme Çalışma Prensibi

Akış şifreleme algoritmalarının temel çalışma prensibi, bir anahtar ve genellikle bir başlatma vektörü (IV) kullanarak bir anahtar akışı (keystream) üretmektir. Bu anahtar akışı, açık metinle (plaintext) bit düzeyinde XOR işlemine tabi tutularak şifreli metin (ciphertext) elde edilir. Deşifreleme işlemi ise aynı anahtar akışıyla şifreli metnin tekrar XOR işlemine tabi tutulmasıyla gerçekleştirilir. Akış şifreleme, veriyi bireysel bitler veya baytlar düzeyinde şifreleyen bir sistemdir. Şifreleme sırasında şu adımlar izlenir:

Anahtar Akışı Üretimi: Anahtar akışı üreteci, bir başlangıç anahtarı ve bir başlangıç vektörü (IV) kullanarak uzun bir anahtar dizisi (key stream) oluşturur. Bu diziler, rastgele bir akış gibi görünür, ancak tamamen deterministiktir [14].

XOR İşlemi: Anahtar akışı, şifrelenecek veriyle (plaintext) bit düzeyinde XOR işlemine tabi tutulur. XOR işlemi şu şekilde çalışır:

- Eğer bitler aynıysa (0 ve 0 veya 1 ve 1), sonuç 0 olur.
- Eğer bitler farklıysa (0 ve 1 veya 1 ve 0), sonuç 1 olur. [14]

Şifreli Veri: XOR işleminin çıktısı, şifrelenmiş veri (ciphertext) olarak elde edilir. Aynı anahtar akışı, ciphertext ile XOR yapıldığında orijinal veriyi (plaintext) geri verir.

Akış şifreleme algoritmaları, donanım uygulamalarında ve gerçek zamanlı veri iletiminde yaygın olarak kullanılmaktadır. Özellikle düşük donanım maliyeti ve yüksek hız gerektiren uygulamalarda tercih edilmektedir. Ancak, akış şifreleme algoritmalarının güvenliği, kullanılan anahtar akışının rastgeleliği ve gizliliği ile doğrudan ilişkilidir. Bu nedenle, anahtar yönetimi ve başlatma vektörlerinin doğru kullanımı kritik öneme sahiptir.

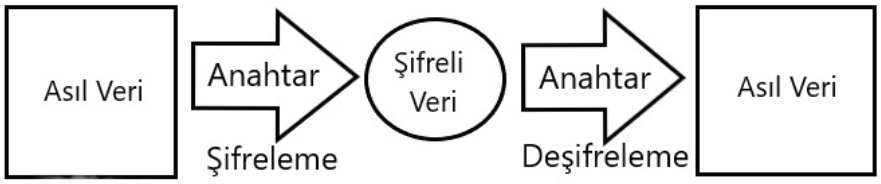
Akış şifreleme algoritmalarının güvenliği, üretilen anahtar akışının rastgeleliği ve tahmin edilemezliği ile doğrudan ilişkilidir. Eğer anahtar akışı yeterince rastgele değilse veya tekrar ediyorsa, saldırganlar şifreli metni çözebilmektedir. Bu nedenle, güvenli bir akış şifreleme sistemi için güçlü bir anahtar yönetimi ve uygun başlatma vektörü (IV) kullanımı gerektirmektedir. Akış şifreleme algoritmalarının avantajları arasında yüksek hız, düşük gecikme ve donanım uygulamalarına uygunluk bulunmaktadır. Ancak, anahtar ve IV yönetimi zorlukları, potansiyel güvenlik açıkları ve senkronizasyon gereksinimleri gibi dezavantajları da vardır [15].

Akış şifreleme algoritmaları, donanım maliyeti açısından düşük ve hız açısından yüksek uygulamalar tercih edildiği görülmektedir. Örnek olarak kablosuz iletişim, akıllı kartlarda ve gerçek zamanlı veri şifrelemelerde farklı uygulamalarda kullanılır. Simetrik şifreleme için Akış Şifreleme algoritmaları önemli bir yere sahip ve belirli uygulama alanlarında avantajları olduğu düşünülür. Ancak, güvenli bir kullanım için dikkatli bir anahtar yönetimi ve algoritma seçimi önemlidir.

3.1.1 Akış Şifreleme Türleri

3.1.1.1 Simetrik Şifreleme

Gönderilen bir metnin şifrelemek ve şifreyi çözmek için kullanılan tek anahtar olan bir şifreleme türüdür. Burada şifreyi çözmek için kullanılan bir anahtar varken sistem daha basit ve hızlıdır ancak buradaki dezavantaj iki tarafında anahtara doğru ve düzgün şekilde ulaşabilmesidir. Anahtara ulaşılsa bile tam metine ulaşılabilmesi kesin değildir [16]. Sezar, DES, 3DES, Blowfish gibi algoritmalar da örnek olarak verilebilir.

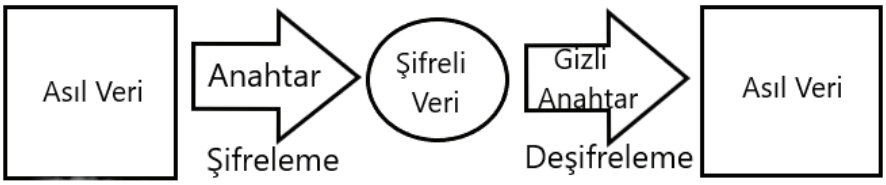


Şekil 1. Simetrik Şifreleme.

Simetrik Şifreleme avantajları olarak sadece anahtara sahip kişi şifreyi çözebileceği için metnin çözülmesi mümkün değildir. Veri kayıplarından etkilenmediği düşünülmektedir.

3.1.1.2 Asimetrik Şifreleme

Simetrik şifrelemede tek anahtar varken burada şifreleme için açık anahtar kullanılır. Deşifreleme işlemi için gizli ayrı bir anahtar kullanılmaktadır. Buradaki ayrıntı anahtarın simetrik olmamasıdır. Açık anahtar saldırgan eline geçse bile gizli anahtarı bilmediği için her hangi bir işe yaramamaktadır. RSA şifreleme algoritması da buna örnek olarak verilebilir. Şifrelemede açık anahtar alıcıya koruma yapılmadan iletildiğinde çözecek kişi açık anahtardan gizli anahtarı üreterek deşifreleme yapar. Açık anahtarın da tehlikeli kişilerin eline geçmesi bir şey ifade etmemektedir [17].



Şekil 2. Asimetrik Şifreleme.

3.1.2 Avantajları ve Dezavantajları

Akış şifreleme algoritmaları hız ve sürekli veri akışları daha iyi olduğu için ve düşük kaynak tüketimi açısından donanıma sahip IoT cihazları gibi uygulamalarda da kullanımı idealdir. Esneklik gerektiren gerçek zamanlı olması gereken uygulamalarda da güvenli mesajlaşma gibi uygunluğu avantajlarından biridir.

Şifreleme ve deşifrelemede aynı anahtar akışını senkronize bir şekilde kullanmayı gerektirmektedir. Aksi takdirde veriler erişilemez olur. Anahtarların güvenliği kritik öneme sahiptir ve güvenli olmayan anahtar yönetimi sistem için ciddi riskler oluşturabilmektedir. RC4 gibi eski algoritmalar, içerdiği zayıflıklar nedeniyle modern saldırılara karşı savunmasız hale gelmektedir. Bunlar da dezavantajları arasında değerlendirilebilmektedir.

3.1.3 Post-Kuantum Dönem ve Akış Şifreleme

Kuantum bilgisayarların gelişmesiyle birlikte akış şifreleme algoritmalarının güvenliği yeniden ele alındığında kuantum bilgisayarların Shor Algoritması ile asimetrik şifrelemeyi kırma yeteneği, Grover Algoritması ile simetrik şifrelemede anahtar arama sürelerini hızlandırma potansiyeli, akış şifreleme algoritmalarının da güvenlik seviyelerinin artırılmasını gerektirmiştir.

ChaCha20 gibi modern akış şifreleme algoritmalarının kuantum sonrası dönemde kullanılabilirliği araştırılmaktadır. Ayrıca, daha uzun anahtar boyutlarının kullanımı (örneğin, 256 bit ve üzeri) bu tür tehditlere karşı etkili bir savunma sunmaktadır.

AES-256, 256 bitlik anahtar uzunluğuyla yüksek güvenlik sağlamasıyla öne çıkar ve hassas verilerin korunmasında tercih edilen bir yöntemdir. Hem donanım hem de yazılım uygulamaları için hızlı ve etkili bir çözüm sunan bu algoritma, disk şifreleme ve güvenli iletişim gibi çeşitli alanlarda yaygın olarak kullanılmaktadır [18].

4. Kafes Tabanlı Algoritma

Kafes tabanlı algoritmalar, günümüzün klasik kriptografik sistemlerinin kuantum bilgisayarlar tarafından tehdit edilmesi durumuna karşı geliştirilen en etkili post-kuantum kriptografi yöntemlerinden biridir. Bu algoritmalar, matematiksel olarak çok boyutlu kafes adı verilen yapılara dayanmakta ve özellikle güçlü güvenlik özellikleriyle

dikkat çekmektedir. Klasik ve kuantum bilgisayarların çözmesi matematiksel olarak son derece zor olan belirli problemleri temel almaktadır. Bu nedenle, kuantum bilgisayarlar gibi güçlü teknolojilerin bile bu algoritmaları kırması pratikte mümkün değildir [2].

Tablo 1. Bilinen bazı kuantum işlemcileri.

İsim	Geliştirici	Kübit Sayısı	Geliştirme Yılı
IBM Osprey	IBM (Amerika Birleşik Devletleri)	433	2022 (Kasım)
Borealis	Xanadu (Kanada)	216	2022 (Haziran)
IBM Eagle	IBM (Amerika Birleşik Devletleri)	127	2021
Jiuzhang	Çin Bilim ve Teknoloji Üniversitesi (ÇHC)	76	2020
Sycamore	Google (Amerika Birleşik Devletleri)	53	2019
Tangle Lake	Intel (Amerika Birleşik Devletleri)	49	2018
Advantage	D-Wave (Kanada)	5640	2020

Kafes tabanlı algoritma çok boyutlu bir uzayda düzenli bir şekilde dağıtılmış noktalar kümesi olarak tanımlanmaktadır. Matematiksel olarak, kafes bir temel vektör kümesiyle oluşturulan tüm tamsayı kombinasyonlarıyla ifade edilmektedir [19]. Örneğin, iki boyutlu bir kafes, bir düzlemde düzenli bir şekilde yerleştirilmiş sonsuz sayıda nokta olarak düşünülebilir. Daha yüksek boyutlarda, bu yapı karmaşık matematiksel özelliklere sahip olur ve güvenlik açısından avantaj sağlamaktadır. Bu tanım, kafes kavramının matematiksel ve kriptografik bağlamdaki genel kabul görmüş tanımına dayanmaktadır. Kafes tanımı, lineer cebir ve matematiksel analizde kullanılan temel bir kavramdır.

Kafes, bir temel vektör kümesiyle (örneğin, $b_1, b_2, ..., b_n$) oluşturulan ve bu vektörlerin tüm tamsayı kombinasyonlarını içeren nokta kümesi olarak ifade edilir:

$$L = \{\sum_{i=1}^{n}(z_i b_i \mid \in \mathbb{Z})\}$$

Bu matematiksel model, kriptografi uygulamalarında kafes tabanlı problemler için temel oluşturmaktadır [19].

Kafes tabanlı algoritmalar, özellikle şu iki zor matematiksel probleme dayanır: Shortest Vector Problem (SVP): Bir kafesteki en kısa vektörün bulunması.

Closest Vector Problem (CVP): Rastgele bir noktaya en yakın kafes noktasının belirlenmesi [13].

Bu problemlerin, hem klasik hem de kuantum bilgisayarların çözmesi açısından hesaplama olarak oldukça zor olduğu kabul edilmektedir.

Kafes tabanlı algoritmalar, homomorfik şifreleme gibi yenilikçi uygulamalara olanak tanımaktadır. Bu teknik, verilerin şifreli haldeyken işlem görmesine imkan verir ve bulut bilişim gibi alanlarda büyük avantajlar sağlamaktadır. Ancak anahtar boyutu olarakta klasik sistemlere kıyasla daha büyük anahtar boyutlarına sahip olması depolama ve işlem gücü gereksinimlerini artırabilmektedir.

Güvenlik yönünden dikkat çeken kafes tabanlı problemler, hem klasik hem de kuantum bilgisayarlarla çözülmesi zor matematiksel yapılara dayanırken uygulama alanları da dijital imzalar, anahtar değişimi ve şifreleme gibi kritik kriptografik işlevlerde kullanılmaktadır. Bu tür algoritmalar, NIST'in post-kuantum kriptografi standartlaştırma sürecinde öne çıkan adaylar arasında yer almaktadır. Dayanıklılık açısından şifreleme algoritmasını belirlemek için yürütülen çalışmalarda CRYSTALS-KYBER ve CRYSTALS-Dilithium gibi algoritmaları standart olarak kabul etmişlerdir. Dijital imza, anahtar oluşturma gibi işlemler için tasarlanmışlardır [20].

"Klasik bilgisayarlardaki bitlerin aksine kuantum bilgisayarlardaki kübitler, sadece "0" ve "1" durumunda değil bu durumların bir süperpozisyonunda da bulunabilmektedir. Kübitler üzerinde yapılan

işlemler her iki durumu da aynı anda etkilemektedir. Kuantum bilgisayarları n tane kübit varsa, kuantum mekaniği ilkeleriyle uyumlu, 2^n farklı durumun süperpozisyonunda bulunabilmektedir. Dolayısıyla n tane kübite sahip bir kuantum bilgisayarı, tek bir seferde 2^n tane işlemi paralel olarak gerçekleştirebilmektedir. Kuantum bilgisayarların klasik bilgisayarlara kıyasla güçlü olmasını sağlayan bu özelliktir." [2]

5. Yöntem

Literatür taramasında, öncelikli olarak Shor, Grover algoritmalarının değerlendirmelerine ve akış şifreleme algoritmalarının güvenliği, kriptografi yöntemlerinin kuantum bilgisayarların tehditlerine karşı güvenliğe nasıl bir çözüm sunduğunu ve NIST'in post-kuantum kriptografi standartlaştırma sürecinde bu algoritmaların önemi ele alındı. Bu bölümde, çalışmamızın uygulama aşamasında izlenen yöntemsel çerçeve açıklanacaktır.

Bu çalışmada, NIST'in standartlaştırma sürecinde önerilen Kyber ve Dilithium gibi öne çıkan, yayımlanan kafes tabanlı algoritmalardan Kyber'in yayımlanan açık kaynak kodları çeşitli testler ve analizler gerçekleştirilmiştir. Temel amaç, bu algoritmanın performans, güvenlik ve uygulama uygunluğu açısından değerlendirilmesi ve kuantum sonrası dönemde kullanılabilirliğinin ortaya konmasıdır.

5.1 Test Ortamının Kurulması

Performans ve güvenlik analizleri için deney ortamı oluşturulacaktır. Bu ortamda:

Testler, belirli işlemci ve bellek kapasitelerine sahip bir sistemde gerçekleştirilecektir. Algoritmaların NIST tarafından sağlanan CRYSTALS-Kyber kodlarının farklı parametre setlerinde (Kyber512, Kyber768, Kyber1024) performansını ve doğruluğunu, algoritmanın şifreleme, şifre çözme ve ortak anahtar üretim süreçlerinin doğruluğunu

değerlendirmek için test vektörleri kullanarak doğruluğu ispatlanacaktır [21].

Test ortamında kullanılan araç ve teknolojiler:

- Dil ve Kütüphaneler:
  - o Programlama dili: JavaScript
  - o Kriptografik kütüphaneler: SHA3, SHAKE (Node.js için).
  - o Rastgele sayı üretimi: WebCrypto API.
- Sistem Özellikleri:
  - o Windows 10
  - o Intel(R) Core(TM) i7-10750H CPU @ 2.60GHz 2.59 GHz
- Test Verileri:
  - o PQCkemKAT_1632.rsp, PQCkemKAT_2400.rsp gibi dosyalar (NIST tarafından sağlanan test vektörleri) [22].
- Araçlar:
  - o Node.js dosya okuma modülü (fs), algoritma uygulamaları ve doğrulama işlemleri.

5.2 Algoritma ve Akış

5.2.1 Crystals-Kyber Algoritması

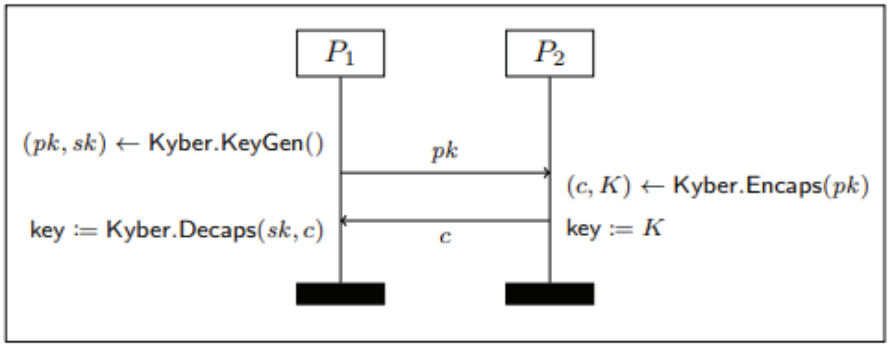
Kyber parametre setlerinde, her parametre dizisi belirli bir anahtar uzunluğu ve performans gereksinimine sahiptir. Kyber'in esnekliği ve güvenlik avantajlarıyla birlikte, Halka Tabanlı Hatalar ile Öğrenme (Ring-LWE) tabanlı şemalara benzer verimlilik sunduğunu göstermektedir. Bu özellikleriyle Kyber, post-kuantum kriptografi standartları arasında öne çıkmaktadır [21].

- **Kyber512:** Hafif güvenlik düzeyi.
- **Kyber768:** Orta güvenlik düzeyi.
- **Kyber1024:** Yüksek güvenlik düzeyi.

Anahtar Üretimi (KeyGen): Algoritmanın KeyGen işlevi ile şifreleme ve şifre çözme için kullanılan anahtar çifti üretilir.

- Kyber algoritmasıyla uyumlu bir genel anahtar (pk) ve özel anahtar (sk) oluşturur.

• Özel anahtar, genel anahtarın bir hash değeri (h(pk)) ve rastgele değerlerden (rnd) oluşan birleştirilmiş bir yapıya sahiptir.



Şekil 3. Kyber.KE – Kyber anahtar kapsülleme mekanizmasını (KeyGen, Encaps, Decaps) kullanan bir anahtar değişim protokolü [21].

Şifreleme (Encrypt): Rastgele bir mesaj alınır, bu mesaj şifreleme işlevi kullanılarak şifrelenir.

• Bir genel anahtar (pk) ile bir mesajı şifreler ve bu işlem sonucunda bir şifreli metin (c) ve simetrik bir anahtar (ss) oluşturur.
• SHA3 ve SHAKE gibi kriptografik hash algoritmaları kullanılarak güvenlik sağlanır.

Şifre Çözme (Decrypt): Şifrelenen mesaj, Decrypt işlevi ile çözülür ve paylaşılan anahtar (shared secret) doğrulanır.

• Bir şifreli metni (c) ve özel anahtarı (sk) kullanarak simetrik anahtarı (ss) geri elde eder.
• Şifreleme sırasında kullanılan adımlar tersine uygulanarak güvenli bir şekilde çözümleme yapılır.

IND-CPA ve IND-CCA2 dönüşümünde kod, IND-CPA güvenlik seviyesinde bir anahtar çifti oluşturur ve ardından "FO dönüşümü" kullanarak IND-CCA2 güvenliği sağlamaktadır. Matris ve polinom işlemlerinde A matrisi oluşturma, polinomu baytlara çevirme, Modüler Sayı Dönüşümü, sadeleştirme gibi işlemler polinomlar üzerinde matematiksel işlemleri gerçekleştirmektedir. Kriptografik hash

kullanımında SHA3-256, SHA3-512 ve SHAKE-256, çeşitli veri yapılarını hashleyerek güvenliği artırır [23].

5.2.2 Testlerin Detayları ve Çıktıları

Kyber'in vermiş olduğu test verilerinden yola çıkıp algoritma akışını inceleyelim.

5.2.2.1 Test Verilerinin Okunması

NIST tarafından sağlanan test dosyaları (PQCkemKAT_*) kullanılarak testler yapılmıştır. Örnek:

Plaintext

ct: Ciphertext

ss: Shared Secret sk: Private Key

5.2.2.2 Kod Örneği

Javascript

let fs = require('fs');

let textByLine = fs.readFileSync('./node_modules/crystals- kyber/PQCkemKAT_1632.rsp').toString().split("\n");

Her test vektörü, algoritmanın şifreleme ve deşifreleme işlevleriyle doğrulandı.

5.2.3 Test Sonuçları

5.2.3.1 Doğruluk Kontrolü

Şifreleme ile üretilen paylaşılan gizli şifreleme anahtarı (SS1) ve deşifreleme ile üretilen paylaşılan gizli deşifreleme anahtar (SS2) karşılaştırılmıştır. Doğruluk için SS1 ve SS2'nin eşit olması beklenmektedir.

Çıktı:
plaintext
Test run [0] success Test run [1] success
...
Test run [99] success

5.2.3.2 Başarısız Test Durumları

Eğer SS1 ve SS2 farklıysa, test çıktısı hata olarak işaretlenir. Örnek:
plaintext
Test run [10] failed

5.2.4 Performans ve Doğruluk Analizi

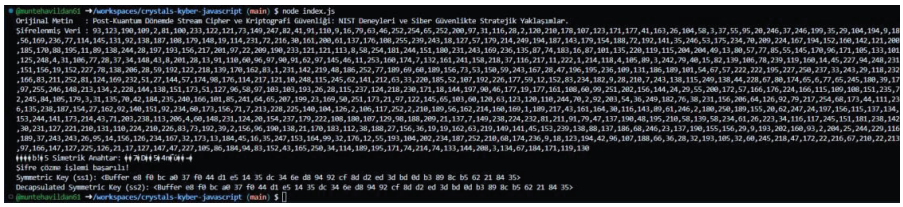
Testlerden elde edilen bulgular, doğruluk ve performans açısından analiz edilerek karşılaştırmalı bir şekilde incelenmiştir.

5.2.4.1 Doğruluk

Elde edilen datalarda Kyber512, Kyber768 ve Kyber1024 de ayrı ayrı yapılan testlerde SS1 ve SS2 değerlerinin hepsi için eşit olduğu görülmüştür. SS1 ve SS2'nin eşit olmaları algoritmanın doğruluğunu kanıtlamaktadır.

5.2.4.1.1 Kyber512 Testi

Symmetric Key (ss1): <Buffer e8 f0 bc a0 37 f0 44 d1 e5 14 35 dc 34 6e d8 94 92 cf 8d d2 ed 3d bd 0d b3 89 8c b5 62 21 84 35>
Decapsulated Symmetric Key (ss2): <Buffer e8 f0 bc a0 37 f0 44 d1 e5 14 35 dc 34 6e d8 94 92 cf 8d d2 ed 3d bd 0d b3 89 8c b5 62 21 84 35>

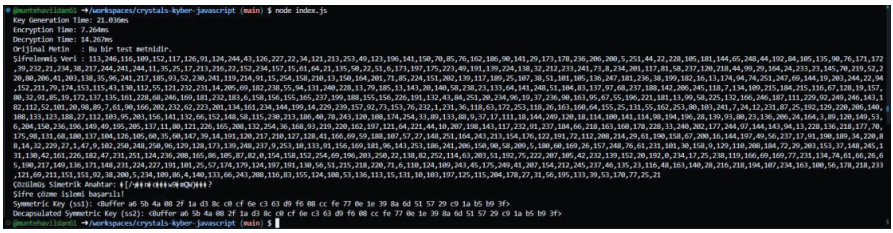


Şekil 4. Kyber512 Test Çıktısı.

Symmetric Key (ss1): <Buffer a6 5b 4a 08 2f 1a d3 8c c0 cf 6e c3 63 d9 f6 08 cc fe 77 0e 1e 39 8a 6d 51 57 29 c9 1a b5 b9 3f>

Decapsulated Symmetric Key (ss2): <Buffer a6 5b 4a 08 2f 1a d3 8c c0 cf 6e c3 63 d9 f6 08 cc fe 77 0e 1e 39 8a 6d 51 57 29 c9 1a b5 b9 3f>

Key Generation Time: 21.036ms Encryption Time: 7.264ms Decryption Time: 14.267ms



Şekil 5. Kyber512 Test Çıktısı.

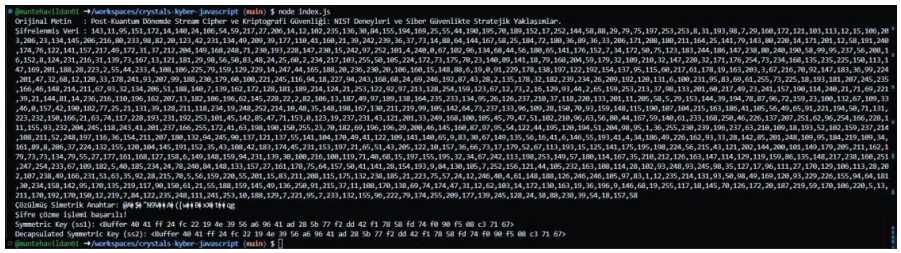
5.2.4.1.2 Kyber768 Testi

Symmetric Key (ss1): <Buffer 40 41 ff 24 fc 22 19 4e 39 56 a6 96 41 ad 28 5b 77 f2 dd 42 f1

78 58 fd 74 f0 90 f5 08 c3 71 67>

Decapsulated Symmetric Key (ss2): <Buffer 40 41 ff 24 fc 22 19 4e 39 56 a6 96 41 ad 28 5b

77 f2 dd 42 f1 78 58 fd 74 f0 90 f5 08 c3 71 67>

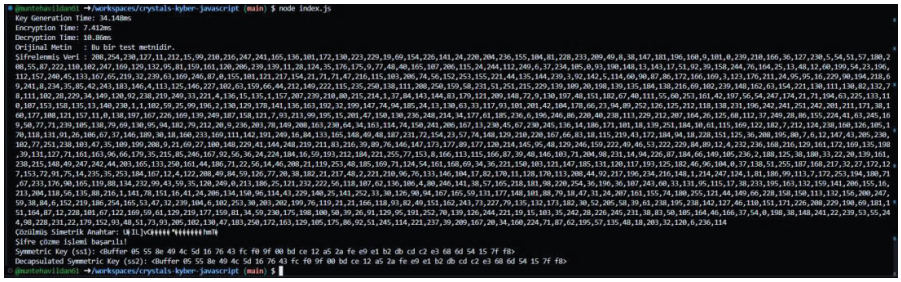


Şekil 6. Kyber768 Test Çıktısı.

Symmetric Key (ss1): <Buffer 05 55 8e 49 4c 5d 16 76 43 fc f0 9f 00 bd ce 12 a5 2a fe e9 e1 b2 db cd c2 e3 68 6d 54 15 7f f8>

Decapsulated Symmetric Key (ss2): <Buffer 05 55 8e 49 4c 5d 16 76 43 fc f0 9f 00 bd ce 12 a5 2a fe e9 e1 b2 db cd c2 e3 68 6d 54 15 7f f8>

Key Generation Time: 34.148ms Encryption Time: 7.412ms Decryption Time: 10.86ms



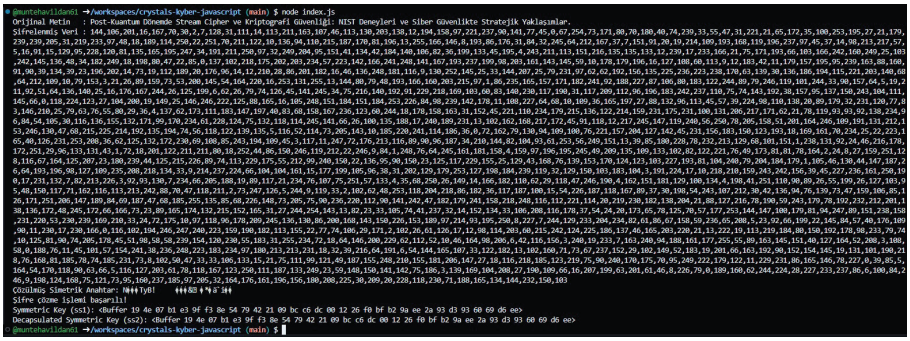
Şekil 7. Kyber768 Test Çıktısı.

5.2.4.1.3 Kyber1024 Testi

Symmetric Key (ss1): <Buffer 19 4e 07 b1 e3 9f f3 8e 54 79 42 21 09 bc c6 dc 00 12 26 f0 bf

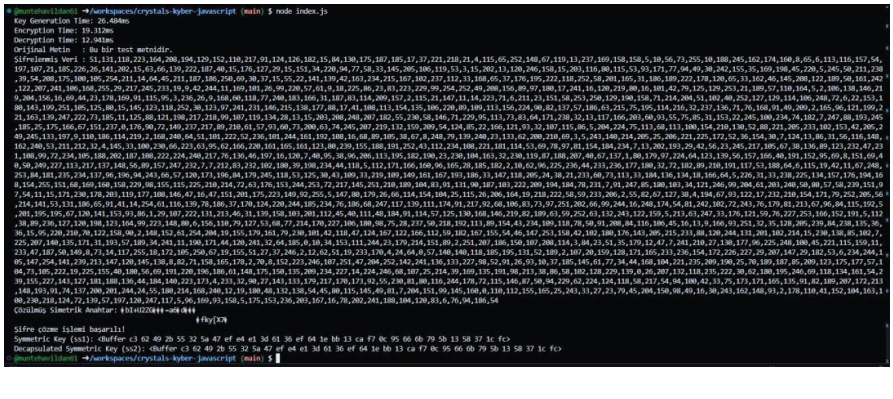
b2 9a ee 2a 93 d3 93 60 69 d6 ee>

Decapsulated Symmetric Key (ss2): <Buffer 19 4e 07 b1 e3 9f f3 8e 54 79 42 21 09 bc c6 dc
00 12 26 f0 bf b2 9a ee 2a 93 d3 93 60 69 d6 ee>



Şekil 8. Kyber1024 Test Çıktısı.

Symmetric Key (ss1): <Buffer c3 62 49 2b 55 32 5a 47 ef e4 e1 3d 61 36 ef 64 1e bb 13 ca f7
0c 95 66 6b 79 5b 13 58 37 1c fc>
Decapsulated Symmetric Key (ss2): <Buffer c3 62 49 2b 55 32 5a 47 ef e4 e1 3d 61 36 ef 64
1e bb 13 ca f7 0c 95 66 6b 79 5b 13 58 37 1c fc> Key Generation Time: 26.484ms
Encryption Time: 19.312ms Decryption Time: 12.941ms



Şekil 9. Kyber1024 Test Çıktısı.

5.2.4.2 Karşılaştırma

Anahtar boyu olarak farklılık gösterse de Kyber512, Kyber768 ve Kyber1024 için doğrulukları, anahtarların denk olduğu görülerek kanıtlanmıştır. Deney ortamında yapılan testler, CRYSTALS-Kyber algoritmasının doğruluğunu yüksek güvenle ortaya koymaktadır. Kyber, doğruluk ve performans açısından genelde en dengeli seçimdir. Bunun yanı sıra, testlerde elde edilen şifreleme süreleri (Encryption Time) ve şifre çözme süreleri (Decryption Time) parametre setleri arasında farklılık göstermiştir. Kyber512 ve Kyber768 için şifre çözme süreleri, şifreleme sürelerinden daha uzun bulunurken, Kyber1024 testinde durum tersine dönmüş ve şifreleme süresi daha fazla olmuştur. Bu farklılık, özellikle Kyber1024'teki daha büyük anahtar boyutunun şifreleme işlemlerinde ek matematiksel işlem yükü gerektirmesinden kaynaklanabilir. Kyber512 ve Kyber768, düşük kaynak tüketimi gerektiren uygulamalarda uygun bir çözüm sunarken, Kyber1024 yüksek güvenlik gerektiren senaryolarda daha uygun bir seçenek olarak öne çıkmaktadır. Bu bulgular, algoritmanın farklı güvenlik ve performans gereksinimlerini karşılayacak şekilde esneklik sunduğunu göstermektedir.

6. Araştırma Bulguları ve Tartışma

Bu bölümde, CRYSTALS-Kyber algoritması üzerinde yapılan testlerden elde edilen bulgular özetlenmekte ve tartışılmaktadır. Bulgular, algoritmanın doğruluğu, performansı ve post- kuantum güvenlik gereksinimlerini ne ölçüde karşılayabildiği üzerinde yoğunlaşmaktadır.

6.1 Doğruluk ve Güvenlik

CRYSTALS-Kyber algoritması, NIST tarafından sağlanan test vektörleriyle gerçekleştirilen doğrulama testlerinde %100 başarı göstermiştir. Test sonuçlarına göre Symmetric Key (ss1) ve Decapsulated Symmetric Key (ss2) değerleri, her bir parametre dizisi (Kyber512, Kyber768 ve Kyber1024) için birebir eşleşmiştir.

Bu sonuç, algoritmanın hem şifreleme hem de şifre çözme işlemlerini güvenilir bir şekilde gerçekleştirdiğini ve hatasız bir çalışma prensibine sahip olduğunu kanıtlamaktadır.

6.2 Performans Analizi

Şifreleme ve şifre çözme süreleri bakımından Kyber512, daha hafif bir güvenlik seviyesine sahip olduğu için en hızlı işlem süresini sunmuştur. Kyber768 ve Kyber1024 ise güvenlik seviyesine bağlı olarak daha fazla işlem gücü gerektirmiştir.

Anahtar boyutları bakımından Kyber512, 512-bit anahtar uzunluğuyla düşük kaynak tüketimi gerektiren uygulamalar için uygundur. Kyber1024 ise daha yüksek güvenlik gerektiren sistemlerde kullanılabilmektedir. Anahtar boyutları, depolama ve iletişim maliyetini arttırsa da güvenlik açısından kabul edilebilir düzeydedir.

6.3 Kyber Parametre Setleri Karşılaştırması

Tablo 2. Kyber parametre setlerinin karşılaştırması.

Parametre Dizisi	Güvenlik Seviyesi	Avantajlar	Dezavantajlar	Uygulama Alanı
Kyber512	Düşük güvenlik	Hafifliği ve hızlı işlem süresi, düşük güç tüketimi gereksinimlerini karşılar	Yüksek güvenlik gereksinimleri için uygun değildir	IoT cihazları, düşük güç tüketimi gerektiren uygulamalar
Kyber768	Orta düzey güvenlik	Güvenlik ve performans arasında iyi bir denge sağlar	Orta düzey güvenlik, kritik uygulamalar için yeterli olmayabilir	Genel güvenlik gereksinimleri, performans-fayda dengesi
Kyber1024	Yüksek güvenlik	En yüksek güvenlik seviyesi, kritik uygulamalar için ideal	Daha yüksek işlem süresi ve bellek kullanımı maliyeti	Finansal sistemler, kritik veri transferi uygulamaları

6.4 Kuantum Sonrası Güvenlik

CRYSTALS-Kyber algoritmasının kuantum sonrası güvenlik açısından etkinliği analiz edilmiştir. Algoritmanın matematiksel temeli, Hatalar ile Öğrenme (Learning With Errors - LWE) problemine dayanır ve bu problem hem klasik hem de kuantum bilgisayarlarla çözülmesi zor bir problem olarak kabul edilmektedir.

Kyber parametre setleri, kuantum bilgisayarların saldırılarına karşı dayanıklı olacak şekilde tasarlanmıştır. Özellikle, IND-CCA2 güvenlik seviyesi, algoritmanın kuantum sonrası güvenlik gereksinimlerini karşıladığını göstermektedir [24].

6.5 Crystals-Kyber ve Alternatif Algoritmalar

Kyber algoritmasının diğer post-kuantum kriptografi algoritmalarıyla karşılaştırıldığında, aşağıdaki avantajlara sahip olduğu gözlemlenmiştir: Kyber, performans açısından dengeli bir çözüm sunar. Özellikle Kyber512, hafif ve hızlı uygulamalar için ideal bir seçenektir. Kyber768 ve Kyber1024, yüksek güvenlik gereksinimlerini karşılarken performans-fayda dengesini korumaktadır. Farklı parametre setleri, çeşitli uygulama senaryolarına uyarlanabilmektedir.

6.6 Dezavantajlar ve İyileştirme Önerileri

Kafes tabanlı algoritmaların anahtar boyutları, klasik kriptografik sistemlere göre daha büyüktür. Bu durum, özellikle sınırlı depolama ve bant genişliği gerektiren uygulamalar için zorluk oluşturabilmektedir.

Daha yüksek güvenlik seviyelerine sahip parametre setleri (ör. Kyber1024), işlem süresi açısından daha fazla maliyet getirmektedir. Bu nedenle, belirli senaryolar için daha optimize edilmiş sürümler geliştirilmelidir.

6.7 Tartışma

CRYSTALS-Kyber algoritması, doğruluk ve güvenlik açısından yüksek bir performans sergilemiştir. Algoritmanın farklı parametre setlerinin, farklı güvenlik ve performans gereksinimlerine uygun olduğu görülmüştür. Özellikle, Kyber512'nin düşük işlem gücü gerektiren IoT cihazları gibi uygulamalarda uygun olduğu, Kyber1024'ün ise daha kritik güvenlik gereksinimlerini karşıladığı anlaşılmıştır.

Sonuç olarak, CRYSTALS-Kyber algoritmasının post-kuantum güvenlik ihtiyaçlarını karşılamada güçlü bir aday olduğu ve NIST'in standartlaştırma sürecinde haklı bir şekilde öne çıktığı kanıtlanmıştır. Ancak, daha geniş çaplı testler ve optimizasyon çalışmaları, algoritmanın uygulama alanlarını daha da genişletebilir ve performansını artırabilmektedir. Bu, özellikle kuantum sonrası dönemin güvenlik gereksinimlerine yanıt vermek açısından önemli bir adım olacaktır.

7. Kaotik Sistem: Lojistik Harita Akış Şifreleme

Kaotik harita (chaotic map), matematikte ve fiziksel sistemlerde kaos teorisi kapsamında incelenen bir kavramdır. Genellikle, başlangıç koşullarına çok duyarlı olan dinamik sistemleri tanımlamak için kullanılmaktadır. Kaotik haritalar, belirli bir başlangıç durumundan hareketle zamanla karmaşık ve öngörülemez davranışlar sergileyen sistemlerin matematiksel modelleridir. Kaos, sistemlerin uzun vadeli davranışlarının, başlangıç koşullarındaki çok küçük değişikliklere son derece hassas olduğu bir durumdur. Bu tür sistemler, belirli kurallara göre işler, ancak sonuçları öngörmek genellikle zordur. Kaotik haritalar bu tür sistemleri matematiksel olarak modellemek için kullanılır ve genellikle belirli kurallar ve denklem formülleri ile tanımlanmaktadır. Bu haritalar, deterministik olmasına rağmen, yani her bir girdiye karşılık bir çıkış olmasına rağmen, sonuçları kaotik ve öngörülemez olabilmektedir [25].

Deterministik Doğa: Kaotik sistemler tamamen deterministiktir; yani başlangıç koşulları sabit tutulursa sonuçlar tekrar edilebilmektedir.

Başlangıç Koşullarına Hassasiyet: Başlangıç değerlerindeki küçük bir değişiklik, tamamen farklı sonuçlara yol açabilmektedir (kelebek etkisi).

Periodiklik ve Karmaşıklık: Bazı kaotik haritalar belirli periyotlarda tekrar eden davranışlar gösterebilirken, bazıları tamamen karmaşık ve tekrar etmeyen yapıya sahiptir.

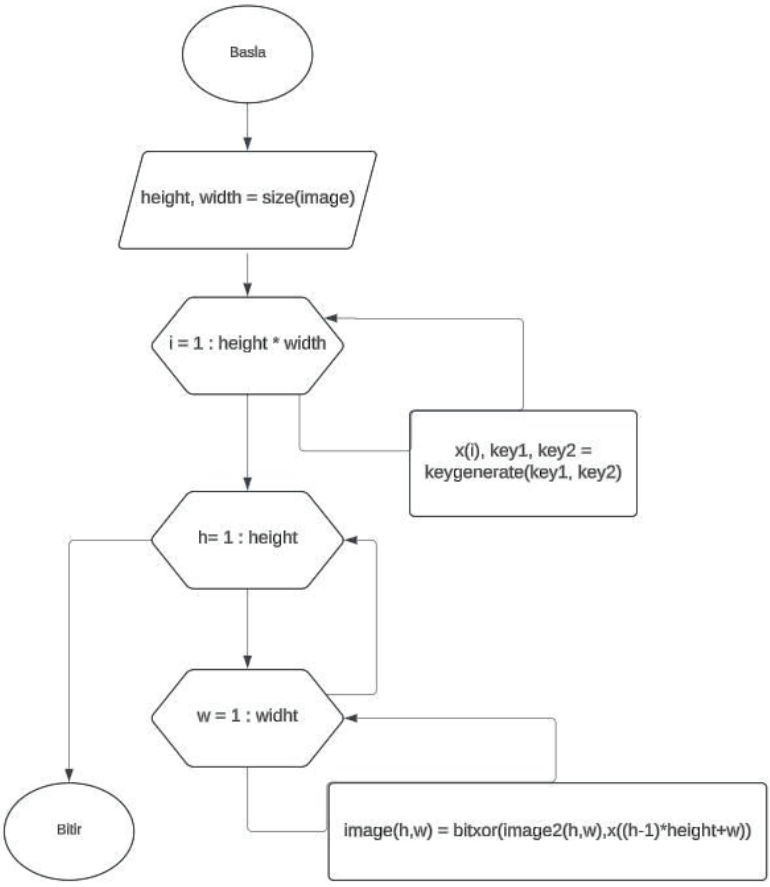
Bölünmüş Alan: Kaotik sistemlerde hareket, belirli bir faz uzayı içinde karmaşık yollar oluşturur ve zamanla tüm olası durumları kapsar.

7.1 Lojistik Harita (Logistic Map)

En yaygın kaotik haritalardan biridir. Bir popülasyon büyümesini modellemek için kullanılmaktadır. Denklem :

$$x_1 = x_0 * \lambda (1 - x_0) \quad (1)$$

Burada λ büyüme oranını temsil eder. x_0, bir sonraki adımın değerini belirlemek için kullanılan mevcut durumdur. λ belirli bir eşik değeri aştığında sistem kaotik davranış gösterir [26].



Şekil 10. Kaotik Şifre Oluşturma Akış Diyagramı [27].

Kaotik haritalar, şifreleme algoritmalarında rastgelelik ve karmaşıklık sağlamak için sıklıkla kullanılır:

Anahtar Üretimi: Kaotik haritalar, öngörülemeyen rastgele anahtarlar üretmek için kullanılır. Veri Şifreleme: Kaotik haritalar, veri bitlerini karıştırmak ve şifrelemek için uygulanabilir.

Görüntü Şifreleme: Görüntülerin piksellerini karıştırmak için kaotik sistemler kullanılabilir [28].

7.2 Anahtarda Lojistik Harita Uygulaması

CRYSTALS-Kyber algoritmasının testlerinden elde edilen Şekil 4 'te yer alan ss1 ve ss2 anahtarını baz alarak şifreleme uygulanacaktır.

Symmetric Key (ss1): <Buffer e8 f0 bc a0 37 f0 44 d1 e5 14 35 dc 34 6e d8 94 92 cf 8d d2 ed 3d bd 0d b3 89 8c b5 62 21 84 35> de bulunan rakamları bir araya getirerek ilk 15 tanesi ile kaotik hesaplamadaki x0 değeri elde edilip, sonraki 15 tane rakam ile de λ değeri elde edilecektir.

$$x0 = 0{,}800370441514353 \quad (2)$$

$$\lambda = 3{,}998949282303898 \quad (3)$$

Şimdi (2) ve (3) değerleri (1) numaralı formülüne uyarlanması:

$$x_1 = 0{,}800370441514353 * 3{,}998949282303898\ (1 - 0{,}800370441514353)$$

$$x_1 = 0.6385665061208377 \quad (4)$$

(4) değeri elde edilir. Bu elde edilen x değerlerini kullanarak anahtar oluşturulur.

$$Key_0 = (x_0 * 10\ \hat{}15) mod 256 \quad (5)$$

(5) denkleminde bulunan bütün x değerleri işleme alınır.

$$Key_0 = (0{,}800370441514353 * 10\hat{}15) mod 256$$

$$Key_0 = (800370441514353) mod 256$$

$$Key_0 = 113 \quad (6)$$

(6) de Key_0 değeri elde edilir. Sonrasında metin belirlenir ve işleme alınıp şifreli metin elde edilir.

"ISTANBUL TICARET UNIVERSITESI" metninin bütün harflerinin binary değerleri bulunur. Elde edilen bütün Key değerlerine binary değerleri ile XOR işlemi uygulanır.

"I" harfinin binary değeri = 01001001 (7)

113'in binary değeri = 01110001 (8)

(7) ve (8) binary değerleri XOR'lanır.

01110001 ⊕ 01001001 = 00111000 değeri elde edilir.

00111000_2 = 56 = 8 (9)

Artık (9) işleminin sonucunda "I" harfinin binary değerine karşılık gelen değer bulundu.

Şifreleme işlemi tamamlanmış oldu. Aynı şekilde bütün işlemler Key değerlerinin hepsine sırasıyla metnin bütün harflerine uyarlanıp şifreleme işlemi gerçekleştirilir.

Şifrelenmiş metin : "8FÿZªMÇ ¼¥á d¿öÖfBÛê r²ÄYnÎƒÿ" şeklinde elde edilir.

Şifreleme işleminden sonra metnin doğru çıktığını teyit etmek için deşifreleme işlemi yapılır. İlk etapta elde edilen şifrelenmiş metnin ilk harfinin ASCII değeri alınır.

"8" ASCII değeri = 56 (10)

(2) ve (3)' de bulunan değerler işleme alınıp Key0 değeri bulunur.

$$Key_0 = (0{,}800370441514353 * 10\text{^}15) mod 256 \quad (11)$$

$$Key_0 = 113 \quad (12)$$

(12) sonucu elde edilir.

(10) ve (12)'de elde edilen değerlerin binary karşılıkları bulunur.

56 = 00111000 ve 113 = 01110001 değerlerine XOR işlemi uygulanır.

00111000 ⊕ 01110001 = 01001001 (13) sonucuna ulaşılmış olunur.

01001001 binarynin ASCII karşılığı 73 çıkar ve 73 ASCII'nin karşılığı da "I" harfine yani metnin ilk harfine denktir. Böylelikle deşifreleme işleminin doğru bir şekilde çalıştığı görülmüştür. Sırasıyla bütün işlemler uygulandığında "ISTANBUL TICARET UNIVERSITESI" metnine ulaşılmış olunur.

8. Sonuç ve Öneriler

Bu çalışmada, NIST'in post-kuantum kriptografi standartlaştırma sürecinde öne çıkan bir kafes tabanlı algoritma olarak ele alınmış ve kapsamlı bir şekilde incelenmiştir. Yapılan testler ve analizler sonucunda, Kyber algoritmasının güvenlik ve doğruluk açısından yüksek performans sergilediği görülmüştür. Simetrik anahtar doğruluğu testlerinde %100 eşleşme sağlanarak algoritmanın güvenilirliği kanıtlanmıştır.

Algoritmanın matematiksel temeli olan Hatalar ile Öğrenme (Learning With Errors - LWE) problemi, kuantum bilgisayarların çözmesi zor bir yapı olarak öne çıkmaktadır. Algoritmanın IND-CPA ve IND-CCA2 güvenlik seviyelerini başarıyla sağlaması, post-kuantum güvenlik standartlarına uygunluğunu kanıtlamaktadır.

Performans açısından değerlendirmek istersek Kyber parametre setlerinin (Kyber512, Kyber768, Kyber1024) farklı güvenlik ve performans gereksinimlerine uyum sağladığı görülmüştür. Kyber512**,** düşük kaynak tüketimi gerektiren uygulamalarda uygun bir seçenek sunarken, Kyber1024 en yüksek güvenlik seviyesini gerektiren senaryolarda güvenilir bir çözüm sunmaktadır. Şifreleme ve deşifreleme süreleri açısından Kyber algoritmasının, diğer kafes tabanlı algoritmalara kıyasla dengeli bir performans gösterdiği anlaşılmıştır.

Kyber algoritması, post-kuantum güvenlikte önemli bir rol oynamakta olup, kuantum sonrası dönemde güvenlik ihtiyaçlarını karşılayacak potansiyele sahiptir. NIST'in standartlaştırma sürecindeki diğer algoritmalarla birlikte, dijital imza, anahtar değişimi ve veri şifreleme gibi kritik uygulamalarda geniş bir kullanım alanı bulabileceği öngörülmektedir.

Kyber algoritmasının anahtar boyutları, klasik sistemlere göre oldukça büyük olduğundan, özellikle düşük depolama kapasitesine sahip cihazlar için daha optimize sürümler geliştirilmelidir. Hafif versiyonların oluşturulması, IoT cihazları gibi düşük işlem gücüne sahip sistemlerde kullanım potansiyelini artıracaktır.

Kyber algoritmasının, finansal sistemler, bulut bilişim ve IoT güvenliği gibi farklı alanlardaki uygulanabilirliği daha geniş çaplı testlerle değerlendirilmelidir. Özellikle veri transfer hızının kritik olduğu uygulamalarda, Kyber algoritmasının performansı artırılabilir.

Algoritmanın farklı güvenlik senaryolarında (ör. saldırı simülasyonları) uzun vadeli testlerle değerlendirilmesi gerekmektedir. Kuantum bilgisayarların daha ileri seviyelere ulaşması durumunda algoritmanın güvenlik seviyesini koruyup koruyamayacağına dair simülasyonlar yapılmalıdır.

Standartların uygulanması NIST tarafından belirlenen post-kuantum güvenlik standartlarının farklı sektörlerde uygulanabilirliğini artırmak için eğitim ve farkındalık çalışmaları yapılmalıdır. Özellikle kritik altyapıların ve kamu kuruluşlarının, post-kuantum güvenlik standartlarına uyum sağlaması için teşvik edilmesi gerekmektedir.

Gelecekteki yapılacak çalışmalarda da Kyber algoritması üzerinde yapılacak yeni çalışmalar, hem matematiksel yapısının daha verimli hale getirilmesine hem de performans-fayda dengesinin daha iyi optimize edilmesine odaklanmalıdır. Diğer kafes tabanlı algoritmalarla yapılan karşılaştırmalı çalışmalar, post-kuantum güvenlik ekosistemini zenginleştirebilir.

Kyber algoritmasının test sonuçları, bu algoritmanın post-kuantum dönemin güvenlik ihtiyaçlarını karşılamada güçlü bir aday olduğunu göstermektedir. Gerek performans gerekse güvenlik açısından elde edilen bulgular, bu algoritmanın gelecekteki standartlar ve uygulamalar için kritik bir bileşen olabileceğini işaret etmektedir. Ancak, algoritmanın belirli alanlarda optimize edilmesi ve geniş çaplı uygulamalarda test edilmesi, potansiyelini tam anlamıyla ortaya koymak açısından önemlidir.

Bu çalışmada yapılan kaotik map uygulaması, CRYSTALS-Kyber algoritmasının performansını ve güvenlik seviyesini artırmada önemli bir role sahiptir. Kaotik map'lerden türetilen anahtarlar, algoritmanın şifreleme ve şifre çözme süreçlerinde başarıyla uygulanmış ve kaotik map'lerden türetilen anahtarlar, algoritmanın rastgelelik ve karmaşıklık gereksinimlerini karşılamış, şifreleme sürecinde güçlü bir güvenlik sağlamıştır. Logistic map formülüne dayalı anahtar üretim yöntemi, algoritmanın farklı güvenlik seviyelerinde test edilmesine olanak tanımış ve hem Symmetric Key (ss1**)** hem de Decapsulated Symmetric Key (ss2) değerleriyle başarılı bir şekilde entegre edilmiştir. Test sonuçlarında, kaotik harita uygulaması sayesinde elde edilen anahtarların, CRYSTALS-Kyber algoritmasının doğruluk ve performansında başarılı sonuçlar alındığı görülmüştür.

Bu bağlamda, kaotik map'in güvenlik ve performans üzerindeki etkisi, algoritmanın gelecekteki uygulama potansiyelini artıran önemli bir yenilik olarak değerlendirilebilir.

Teşekkür

Bu araştırma için beni yönlendiren, karşılaştığım zorlukları bilgi ve tecrübesi ile aşmamda yardımcı olan değerli Hocam Doç. Dr. Mustafa Cem KASAPBAŞI'na teşekkürlerimi sunarım.

Bu çalışmanın tamamlanmasında desteğini ve yardımlarını gördüğüm Burak SARAL'a teşekkür ederim.

Referanslar

[1] Avanzi, R., Bos, J., Ducas, L., Kiltz, E., Lepoint, T., Lyubashevsky, V., Schanck, J. M., Schwabe, P., Seiler, G. ve Stehlé, D., CRYSTALS-Kyber Algorithm Specifications And Supporting Documentation, 2017.

[2] Ocak, D. M., Kuantum Bilgisayarlar Çağında Kriptografi, 2020.

[3] Bavdekar, R. ve Jozsa, E., Post Quantum Cryptography: Techniques, Challenges, Standardization, and Directions for Future Research, 2022.

[4] Çelik, S. Kuantum Kriptolojisi ve Siber Güvenlik, 14(1), 2021.

[5] Shor, P. W. Algorithms for Quantum Computation, 35th Annual Symposium on Foundations of Computer Science (FOCS), 1994.

[6] Niederhagen, R. Practical Post-Quantum, Fraunhofer Institute for Secure Information Technology (Fraunhofer SIT), 2024.

[7] Grover, L. K. A Fast Quantum Mechanical Algorithm for Database Search, Proceedings of the Twenty- Eighth Annual ACM Symposium on Theory of Computing (STOC), ACM, 1996.

[8] Jozsa, R., Quantum Factoring, Discrete Logarithms, and the Hidden Subgroup Problem, 2001.

[9] Bernstein, D. J., Post-Quantum Cryptography, 2017.

[10] Abiade, O., The Impact of Quantum Computing on RSA and ECC Algorithms, EasyChair, 2024.

[11] Chandra, S., Bhattacharyya, S., Paira, S. ve Alam, S. S., A Study and Analysis on Symmetric Cryptography, IEEE, 2017.

[12] Hasija, T., Ramkumar, K., Singh, B., Kaur, A., Mittal, S. K., Jhanda, K. ve Kaiserslautern, S., Symmetric Key Cryptography: Review, Algorithmic Insights, and Applications, Chitkara University Research and Innovation Network (CURIN), 2023.

[13] Chi, D. P., Choi, J. W., Kim, J. S. ve Kim, T., Lattice-Based Cryptography for Beginners, IACR Cryptology ePrint Archive, 2015.

[14] Fischer, S., Analysis of Lightweight Stream Ciphers, 2008.

[15] Garipcan, A. M., Erdem, E. ve Tuncer, T., Donanım Tabanlı Trivium Akış Şifreleme Algoritmasının FPGA Ortamında Gerçekleştirilmesi, 29(2), 2017.

[16] Aghayev, M., Kriptoloji ve Veri Şifreleme Teknikleri Üzerine, Yök Açık Bilim/ Ege Üniversitesi, 2017.

[17] Yerlikaya, T., Yeni Şifreleme Algoritmalarının Analizi, Trakya Üniversitesi / Fen Bilimleri Enstitüsü, 2006.

[18] «Veri Şifreleme: Nasıl çalışır, neden ihtiyacınız var?», (Erişildi: 12 2024).

[19] Eduard, S., Post-Quantum Cryptography: Lattice-based Encryption, 2016.

[20] «https://www.nist.gov/news-events/news/2024/08/nist-releases-first-3-finalized-post-quantum-encryption-standards», (Erişildi: 12 2024).

[21] Bos, J., Ducas, L., Kiltz, E., Lepoint, T., Lyubashevsky, V., Schanck, J. M., Schwabe, P., Seiler, G. ve Stehlé, D., CRYSTALS – Kyber: A CCA-secure module-lattice-based KEM, 2017.

[22] «https://pq-crystals.org/kyber/software.shtml», (Erişildi: 12 2024).

[23] Zeng, P., Chen, S. ve Choo, K.-K. R., An IND-CCA2 Secure Post-Quantum Encryption Scheme and a Secure Cloud Storage Use Case, 9(32), 2019.

[24] Bernstein, D. J., Chuengsatiansup, C., Lange, T. ve v. Vredendaal, C., NTRU Prime: Reducing Attack Surface at Low Cost, 2017.

[25] Çıraklı, Y. D. D. Ü., Dalkılıç, A. G. S. ve Hacıhasanoğlu, D. D. T., Kaos Teorisi, Karmaşık Teorisi, Karmaşık Uyarlamalı Sistemler: Sağlık Hizmetleri Açısından Bir Derleme, International Journal of Academic Value Studies, pp. 330-343, 2017.

[26] Aydın, Y. ve Özkaynak, F., Kaotik Sistemler Tabanlı Kriptografik Tasarımlar İçin Bir Analiz Aracı, Turkish Journal of Science and Technology, 18(2), pp. 387-395, 2023.

[27] Seval, G. ve Kasapbaşı, M. C., Görüntüler İçin Kaotik Şifreleme Sistemi ve Performans Analizi, Avrupa Bilim ve Teknoloji Dergisi, no. 44, pp. 13-20, 2022.

[28] Tuna, M. ve Fidan, C. B., A Study on the Importance of Chaotic Oscillators Based on FPGA for True Random Number Generating (TRNG) and Chaotic Systems, Gazi Üniversitesi Mühendislik Mimarlık Fakültesi Dergisi, pp. 473-491, 2018.