POST-KUANTUM KRİPTOGRAFİ VE GELECEĞİN GÜVENLİK STANDARTLARI

Yazılım Mühendisliği Ana Bilim Dalı
Bitirme Projesi

Arif Özel

Proje Danışmanı: Dr. Öğr. Üyesi Mansur Alp Toçoğlu

Ocak 2024

POST-KUANTUM KRİPTOGRAFİ VE GELECEĞİN GÜVENLİK STANDARTLARI

Yazılım Mühendisliği Ana Bilim Dalı
Bitirme Projesi

Arif Özel

Proje Danışmanı: Dr. Öğr. Üyesi Mansur Alp Toçoğlu

Ocak 2024

POST-KUANTUM KRİPTOGRAFİ VE GELECEĞİN GÜVENLİK STANDARTLARI

Öz

Bu araştırma projesi, kuantum bilgisayarların geleneksel kriptografiyi tehdit etmesi ihtimalini göz önünde bulundurularak, post-kuantum kriptografinin önemini ele alıyor. Post-kuantum kriptografi, temelde kuantum bilgisayar saldırılarına karşı dirençli kriptografik algoritmalar geliştirmeyi amaçlamaktadır. Bu çalışmada, bu yeni nesil algoritmaların temel matematiksel prensiplerini inceleyerek, mevcut güvenlik standartlarının evrileceği yol araştırılacak. Ayrıca, post-kuantum kriptografinin uygulamaları ve gelecekteki bilgi güvenliği standartlarına olan etkileri üzerinde durulacaktır. Son olarak, bilgi güvenliği alanında yeni bir çağın kapılarını aralayarak, geleceğin kriptografik güvenlik standartlarına ışık tutmayı amaçlamaktadır.

Anahtar Sözcükler: *Kuantum bilgisayar, Post – Kuantum Kriptograf, Bilgi Güvenliği*

POST-QUANTUM CRYPTOGRAPHY AND FUTURE SECURITY STANDARDS

Abstract

This research project addresses the importance of post-quantum cryptography, considering the possibility that quantum computers may threaten traditional cryptography. Post-quantum cryptography essentially aims to develop cryptographic algorithms that are resistant to quantum computer attacks. In this study, the way in which current security standards will evolve will be investigated by examining the basic mathematical principles of these new generation algorithms. Additionally, the applications of post-quantum cryptography and its implications for future information security standards will be emphasized. Finally, it aims to shed light on the cryptographic security standards of the future, opening the doors to a new era in the field of information security.

Key Words: *Quantum computer, Post – Quantum Cryptography, Information Security*

Bu proje çalışmamı, eğitim hayatım boyunca benden hiçbir desteğini esirgemeyen ve her daim yanımda olan sevgili annem ve babama ithaf ediyorum.

Teşekkür

Yazılımı bana sevdiren, öğretmekten kaçınmayan tüm hocalarıma ve özellikle proje danışmanım Dr. Öğr. Üyesi Mansur Alp Toçoğlu'na ayrıca teşekkür ederim.

İÇİNDEKİLER

GİRİŞ

Dijital dünyada hızla ilerleyen teknoloji, yeni olanaklar sunarken aynı zamanda güvenlik tehditlerini de beraberinde getiriyor. Bu tehditlerden biri de geleneksel kriptografinin kuantum bilgisayarlar karşısında güvenliğini kaybetme riskidir. Kuantum bilgisayarlar, klasik bilgisayarların çözemeyeceği matematiksel problemleri anında çözebilme potansiyeline sahiptir. Bu durum, şu anda kullanılan şifreleme algoritmalarının gelecekte çözülebileceği endişelerini doğuruyor. Ancak umutsuzluğa kapılmaya gerek yok; çünkü post-kuantum kriptografi, bu yeni tehditlere karşı koymak ve gelecekteki güvenlik standartlarını belirlemek üzere bir çıkış kapısı sunuyor. Bu makalede, post-kuantum kriptografisinin temel prensiplerini, kullanılan algoritmaları ve gelecekteki güvenlik standartlarını anlamaya odaklanacağız.

Makalemizin başlangıcında, kuantum bilgisayarların güvenlik paradigmasını nasıl değiştirebileceğini anlamak için kısaca kuantum bilgisayarlar ve geleneksel kriptografi arasındaki temel farklara göz atacağız. Ardından, post-kuantum kriptografisinin ortaya çıkışını ve temel ilkelerini keşfedeceğiz. Bu yeni nesil kriptografinin, geleceğin güvenlik standartlarını belirleme sürecinde nasıl bir rol oynadığını ve mevcut şifreleme yöntemlerine nasıl bir çözüm sunduğunu ele alacağız.

Gelgelelim, post-kuantum kriptografisinin önümüzdeki dönemde ne gibi zorluklarla karşılaşacağını ve bu yeni güvenlik standartlarının nasıl benimsenebileceğini de değerlendireceğiz. Bu yazı, dijital dünyada güvenlik konusunda bir devrimin eşiğinde olduğumuz gerçeğini gözler önüne sermek ve bu değişime hazırlıklı olmak isteyen herkes için bir rehber niteliği taşıyacak.

Son olarak, post-kuantum kriptografisinin, günümüzün karmaşık güvenlik sorunlarına nasıl bir çözüm sunabileceğini ve dijital dünyamızı daha güvenli bir geleceğe nasıl taşıyabileceğini inceleyeceğiz. Geleneksel kriptografinin temelleri, sayı teorisi, cebirsel yapılar ve hesaplamalı matematik gibi alanlara dayanır. Ancak, kuantum bilgisayar teknolojisinin yükselişi ile bu temeller sarsılmış durumda. Kuantum bilgisayarlar, çoğu geleneksel kriptografik algoritmayı etkisiz hale getirme potansiyeline sahiptir. Bu bağlamda, post-kuantum kriptografisi, geleceğin güvenlik standartlarını belirlemede kritik bir rol oynamaktadır. Post-kuantum kriptografisi, kuantum bilgisayarların potansiyel tehdidine karşı dayanıklı olacak şekilde tasarlanmış kriptografik algoritmaların geliştirilmesini amaçlar. Bu algoritmalar, sayı teorisi temelli olup, büyük sayıların faktörizasyonu ve diskret logaritma problemleri gibi zorlu matematiksel problemlere dayanır. Mevcut güvenlik standartları, kuantum bilgisayarlarla başa çıkmak için yetersiz kalabilir. Bu nedenle, post-kuantum kriptografisi, gelecekteki bilgi güvenliğini sağlamak için kritik bir öneme sahiptir. Bu alandaki çalışmalar, bilgi güvenliği uzmanları, matematikçiler ve kriptografi araştırmacıları arasında hızla artmaktadır.

Post-kuantum kriptografisinin temel ilkelerini anlamak, geleceğin güvenlik standartlarını belirlemede önemlidir. Bu alanda yapılan araştırmalar, geleneksel kriptografinin sınırlarını aşarak, bilgi güvenliği alanında yeni ufuklar açmaktadır. Kuantum bilgisayarlarla başa çıkmak için tasarlanan post-kuantum kriptografisi, geleceğin bilgi güvenliği standartlarının temelini oluşturacaktır. Post-kuantum kriptografisinin temel ilkeleri, sayı teorisi, cebirsel yapılar ve matematiksel problemler üzerine kurulu bir zeminde yükselir. Bu algoritmalar, büyük sayıları asal çarpanlarına ayırma veya diskret logaritma problemlerini çözme gibi zor problemlerin üstesinden gelebilirler. Bu, geleneksel kriptografinin dayandığı matematiksel güvenliği daha da ileri taşıyarak, geleceğin güvenlik ihtiyaçlarına cevap verir.
Kuantum bilgisayarlar, kuantum bitlerinin süperpozisyonunu ve kuantum dolanıklığını kullanarak belirli matematiksel problemleri çözme potansiyeline sahiptir. Bu, geleneksel kriptografinin temelini oluşturan sayı teorisi ve cebirsel yapıların güvenliklerini sorgulatır. Ancak, post-kuantum kriptografisi, bu tehdide karşı dayanıklı matematiksel algoritmalar geliştirerek bilgi güvenliğini sağlamak için önemli bir adımdır.
Bu alanda yapılan araştırmalar, post-kuantum kriptografisinin sadece teorik bir kavram olmadığını, aynı zamanda pratik uygulamalara da evrildiğini göstermektedir. Çeşitli kriptografik algoritmalar, güçlü matematiksel temellere dayanarak geliştirilmekte ve mevcut güvenlik standartlarına meydan okumaktadır.

Sonuç olarak, post-kuantum kriptografisi, kuantum bilgisayarlarının potansiyel tehdidine karşı bilgi güvenliğini sağlamak için kritik bir öneme sahiptir. Temel matematiksel ilkeleriyle bu algoritmalar, geleceğin güvenlik standartlarını belirleyen önemli bir faktördür. Bu nedenle, post-kuantum kriptografisinin geliştirilmesi ve uygulanması, bilgi güvenliği alanında önemli bir adımdır.

1. Post-Kuantum Kriptografi: Temel İlkeler ve Algoritmalar

Post- Kuantum Kriptografi'den bahsetmeden önce kriptografiden ve tarihinden bahsedecek olursak; kriptografi, bilgilerin güvenliğini sağlama amacıyla kullanılan bir disiplindir ve tarihi oldukça eski dönemlere uzanır. İnsanlar, iletişimlerini ve bilgilerini korumak amacıyla çeşitli yöntemlere başvurmuşlardır. Antik dönemde, Mısırlılar ve Romalılar gibi medeniyetler, basit şifreleme teknikleri kullanarak gizli iletişim sağlamışlardır. Sezar Şifrelemesi gibi temel yöntemler, bu dönemde yaygın olarak kullanılmıştır. Orta Çağ boyunca, özellikle askeri iletişimde, şövalyeler ve kraliyet aileleri arasında şifreleme yöntemleri önem kazanmıştır. Rönesans döneminde ise matematikçiler ve filozoflar, kriptoanaliz konusunda katkılarda bulunarak şifreleme yöntemlerini geliştirmişlerdir. Eski yıllarda, şifreleme yöntemleri daha karmaşık hale gelmiştir. Ancak bu dönemde, bilgisayar teknolojisi henüz gelişmediği için şifreleme ve deşifreleme genellikle manuel olarak gerçekleştirilmekteydi. Bilgisayarların ortaya çıkmasıyla birlikte şifreleme alanında büyük ilerlemeler kaydedildi. İkinci Dünya Savaşı'nda kullanılan Enigma makinesi gibi gelişmiş şifreleme sistemleri, dönemin önemli gelişmelerindendi. Günümüzde, dijital iletişimin yaygınlaşmasıyla birlikte kriptografi, özellikle internet üzerinde güvenli iletişimi sağlamak adına önemli bir role sahiptir. Açık anahtarlı şifreleme gibi modern kriptografi yöntemleri, dijital dünyada

gizlilik ve güvenliği artırmak için kullanılmaktadır. Elektronik ticaret, online bankacılık ve diğer birçok uygulama, kriptografinin temel prensiplerine dayanmaktadır.

Post-kuantum kriptografi, kuantum bilgisayarların geleneksel kriptografik algoritmaları
kırabileceği varsayımına dayanan bir kriptografi dalıdır. Post-kuantum kriptografi, kuantum hesaplama gücüne dayanıklı yeni algoritmalar geliştirmeyi amaçlar. Bu algoritmalar, kuantum bilgisayarların çözemediği veya zorlandığı matematiksel problemlere dayanır. Örneğin, çok büyük sayıların asal çarpanlarına ayrılması, eliptik eğriler üzerinde işlem yapılması veya çok boyutlu ızgaralar üzerinde hesaplanması gibi problemler.

Post-kuantum kriptografi, simetrik ve asimetrik anahtarlı kriptografi olmak üzere iki ana kategoriye ayrılabilir. Simetrik anahtarlı kriptografi, aynı anahtarın hem şifreleme hem de çözümleme işlemlerinde kullanıldığı bir yöntemdir. AES gibi algoritmalar, kuantum bilgisayarlar tarafından kırılamaz, ancak anahtar uzunluğunun iki katına çıkarılması gerekir. Asimetrik anahtarlı kriptografi, farklı anahtarlar kullanılarak şifreleme ve çözümleme işlemleri gerçekleştirilen bir yöntemdir. RSA ve ECC gibi algoritmalar, kuantum bilgisayarlar tarafından kırılabilir, bu yüzden post-kuantum kriptografi, bu algoritmaların yerine kullanılabilecek yeni algoritmalar aramaktadır. Post-kuantum kriptografi, gelecekteki kuantum tehdidine karşı kuruluşların ve bireylerin verilerini korumak için önemli bir araştırma alanıdır. Post-kuantum kriptografi, kuantum bilgisayarların henüz yaygın olmadığı bir dönemde geliştirilmektedir, bu da algoritmaların test edilmesi ve güvenilirliğinin kanıtlanması için zaman tanımaktadır. Post-kuantum kriptografi, kuantum bilgisayarların gelişimine paralel olarak ilerlemeli ve kuantum sonrası bir dünyaya hazırlanmalıdır.

1.1 Tanım

Post-Kuantum Kriptografi, geleneksel kriptografi sistemlerinin kuantum bilgisayarlar tarafından çözülebilme ihtimali göz önünde bulundurularak ortaya çıkan bir kriptografik alanı ifade eder. Kuantum bilgisayarlar, klasik bilgisayarlara göre bazı matematiksel problemleri çözmekte çok daha hızlı olabilirler, bu da mevcut kriptografik algoritmaların güvenliğini sorgulamak için bir neden oluşturur.
Post-Kuantum Kriptografisi, kuantum bilgisayar saldırılarına karşı dayanıklı olacak şekilde tasarlanmış kriptografik algoritmaların geliştirilmesi amacını taşır. Bu algoritmalar, sayı teorisi, cebirsel geometri, hatta girdiği alanlarda zor problemlere dayanarak güvenliklerini temin eder. Örneğin, büyük sayıların asal çarpanlarına ayrılması veya diskret logaritma gibi matematiksel problemler, post-kuantum kriptografinin temelini oluşturur.
Post-Kuantum Kriptografisi, mevcut güvenlik standartlarının kuantum bilgisayar saldırılarına karşı yetersiz kalabileceği endişesiyle doğmuştur. Bu nedenle, gelecekteki bilgi güvenliğini sağlamak için kritik bir rol oynar. Mevcut kriptografik algoritmaların güvenilirliği, bu yeni çağın teknolojik gelişmelerine dayanıklı olup olmadıkları açısından sorgulanır hale gelmiştir.
Bu bağlamda, post-kuantum kriptografisi alanındaki çalışmalar, geleneksel kriptografinin sınırlarını aşarak, bilgi güvenliği alanında yeni bir dönemin kapılarını

aralamaktadır. Kuantum bilgisayarların yükselen etkilerine karşı geliştirilen bu algoritmalar, geleceğin bilgi güvenliği standartlarının temelini oluşturacaktır. Post-Kuantum Kriptografisi, kriptografik dünyanın geleceğini şekillendiren bir önem taşımaktadır ve bu alandaki çalışmalar, bilgi güvenliği uzmanları ve matematikçiler için vazgeçilmezdir.

1.2 Klasik Kriptografi ve Kuantum Bilgisayar Tehdidi

Klasik kriptografi ve kuantum bilgisayar tehdidi, bilgi güvenliği alanında önemli bir konudur.
Klasik kriptografi, geleneksel bilgisayarlar ve matematiksel algoritmalar kullanarak bilgiyi şifreleme ve çözme işlemlerini inceleyen bir alandır. Temel olarak, bu yaklaşım, sayı teorisi ve matematiksel işlemler üzerine kuruludur. Klasik kriptografinin temel amacı, bilgiyi güvenli bir şekilde iletmek veya saklamaktır.
Örneğin, RSA ve ECC gibi klasik kriptografik algoritmalar, büyük sayıların faktörizasyonu veya eliptik eğriler üzerinde işlemler yaparak bilgiyi şifreler. Bu algoritmalar, geleneksel bilgisayarlar için zor problemler oluşturur ve bilgiyi korur.
Kuantum bilgisayarlar, geleneksel bilgisayarlara göre belirli matematiksel problemleri çok daha hızlı çözebilme yeteneğine sahiptir. Özellikle, Shor'un algoritması gibi kuantum algoritmaları, RSA ve ECC gibi klasik kriptografik algoritmaların temelini oluşturan sayı teorisi problemlerini çözmekte oldukça etkilidir. Bu durum, kuantum bilgisayarların mevcut kriptografik standartları zayıflatabileceği veya çözebileceği anlamına gelir. Bu nedenle, bilgi güvenliği alanında kuantum bilgisayarların yükselişiyle birlikte, post-kuantum kriptografisi adı verilen yeni bir alanın doğması kaçınılmaz hale gelmiştir.
Post-kuantum kriptografisi, kuantum bilgisayar tehdidine karşı dayanıklı olacak şekilde tasarlanmış yeni kriptografik algoritmalar geliştirmeyi amaçlar. Bu algoritmalar, geleneksel kriptografinin temelini oluşturan matematiksel problemlere dayanarak güvenliklerini sağlar.
Sonuç olarak, klasik kriptografi ve kuantum bilgisayar tehdidi, bilgi güvenliği alanında bir dönüm noktasını temsil ediyor. Kuantum bilgisayarların yükselmesiyle birlikte, post-kuantum kriptografisi alanındaki çalışmalar, bilgi güvenliğini sağlamak için kritik bir öneme sahip olmuştur. Bu iki alanın etkileşimi, geleceğin bilgi güvenliği standartlarının belirlenmesinde belirleyici bir rol oynayacaktır.

Kuantum bilgisayarlar, klasik bilgisayarların aksine kubitler adı verilen kuantum bitlerini kullanırlar. Bu kubitler, aynı anda birden çok durumda olabilirler (süperpozisyon) ve birbirleriyle dolanıklık (entanglement) oluşturabilirler. Bu özellikler, kuantum bilgisayarların belirli matematiksel problemleri çözme potansiyelini artırır. Özellikle, Shor'un algoritması gibi kuantum algoritmaları, büyük sayıların faktörizasyonu ve eliptik eğriler üzerindeki diskret logaritma problemlerini çözmekte geleneksel bilgisayarlardan çok daha hızlıdır.
Bu kuantum bilgisayar tehdidi, mevcut güvenlik standartlarını sarsmış durumda. Özellikle, RSA ve ECC gibi klasik kriptografik algoritmalar, bu kuantum algoritmaları karşısında zayıf kalabilirler. Büyük asal sayıların faktörizasyonu veya eliptik eğriler

üzerindeki diskret logaritma problemlerini çözmek, kuantum bilgisayarlar için görece kolaydır.
Post-kuantum kriptografisi, bu tehdide karşı bir çözüm olarak ortaya çıkar. Bu alandaki araştırmalar, kuantum bilgisayar tehdidine dayanıklı olacak şekilde tasarlanmış kriptografik algoritmalar geliştirmeyi amaçlar. Bu algoritmalar, sayı teorisi ve cebirsel yapılar gibi matematiksel problemlere dayanarak güvenliklerini temin ederler.
Mevcut kriptografik standartların post-kuantum dünyasında yetersiz kalabileceği düşünüldüğünde, bu yeni algoritmalara olan ihtiyaç açıktır. Post-kuantum kriptografisi, geleceğin bilgi güvenliği için temel bir taş olacaktır. Bu nedenle, bu alandaki çalışmalar ve gelişmeler, bilgi güvenliği uzmanları ve matematikçiler için son derece önemlidir.
Klasik kriptografi ve kuantum bilgisayar tehdidi arasındaki bu etkileşim, bilgi güvenliği alanında yeni bir dönemin başlangıcını işaret ediyor. Post-kuantum kriptografisi, geleceğin bilgi güvenliği standartlarının belirlenmesinde hayati bir rol oynayacak ve bu alandaki çalışmalar, bilgi güvenliği alanında bir dönüm noktası oluşturacaktır.

1.3 Asimetrik Kriptografi ve Kriptografik Algoritmalar

Asimetrik kriptografi, şifreleme ve şifre çözme işlemlerinde farklı anahtarların kullanıldığı bir kriptografi türüdür. Bu anahtarlar birbirleriyle matematiksel olarak ilişkilidir ve biri özel anahtar, diğeri ise açık anahtar olarak adlandırılır. Özel anahtar, sahibi tarafından gizli tutulur ve şifreli mesajları çözmek için kullanılır. Açık anahtar ise herkese açık olarak paylaşılır ve mesajları şifrelemek için kullanılır. Bu sayede, şifreleme yapan kişi, alıcının açık anahtarını kullanarak mesajı şifreler ve sadece alıcının özel anahtarına sahip olduğu için şifreyi çözebilir. Bu yöntem, şifreleme anahtarını güvenli bir şekilde paylaşma sorununu ortadan kaldırır ve gizlilik, kimlik doğrulama, veri bütünlüğü gibi bilgi güvenliği hizmetleri sağlar.
Kriptografik algoritmalar, kriptografi uygulamalarında kullanılan matematiksel işlemlerdir. Bu algoritmalar, verileri şifrelemek, şifre çözmek, özetlemek, imzalamak, doğrulamak gibi işlevler gerçekleştirir. Kriptografik algoritmalar, simetrik ve asimetrik olmak üzere iki ana kategoriye ayrılır. Simetrik algoritmalar, hem şifreleme hem de şifre çözme işlemlerinde aynı anahtarın kullanıldığı algoritmalar olup, hızlı ve verimli çalışırlar. Asimetrik algoritmalar ise, şifreleme ve şifre çözme işlemlerinde farklı anahtarların kullanıldığı algoritmalar olup, daha güvenli ve esnek çalışırlar. Ancak, asimetrik algoritmalar, simetrik algoritmalara göre daha yavaş ve karmaşıktır. Asimetrik kriptografi ve simetrik kriptografi arasındaki fark, şifreleme ve şifre çözme işlemlerinde kullanılan anahtarların sayısı ve türüdür. Simetrik kriptografi, hem şifreleme hem de şifre çözme için aynı anahtarı kullanır. Bu anahtar, şifreli veriyi gönderen ve alan kişiler arasında gizli tutulmalıdır. Asimetrik kriptografi ise, şifreleme için açık anahtar, şifre çözme için özel anahtar adı verilen iki farklı ama birbiriyle ilişkili anahtar kullanır. Açık anahtar, herkese açık olarak paylaşılabilir, ancak özel anahtar, sadece veriyi alacak kişi tarafından bilinmelidir. Simetrik kriptografi, asimetrik kriptografiye göre daha hızlı ve verimli çalışır, ancak anahtarın güvenli bir şekilde paylaşılması ve saklanması sorun yaratabilir. Asimetrik kriptografi, anahtar paylaşımı sorununu çözer, ancak daha yavaş ve karmaşıktır. Ayrıca, asimetrik kriptografi, simetrik kriptografiye göre daha uzun anahtarlar gerektirir. Bu nedenle, simetrik ve asimetrik kriptografi, farklı senaryolarda farklı avantaj ve dezavantajlara sahiptir.

Güvenlik ve hız olarak karşılaştıracak olursak; Genel olarak, asimetrik şifreleme, anahtar paylaşımı sorununu çözerek daha yüksek bir güvenlik seviyesi sağlar, ancak daha yavaş ve karmaşıktır. Simetrik şifreleme ise daha hızlı ve verimli çalışır, ancak anahtarın güvenli bir şekilde paylaşılması ve saklanması sorun yaratabilir. Ayrıca, asimetrik şifreleme, simetrik şifrelemeye göre daha uzun anahtarlar gerektirir, çünkü açık ve özel anahtar arasında matematiksel bir ilişki olmalıdır. Bu nedenle, simetrik ve asimetrik şifreleme, farklı senaryolarda farklı güvenlik gereksinimlerine göre kullanılabilir. Simetrik ve asimetrik şifreleme arasındaki hız farkı, şifreleme ve şifre çözme işlemlerinde kullanılan anahtarların sayısı, türü ve uzunluğu ile ilgilidir. Genel olarak, simetrik şifreleme, aynı anahtarın kullanılması ve daha kısa anahtar uzunlukları nedeniyle asimetrik şifrelemeye göre daha hızlı ve verimli çalışır. Asimetrik şifreleme ise, farklı ve daha uzun anahtarların kullanılması ve matematiksel işlemlerin daha karmaşık olması nedeniyle daha yavaş ve zorlayıcıdır. Bu nedenle, simetrik ve asimetrik şifreleme, farklı senaryolarda farklı performans gereksinimlerine göre kullanılabilir.

1.4 Temel Post-Kuantum Kriptografik Algoritmaların İncelenmesi

Temel Post-Kuantum Kriptografik Algoritmalarım İncelenmesi, kuantum bilgisayarların geleneksel kriptografiyi kırabileceği bir gelecekte verilerin güvenliğini sağlamak için yeni şifreleme yöntemleri araştıran bir konudur. Bu konuda birçok farklı yaklaşım vardır, ancak genel olarak kuantum sonrası kriptografi, kuantum hesaplama gücüne dayanıklı matematiksel problemlere dayanır. Bazı örnekler şunlardır:
Kafes tabanlı kriptografi: Bu yöntem, kafes şekilleri üzerinde tanımlanan matematiksel işlemleri kullanır. Kafes tabanlı kriptografi, hem anahtar kapsülleme mekanizmaları hem de dijital imzalar için uygundur. Öne çıkan teklifler, Crystals-Kyber ve Crystals-Dilithium'dur.
Kod tabanlı kriptografi: Bu yöntem, hata düzeltme kodları üzerinde tanımlanan matematiksel işlemleri kullanır. Kod tabanlı kriptografi, özellikle McEliece şifreleme sistemi ve varyantları ile bilinir. Öne çıkan teklifler, Classic McEliece, BIKE ve LEDAcrypt'tir.
Çok değişkenli kriptografi: Bu yöntem, çok değişkenli polinomlar üzerinde tanımlanan matematiksel işlemleri kullanır. Çok değişkenli kriptografi, özellikle dijital imzalar için uygundur. Öne çıkan teklifler, Rainbow, GeMSS ve MQDSS'dir. Bu yöntemlerin her biri, kuantum sonrası kriptografi alanında önemli bir rol oynamaktadır. Ancak, henüz tam olarak olgunlaşmadıkları ve bazı dezavantajlara sahip oldukları da unutulmamalıdır. Örneğin, kuantum sonrası kriptografi, geleneksel kriptografiye göre daha uzun anahtarlar ve daha yavaş işlemler gerektirebilir. Bu nedenle, kuantum sonrası kriptografi, sürekli araştırma ve geliştirme gerektiren bir alandır.

1.4.1 NTRUEncrypt

NTRUEncrypt, kuantum bilgisayarlarla kırılamayacağı varsayılan kafes tabanlı bir şifreleme yöntemidir. NTRU kafesindeki en kısa vektör problemini çözmeye dayanır. NTRUEncrypt, RSA ve eliptik eğri kriptografisine göre daha hızlı ve daha

güvenli bir alternatif olarak önerilmiştir. Ancak, henüz yeterince kriptografik analize tabi tutulmadığı için bazı riskleri de vardır.
NTRUEncrypt, üç tam sayı parametresi (N, p, q) kullanır. Burada N, polinom derecesi sınırı, p küçük modül, q ise büyük modüldür. N asal, q her zaman p'den çok daha büyük ve p ile q aralarında asal olacak şekilde seçilir. Düz metin mesajları p modülü, şifreli metin mesajları ise q modülü olarak alınır. Şifreleme işlemi, düz metin mesajına rastgele seçilmiş bir halka açık anahtar katı eklemekten ibarettir. Halka açık anahtar, küçük modül p'nin bir katı olarak da görülebilir. Bu, özel anahtara sahip olanın, şifreli metinden düz metni çıkarabilmesini sağlar.
NTRUEncrypt'in avantajları:
Şifreleme ve deşifreleme işlemleri sadece basit polinom çarpımlarını içerir, bu yüzden diğer asimetrik şifreleme yöntemlerine göre çok daha hızlıdır.
Kuantum bilgisayarlarla kırılması mümkün olmayan bir matematiksel probleme dayanır, bu yüzden kuantum sonrası kriptografi için uygun bir adaydır.
Anahtar boyutu ve işlem karmaşıklığı, RSA ve eliptik eğri kriptografisine göre daha düşüktür.
NTRUEncrypt'in dezavantajları:
Henüz tam olarak olgunlaşmamış ve standartlaşmamış bir kriptosistemdir, bu yüzden bazı parametre seçimleri ve uygulama detayları güvenlik açıklarına yol açabilir.
Bazı yayınlanmış saldırılara karşı savunmasız olabilir, bu yüzden dikkatli bir şekilde parametre seçimi yapmak gerekir.
Geleneksel kriptografiden daha uzun anahtarlar ve daha yavaş işlemler gerektirebilir, bu yüzden performans ve depolama açısından bazı zorluklar oluşturabilir.
NTRUEncrypt, kuantum sonrası kriptografi alanında önemli bir rol oynamaktadır. Ancak, sürekli araştırma ve geliştirme gerektiren bir alandır.

1.4.2 Lattice tabanlı kriptografi

Lattice tabanlı kriptografi, matematiksel ızgara (lattice) yapıları üzerine kurulu bir kriptografi dalıdır. Bu algoritma, kuantum bilgisayarlarının bazı matematiksel problemleri etkili bir şekilde çözebilme yeteneğini azaltma amacıyla geliştirilmiştir. Lattice, matematikte bir kavram olup düzlemsel bir yapıda noktaların oluşturduğu düzensiz bir ağdır. Lattice tabanlı kriptografinin temelini oluşturan problemler arasında "Learning With Errors (LWE)" ve "Ring-LWE" gibi karmaşık matematiksel problemler bulunur. Bu problemlerin çözümü, klasik bilgisayarlar üzerinde etkili bir şekilde yapılabilirken, kuantum bilgisayarları için oldukça zorlayıcıdır.

Learning With Errors (LWE):

LWE, lattice tabanlı kriptografinin temelini oluşturan bir matematiksel problemidir. Bu problem, bir nokta kümesi üzerindeki lineer denklemler ile bu noktalara rastgele eklenen hataların öğrenilmesi üzerine kuruludur. LWE'nin çözümü, kuantum bilgisayarlar tarafından etkili bir şekilde yapılamaz. Ring-LWE, LWE'nin bir genişletmesidir ve polinomlar üzerine kurulmuştur. Bu problem, özellikle halka (ring) yapısını kullanarak LWE'nin matematiksel yapısını genişletir. Ring-LWE, Lattice tabanlı kriptografinin temel protokollerinden biri olan NTRUEncrypt gibi algoritmaların dayandığı problemlerden biridir.
Anahtar Değişimi ve Şifreleme: Lattice tabanlı kriptografi, anahtar değişimi ve veri şifreleme için kullanılabilir. Bu algoritmalar, güvenli iletişim kurma amacıyla genellikle

kullanılır. Örneğin, NTRUEncrypt algoritması lattice tabanlı bir şifreleme algoritmasıdır.
Lattice tabanlı kriptografi, geleneksel kriptografik yöntemlere kıyasla kuantum bilgisayarlarına karşı daha dayanıklıdır. LWE ve benzeri matematiksel problemlerin çözümü, kuantum bilgisayarlar tarafından çok zor veya etkisiz bir şekilde gerçekleştirilebilir.

Lattice tabanlı kriptografi algoritmaları, NIST (National Institute of Standards and Technology) gibi kuruluşlar tarafından post-kuantum kriptografisi standartlarının oluşturulması sürecinde değerlendirilmektedir. Bu standartlar, gelecekteki güvenli iletişim ihtiyaçlarına karşı dirençli algoritmaların belirlenmesini amaçlar.
Lattice tabanlı kriptografi, kuantum bilgisayarlarına karşı dayanıklı olma potansiyeli nedeniyle gelecekteki kriptografik uygulamalarda önemli bir rol oynaması beklenen bir alanı temsil eder. Ancak, bu algoritmaların tam güvenliği ve dayanıklılığı üzerinde çalışmalar devam etmektedir.

1.4.3 Hash Tabanlı Şifreleme

Hash Tabanlı Şifreleme, bir mesajın hash fonksiyonu kullanılarak şifrelenmesi ve deşifrelenmesi yöntemidir. Hash fonksiyonu, herhangi bir uzunluktaki bir girdiyi, sabit uzunlukta ve benzersiz bir çıktıya dönüştüren bir matematiksel işlemdir. Hash Tabanlı Şifreleme, kuantum bilgisayarların kırabileceği geleneksel şifreleme yöntemlerine karşı bir alternatif olarak önerilmiştir.
Hash Tabanlı Şifreleme, iki temel bileşenden oluşur: bir anahtar üretme algoritması ve bir şifreleme algoritması. Anahtar üretme algoritması, rastgele bir gizli anahtar seçer ve bu anahtarı hash fonksiyonu ile işleyerek bir dizi alt anahtar oluşturur. Bu alt anahtarlar, şifreleme algoritması tarafından kullanılır. Şifreleme algoritması, mesajı bit dizisine dönüştürür ve her bir biti, bir alt anahtar ile XOR işlemine tabi tutar. XOR işlemi, iki bitin eşit olması durumunda 0, farklı olması durumunda 1 üreten bir mantıksal işlemdir. Böylece, şifreli mesaj elde edilir. Deşifreleme işlemi, aynı alt anahtarlar ile XOR işlemi tekrarlanarak yapılır.
Hash Tabanlı Şifrelemenin avantajları:
Kuantum bilgisayarlarla kırılması zor olan bir matematiksel probleme dayanır, bu yüzden kuantum sonrası kriptografi için uygun bir adaydır. Hash fonksiyonları, basit ve hızlı bir şekilde hesaplanabilir, bu yüzden performans açısından avantajlıdır.
Hash fonksiyonları, yaygın ve standart bir şekilde kullanılır, bu yüzden uyumluluk açısından avantajlıdır.
Hash Tabanlı Şifrelemnin dezavantajları:
Her bir gizli anahtar, sadece bir kez kullanılabilir, bu yüzden anahtar yönetimi açısından zorluklar oluşturabilir.
Şifreli mesaj, orjinal mesajdan daha uzun olabilir, bu yüzden depolama ve iletim açısından zorluklar oluşturabilir.
Hash fonksiyonlarının güvenliği, seçilen parametrelere ve uygulama detaylarına bağlıdır, bu yüzden güvenlik açıklarına yol açabilir.
Hash Tabanlı Şifreleme, kuantum sonrası kriptografi alanında önemli bir rol oynamaktadır.

Hash tabanlı şifreleme," aslında bir terim çelişkisine işaret eder. Hash fonksiyonları genellikle tek yönlü (one-way) fonksiyonlardır ve şifreleme işlemi geri döndürülemez. Dolayısıyla, "hash tabanlı şifreleme" ifadesi doğru bir kavram değildir. Ancak, bu ifade bazen daha genel anlamda bir kriptografik işlemi ifade etmek için kullanılabilir.
Bir hash fonksiyonu, belirli bir girdi kümesini (mesela bir metin ya da dosya) sabit uzunluktaki bir çıktıya dönüştüren bir matematiksel fonksiyondur. Bu çıktı, genellikle "hash değeri" veya "hash kodu" olarak adlandırılır. Hash fonksiyonları genellikle aşağıdaki özelliklere sahiptir:

1.4.4 Code Tabanlı Kriptografi

Code Tabanlı Kriptografi, hata düzeltici kodlar kullanarak açık anahtarlı şifreleme oluşturan bir kuantum sonrası kriptografi yöntemidir. Bu yöntem, 1978'de Robert McEliece tarafından önerilmiştir ve kuantum bilgisayarların kırabileceği geleneksel şifreleme yöntemlerine karşı bir alternatif olarak sunulmuştur.
Code Tabanlı Kriptografi, bir mesajı, bir hata düzeltici kodun bir parolası olarak şifreler. Bu kod, bir matris çarpımı ile elde edilen bir kod sözcüğüdür. Şifreleme işlemi, kod sözcüğüne rastgele bir hata vektörü eklemekten ibarettir. Bu, kod sözcüğünü tanınmaz hale getirir. Deşifreleme işlemi, özel anahtara sahip olanın, şifreli mesajdan hata vektörünü çıkarabilmesini sağlar. Kuantum bilgisayarlarla kırılması zor olan bir matematiksel probleme dayanır, bu yüzden kuantum sonrası kriptografi için uygun bir adaydır. Yaygın ve standart bir şekilde kullanılır. Şifreleme ve deşifreleme işlemleri, basit matris çarpımlarını içerir.
Şifreli mesaj, orijinal mesajdan çok daha uzun olabilir. Anahtar boyutu ve işlem karmaşıklığı, geleneksel şifreleme yöntemlerine göre daha yüksektir, bu yüzden performans ve depolama açısından zorluklar oluşturabilir. Bazı yayınlanmış saldırılara karşı savunmasız olabilir, bu yüzden dikkatli bir şekilde parametre seçimi yapmak gerekir.

Hata Düzeltici Kodlar (Error-Correcting Codes):

Hata düzeltici kodlar, veri iletimi veya depolama sırasında oluşan hataları düzeltmek için kullanılan matematiksel kodlardır. Bu kodlar, özellikle hata düzeltici özelliklere sahip vektörlerle çalışarak hataları tespit edip düzeltebilirler. Code tabanlı kriptografide, hata düzeltici kodlar genellikle güvenli anahtar dağıtımı ve şifreleme işlemleri için kullanılır.
McEliece kriptosistemi, code tabanlı bir kriptografik sistemdir ve özkodları kullanarak güvenli anahtar değişimi sağlar. Bu sistem, matris çarpımı ve hata düzeltici kodları gibi matematiksel kavramlara dayanır. McEliece kriptosistemi, özellikle post-kuantum kriptografisi bağlamında ilgi çekici bir alternatif olarak değerlendirilir.
Kod Tabanlı Şifreleme Algoritmaları:
Code tabanlı kriptografi, özellikle kuantum bilgisayarların geleneksel şifreleme algoritmalarını çözebilecek potansiyeli göz önüne alındığında, alternatif bir güvenlik

yaklaşımı olarak ortaya çıkmıştır. Bu tür algoritmalar, hata düzeltici kodları ve matematiksel kodlama teorisi prensiplerini içerebilir.
Anahtar Değişimi ve Şifreleme:Code tabanlı kriptografi, güvenli anahtar değişimi ve veri şifreleme işlemleri için kullanılabilir. Bu algoritmalar, özellikle hata düzeltici kodların kullanımı sayesinde güvenli iletişim sağlamak amacıyla tasarlanmıştır.
Güvenlik ve Dayanıklılık:
Code tabanlı kriptografi, post-kuantum dünyasında güvenlik sağlamak üzere tasarlanmıştır. Hata düzeltici kodlar, çoğunlukla kuantum bilgisayarların etkili bir şekilde çözemeyeceği problemlere dayandığından, bu tür kriptografik sistemler gelecekteki güvenlik ihtiyaçlarına karşı dayanıklı olabilir.
Code tabanlı kriptografi, özellikle post-kuantum kriptografisi alanındaki araştırmalarda önemli bir rol oynamaktadır. Ancak, bu tür sistemlerin geniş ölçüde benimsenmesi ve standartlaşması için daha fazla araştırma ve değerlendirme süreci devam etmektedir.

1.4.5 Multivariate Polynomial Kriptografi

Multivariate Polynomial Kriptografi, çok değişkenli polinomlar üzerinde tanımlanan matematiksel işlemleri kullanarak asimetrik kriptografik ilkel oluşturan bir kuantum sonrası kriptografi yöntemidir. Bu yöntem, 1988'de Tsutomu Matsumoto ve Hideki Imai tarafından önerilmiştir ve kuantum bilgisayarların kırabileceği geleneksel kriptografi yöntemlerine karşı bir alternatif olarak sunulmuştur. Multivariate Polynomial Kriptografi, bir açık anahtar ve bir gizli anahtar olmak üzere iki anahtardan oluşur. Açık anahtar, çok değişkenli polinomlardan oluşan bir sistemdir. Gizli anahtar, bu polinomları oluşturmak için kullanılan iki a ne dönüşüm ve bir tersine çevrilebilir çok değişkenli polinomlardan oluşan bir sistemdir. Şifreleme işlemi, açık anahtarın polinomlarını mesajın bileşenleri üzerinde uygulamaktan ibarettir. Deşifreleme işlemi, gizli anahtarın polinomlarını şifreli mesajın bileşenleri üzerinde uygulamaktan ibarettir.
Multivariate Polynomial Kriptografi, birçok farklı varyant ve alt sınıfa sahiptir. Örneğin, polinomların derecesi iki ise, çok değişkenli kuadratik kriptografi olarak adlandırılır. Polinomların derecesi üç veya daha yüksek ise, çok değişkenli yüksek dereceli kriptografi olarak adlandırılır. Polinomlar, hem bir temel alan hem de bir genişletme alanı üzerinde tanımlanmışsa, gizli alan denklemleri olarak adlandırılır. Polinomlar, yağ ve sirke tekniği ile oluşturulmuşsa, yağ ve sirke kriptografisi olarak adlandırılır
Multivariate Polynomial Kriptografisi, matematiksel olarak çok değişkenli polinomlar üzerine dayanan bir kriptografik yaklaşımı ifade eder. Bu tür kriptografik sistemler, polinomların üzerinde çalışarak güvenlik sağlamayı amaçlar. Multivariate Polynomial Kriptografisi, özellikle post-kuantum kriptografisi bağlamında güvenlik sağlamak üzere tasarlanmıştır.

Çok Değişkenli Polinomlar:

Multivariate Polynomial Kriptografisi, birçok değişken içeren polinomları temel alır. Bu polinomlar, genellikle lineer ve non-lineer terimleri içerebilir. Polinomlardaki değişkenler, matematiksel karmaşıklığı artırarak güvenlik düzeyini artırabilir.

Bu kriptografik sistemler, çok değişkenli polinomlardan türetilen matematiksel problemlere dayanarak güvenlik sağlamayı amaçlar. Bu problemlerin çözümü, klasik bilgisayarlar üzerinde etkili bir şekilde yapılabilecekken, kuantum bilgisayarları için zorlayıcıdır.

Güvenli Anahtar Değişimi ve Şifreleme:

Multivariate Polynomial Kriptografisi, güvenli anahtar değişimi ve veri şifreleme için kullanılabilir. Bu, iletişimde güvenliği sağlamak, dijital imzalar oluşturmak ve veri güvenliğini temin etmek amacıyla kullanılabilir.

Rainbow ve HFE:

Multivariate Polynomial Kriptografisi'nin örneklerinden biri, Rainbow ve Hidden Field Equations (HFE) gibi algoritmaları içerir. Rainbow, özellikle çok değişkenli polinomlara dayanan bir imza şemasını ifade eder. HFE ise birçok değişkenli polinomlar üzerine kurulu bir şifreleme algoritmasıdır.

Bu tür kriptografik sistemlerin dayandığı matematiksel problemler, özellikle çok değişkenli polinomların sistemli çözümüne yönelik zorluklar içerir. Bu zorluklar, kuantum bilgisayarlar gibi gelişmiş bilgisayar sistemlerinin çözme potansiyelini sınırlamayı hedefler.

Multivariate Polynomial Kriptografisi, geleneksel sayı teorisi veya cebirsel geometri gibi diğer kriptografik temellerin yanında, matematiksel problemleri çözme zorlukları üzerine kurulu bir güvenlik modeline dayanır. Bu tür sistemler, kuantum bilgisayarlarına karşı dirençli olma amacıyla post-kuantum kriptografisinin bir parçası olarak değerlendirilir.

2. Kuantum Bilgisayarların Kriptografiye Etkisi ve Güvenlik Standartları

Dijital çağın gelişimi, bize inanılmaz bir bilgi işleme kapasitesi ve bağlantılılık düzeyi sunarken, bu aynı zamanda gizliliği ve güvenliği de zorlayan bir döneme işaret ediyor. Kuantum bilgisayarlar, bu evrimin belki de en çarpıcı unsurlarından biri olarak öne çıkıyor. Geleneksel bilgisayarlar, işlemlerini bitleri kullanarak yaparken, kuantum bilgisayarlar kuantum bitleri veya "qubit"leri kullanarak işlemlerini gerçekleştirir. Bu durum, belirli matematiksel problemleri çözme konusunda inanılmaz bir potansiyele işaret eder, ancak aynı zamanda kriptografi alanında ciddi soruları da gündeme getirir.

Kuantum bilgisayarların bu çığır açan potansiyeli, özellikle kriptografinin temellerini sarsmaktadır. Geleneksel kriptografi algoritmaları, genellikle büyük sayıları çözme zorluğuna dayanır ve bu durum, günümüz bilgisayarlarının işleme gücüyle başa

çıkılabilecek düzeydedir. Ancak, kuantum bilgisayarlar, kuantum süperpozisyonu ve kuantum dolanıklığı gibi özellikleri sayesinde, bu büyük sayıları paralel olarak işleyebilme yeteneğine sahiptir. Bu, RSA gibi mevcut kriptografik algoritmaların temelini oluşturan matematiksel problemleri, klasik bilgisayarlarla günlerce sürecek işlemlerden sadece saniyeler içinde çözebilmelerine olanak tanır.

Kuantum bilgisayarlarının bu çığır açan hesaplama gücü, özellikle günlük yaşantımızda sıkça karşılaştığımız güvenlik standartlarını zorlayan bir tehdit oluşturuyor. İletişimlerimizin şifrelenmesinden, dijital imzalara, hatta finansal işlemlerimize kadar birçok alanda kriptografi kullanılır. Ancak, bu sistemlerin dayandığı matematiksel zorluklar, kuantum bilgisayarlar karşısında çözülebilecek düzeyde zayıflayabilir. Bu durum, gizlilik ve bütünlük prensiplerini derinden sarsabilir.

Kuantum Sonrası Kriptografi Çözümleri:

Ancak, umutsuzluğa kapılmak yerine, bu kuantum tehdidiyle başa çıkmak üzere post-kriptografik, yani kuantum sonrası kriptografi çözümleri geliştirilmektedir. Bu yeni nesil güvenlik yaklaşımları, kuantum bilgisayarlar karşısında dirençli olacak şekilde tasarlanmıştır. Lattice tabanlı kriptografi, code tabanlı kriptografi, ve çok değişkenli polinom kriptografisi gibi teknolojiler, kuantum sonrası dönemde güvenliği sağlamak için önemli bir rol oynamaktadır.

Kuantum bilgisayarların kriptografiye olan etkisi, sadece güvenlik standartlarını değil, aynı zamanda kriptografinin temel anlayışını da yeniden şekillendirme potansiyeline sahiptir. Bu durum, kuantum sonrası kriptografi çözümlerinin geliştirilmesi ve benimsenmesi ihtiyacını ortaya koymaktadır. Ancak, bu yeni çağda güvenliğin teminat altına alınması, sadece teknoloji geliştirmekle değil, aynı zamanda bilinçli ve işbirliğine dayalı bir çaba ile mümkün olacaktır.

2.1 Kuantum Bilgisayarların Çalışma Prensibi

Kuantum bilgisayarlar, klasik bilgisayarlarla karşılaştırıldığında temelde farklı bir çalışma prensibine sahiptir. Kuantum bilgisayarlar, kuantum mekaniği prensiplerine dayanarak bilgiyi işler ve bu prensipler, geleneksel bilgisayarların kullanımına göre oldukça farklıdır.
Kuantum bilgisayarların çalışma prensibi, kuantum mekaniğinin temel yasalarını kullanarak veri işlemeye dayanır. Kuantum bilgisayarları, geleneksel bilgisayarlardan farklı olarak, bilgiyi 0 veya 1 değerini alabilen bitler yerine, aynı anda hem 0 hem de 1 değerini alabilen kuantum bitleri (qubit) olarak depolar ve işler. Bu özellik, kuantum bilgisayarlarının çok daha hızlı ve güçlü hesaplamalar yapabilmesini sağlar. Kuantum bilgisayarlarının çalışma prensibini anlamak için, kuantum mekaniğinin iki önemli ilkesini bilmek gerekir: süperpozisyon ve dolanıklık. Süperpozisyon ilkesi, bir kuantum sisteminin birden fazla olası durumun bir karışımı olarak var olabileceğini söyler. Dolanıklık ilkesi ise, birbirine bağlı olan iki veya daha fazla kuantum sisteminin, birbirinden uzakta olsalar bile, birlikte davrandığını söyler. Bu iki ilke sayesinde, kuantum bilgisayarları, geleneksel bilgisayarlara göre çok daha fazla veriyi aynı anda

işleyebilir ve paralel olarak çalışabilir. Kuantum bilgisayarlarının çalışma prensibini, bir örnek üzerinden açıklamaya çalışalım. Diyelim ki, bir geleneksel bilgisayar, bir mesajı şifrelemek için 4 bitlik bir anahtar kullanıyor. Bu durumda, anahtarın alabileceği olası değerler 0000, 0001, 0010, 1110, 1111 olmak üzere toplam 16 tanedir. Geleneksel bilgisayar, bu değerlerden birini seçmek için 4 bitlik bir bellek alanı kullanır. Ancak, bir kuantum bilgisayar, aynı işlemi yapmak için 4 qubitlik bir anahtar kullanırsa, anahtarın alabileceği olası değerler, süperpozisyon ilkesi sayesinde, 16 değerin tümünün bir karışımı olabilir. Bu durumda, kuantum bilgisayar, 4 qubitlik bir bellek alanı kullanarak, geleneksel bilgisayarın 4 bitlik bellek alanı ile yapabileceğinden çok daha fazla işlem yapabilir.

Kuantum bilgisayarlarının çalışma prensibinin, birçok alanda büyük bir potansiyeli vardır. Örneğin, kuantum bilgisayarlar, geleneksel bilgisayarların kırabileceği şifreleme yöntemlerine karşı çok daha güvenli bir şekilde veri koruyabilir, kimyasal ve biyolojik sistemlerin davranışlarını çok daha doğru bir şekilde modelleyebilir, optimizasyon ve yapay zeka gibi problemlerde çok daha hızlı ve etkili bir şekilde çözüm bulabilir.

Kuantum bilgisayarların çalışma prensibi, kuantum mekaniğinin karmaşık ve ilginç yasalarını kullanarak, bilgisayar teknolojisinde devrim yaratacak bir alandır. Ancak, kuantum bilgisayarların geliştirilmesi ve kullanılması, halen birçok zorluk ve engel içermektedir. Bu nedenle, kuantum bilgisayarların çalışma prensibi, sürekli araştırma ve geliştirme gerektiren bir alandır.

2.1.1 Kuantum Bit

Kuantum bit ya da kısaca "qubit," kuantum bilgisayarlarında temel bilgi birimi olarak kullanılan kuantum mekaniği özelliklerine dayalı bir konsepttir. Qubit, klasik bilgisayarların temel birimi olan bitin aksine, hem 0 hem de 1 durumunda aynı anda bulunabilen bir durumu ifade eder. Bu durum, qubitin sahip olduğu süperpozisyon özelliği olarak adlandırılır.

Süperpozisyon:

Bir qubit, klasik bitin sadece 0 veya 1 olma durumunun ötesinde, aynı anda hem 0 hem de 1 olabilir. Bu durumu süperpozisyon olarak adlandırılır. Süperpozisyon, qubitin aynı anda bir dizi olası durumu temsil etmesini sağlar.

Belirsizlik İlkesi:

Bir qubitin belirli bir anda hem 0 hem de 1 olma olasılığı, belirsizlik ilkesi ile açıklanır. Bir qubit belirli bir durumda ölçüldüğünde, bu belirsizlik sona erer ve qubit belirli bir değeri alır.

Örüntülenme (Entanglement):

Qubitler arasındaki kuantum dolanıklığı, bir qubitin durumunun diğer bir qubitin durumunu etkileyebilmesi anlamına gelir. İki qubit arasındaki bu örüntülenme, uzaktaki qubitler arasında hemen bir etkileşim kurulabilmesini sağlar.

Kuantum Kapıları:

Kuantum bilgisayarlar, qubitleri manipüle etmek için kuantum kapıları adı verilen işlem birimlerini kullanır. Bu kapılar, qubitler arasındaki süperpozisyonu değiştirebilir veya kuantum dolanıklığını kullanarak özel hesaplamalar gerçekleştirebilir.
Kuantum Paralelizmi:
Qubitlerin süperpozisyon özelliği, kuantum bilgisayarların paralel hesaplamalar gerçekleştirebilme yeteneğine yol açar. Bu, belirli hesaplamaların klasik bilgisayarlarla karşılaştırıldığında çok daha hızlı bir şekilde gerçekleştirilebileceği anlamına gelir.
Qubitlerin bu özellikleri, kuantum bilgisayarların belirli problemleri çözme potansiyelini artırır. Ancak, qubitlerin bu kuantum özelliklerini korumak ve istikrarlı bir şekilde kullanmak, kuantum bilgisayarların geliştirilmesi sürecinde önemli teknik zorluklardan biridir.

2.1.2 Süperpozisyon ve Paralel İşlemler:

Süperpozisyon, kuantum mekaniğinin temel bir ilkesidir ve kuantum bilgisayarlarının önemli bir özelliğini oluşturur. Klasik bilgisayarlar, bir bitin aynı anda hem 0 hem de 1 olmasını düşünemez; ancak kuantum bilgisayarlarında qubitler, süperpozisyon durumunda hem 0 hem de 1 olabilirler. Yani, bir qubitin belirli bir durumda olma olasılığı, 0 ve 1 durumları arasında dağılmıştır.
Bu, bir kuantum bilgisayarının aynı anda bir dizi olası durumu işleyebilmesini sağlar. Örneğin, iki qubitin süperpozisyon durumunda, bu qubitlerin kombinasyonları sayısınca olası durum vardır. Süperpozisyon, kuantum bilgisayarlarının paralel işlemler gerçekleştirme yeteneğinin temelini oluşturur.
Paralel İşlemler:
Süperpozisyonun sağladığı avantaj, kuantum bilgisayarlarının paralel işlemleri çok daha etkili bir şekilde gerçekleştirebilmesidir. Klasik bilgisayarlar, bir işlemci üzerinde belirli bir anda yalnızca bir dizi komutu işleyebilirler. Ancak kuantum bilgisayarlarında, süperpozisyon durumundaki qubitlerin aynı anda birçok olası durumu temsil etmesi, birçok paralel hesaplama yolunun eş zamanlı olarak değerlendirilebileceği anlamına gelir.

Bu durum, belirli problemleri çözmek için klasik bilgisayarların gerektirdiğinden çok daha az adımda işlem yapabilme potansiyelini içerir. Özellikle bazı algoritmalar, kuantum bilgisayarlarının paralel işleme yeteneğini kullanarak klasik bilgisayarlarla karşılaştırıldığında önemli hızlanmalar sağlayabilir. Bu da kuantum bilgisayarlarını belirli problemlerde son derece etkili kılar.

Ancak önemli bir not olarak, süperpozisyon ve paralel işlemler sadece belirli hesaplamalarda avantaj sağlar; kuantum bilgisayarlarının genel performans avantajı, belirli tipteki problemlerde daha belirgindir ve bu avantaj, qubitlerin kuantum özelliklerini korumak ve stabil bir şekilde kullanmak konusundaki teknik zorluklara bağlıdır.

2.1.3 Kuantum Dolanıklığı

Kuantum dolanıklığı, kuantum mekaniğinin temel bir özelliğidir ve iki ya da daha fazla parçacığın birbirleri arasında özel bir bağlantı kurarak birlikte bir durumda bulunmalarını ifade eder. Bu durum, bir parçacığın durumu belirlendiğinde, diğer parçacığın durumunun anında belirlenmesi anlamına gelir, bağlı parçacıklar arasında bir tür "anında etkileşim" sağlar.

Anında Etkileşim:

İki dolanık (entangled) parçacık arasındaki etkileşim anında gerçekleşir. Bir parçacığın durumu ölçüldüğünde, diğer parçacığın durumu belirlenmiş olur, bu da bu parçacıklar arasında bir tür bağlantının olduğunu gösterir.
Kuantum dolanıklığı, parçacıklar arasındaki uzaklığa bağlı olmaksızın gerçekleşebilir. Yani, dolanık parçacıklar birbirinden uzakta olsalar bile, birinin durumu belirlendiğinde diğerinin durumu hemen belirlenir.
Dolanık parçacıklar, belirli bir özellik ya da durum konusunda birbirlerine bağlı olduklarından, birinin ölçümü yapıldığında diğerinin durumu hemen belirlenir. Bu durum, dolanık parçacıkların birbirlerine bağlı bir şekilde karışık durumlar içinde bulunmasını sağlar.
Kuantum dolanıklığı, kuantum iletişim sistemlerinde de kullanılabilir. Uzak mesafelerdeki iki nokta arasında bilgi iletimi için kullanılan kuantum teleportasyon gibi konseptlerde kuantum dolanıklığı önemli bir rol oynar.
Parçacıklar Arasındaki Bağlantı:

Kuantum dolanıklığı, parçacıklar arasında bir tür bağlantının varlığını ifade eder. Bu bağlantı, belirli özelliklerin ya da durumların birbirleriyle ilişkili olduğunu gösterir.
Kuantum dolanıklığı, kuantum bilgisayarlarında ve kuantum iletişim sistemlerinde önemli uygulamalara sahiptir. Özellikle, kuantum bilgisayarlarının ve kuantum iletişim sistemlerinin daha etkili çalışabilmesi için qubitler arasında dolanıklık kurulması kullanışlıdır. Ancak, bu fenomen, kuantum mekaniği içinde oldukça karmaşık ve sık sık çeşitli zorluklarla karşılaşan bir konsepttir.

2.1.4 Ölçüm ve Belirsizlik İlkesi

Kuantum mekaniğinin temel ilkelerinden biri olan ölçüm ve belirsizlik ilkesi, bir parçacığın belirli özelliklerini ölçtüğümüzde, diğer özelliklerin ölçüm sonuçlarını tahmin etme yeteneğimizin sınırlı olduğunu ifade eder. Bu ilke, Werner Heisenberg tarafından 1927 yılında ortaya atılmıştır ve kuantum dünyasında önemli bir rol oynar.

Ölçüm İşlemi:

Bir parçacığın özelliklerini ölçmek, onun belirli bir durumu hakkında bilgi edinmeyi amaçlar. Ancak, kuantum mekaniğinde, bir özelliği ölçmek, o özelliğin belirli bir durumunu belirleme sürecini içerir.
Belirsizlik İlkesi:
Heisenberg'in belirsizlik ilkesi, bir parçacığın konumu ve momentumu gibi çift özelliklerin eş zamanlı olarak tam olarak belirlenemeyeceğini ifade eder. Bu durum, bir özelliğin ölçüldüğünde diğer özelliğin belirsizliğinin artacağı anlamına gelir.
Konum ve Momentum İlişkisi:
Belirsizlik ilkesi, özellikle bir parçacığın konumu ve momentumu arasındaki ilişkiyi vurgular. Tam olarak belirlenmiş bir konum, o parçacığın momentumunun tam olarak belirlenemeyeceği anlamına gelir ve tam olarak belirlenmiş bir momentum, konumun belirsizliğini arttırır.
Matematiksel İfade:

$\Delta x * \Delta p \geq \hbar / 2$
Δx: Konum belirsizliği
Δp: Momentum belirsizliği
$\hbar$ (h çubuğun yarısı): Azaltılmış Planck sabiti
Belirsizlik ve Bilgi:

Bu ilke, bir parçacığın belirli özelliklerinin tam olarak belirlenemeyeceği gerçeğini vurgular. Kuantum mekaniği, parçacıkların belirli durumlarını tam olarak ölçmenin sınırlarını belirler.
Belirsizlik ilkesi, kuantum dünyasındaki temel belirsizliği ve öngörülemezliği ifade eder. Bu durum, klasik mekaniğin aksine, kuantum mekaniği dünyasında bir nesnenin tam olarak nerede olduğunu veya ne kadar hızlı hareket ettiğini kesin olarak belirlemenin imkansız olduğunu gösterir.

2.1.5 Kuantum Kapıları ve Devreler

Kuantum kapıları, mantıksal devre tasarımında bulunan klasik kapılara alternatiftir. Amaç, elektronik devrelerin karar mekanizmasında quantum teknolojisini kullanmaktır.
Klasik kapılarda bulunan ve bitlere göre karar vermeye yarayan mekanizmadan farklı olarak kuantum kapılarında, kubitler (qubits) üzerinden karar verilir. Kuantum kapılarının bir özelliği, geri döndürülebilir olmalarıdır, yani bir girdi için elde edilen sonuç, sonuçtan girdi olarak verildiğinde, girdi geri elde edilebilir.

Bir mantıksal kapının geri döndürülebilir olması, kapının girdisinden elde edilen çıktının tekrar girdi olması halinde, ilk girdinin geri elde edilebilmesidir. Bu karmaşık cümle ile anlatılmak istenen örneğin L kapısı için L(x) = y gibi bir sonuç alınıyorsa, bu kapının tersi olan L’ için L’(y) = x sonucunun alınması beklenir. Veya kapının kendisinin ters olması halinde de L(x) = y ve L(y) = x şartlarının aynı anda sağlanması beklenir.

Örneğin klasik not gate kapısı geri döndürülebilir kapıdır: Bunu doğruluk çizelgesine bakarak kolayca görebiliriz.

Girdi	Çıktı
1	0
0	1

Görüldüğü üzere L(1) = 0 ve L(0)=1 olmakta, dolayısıyla tersi alınabilir bir kapı olmaktadır.

Buna karşılık, geri döndürülebilirlik (reversible) konusunun daha iyi anlaşılabilmesi için, geri döndürülemez bir kapı olan veya kapısının örneği:.

Girdi	Çıktı
00	0
01	1
10	1

Yukarıdaki pigeonholde principle görüldüğü üzere, herhangi bir çıktının, girdiye verilmesi durumunda, girdinin geri elde edilmesi mümkün değildir. Örneğin L(10) = 1 olmakta ama L(1) = 10 olmamaktadır.

Aynı zamanda herhangi bir L' devresi de yukarıdaki tablonun tersini üretemez. Bunun sebebi, 1 çıktısının 01, 10 veya 11 şeklinde geri döndürülme ihtimali olduğu ve 1 çıktısı alındıktan sonra, orijinal girdinin ne olduğunun tahmininin imkânsız olduğudur.

Ve kapısı örneğini ele alarak, bir kapının geri döndürülebilir olması için giriş ve çıkış bitlerinin sayısının aynı olması gerektiğini tahmin edebilirsiniz. Aslında bu durum basitçe pigeonholde principle ile açıklanabilir ve evet bir kapının geri döndürülebilir olması için giriş biti sayısı ile çıkış biti sayısı eşit olmalıdır Şayet giriş bitlerinin sayısı ile çıkış bitlerinin sayısı eşit ise, kapının karakterini, yukarıdaki örneklerde olduğu gibi doğruluk çizelgesi (truth table) şeklinde klasik gösterimden farklı olarak gösterebiliriz. Aslında kuantum kapıları için vaz geçilmez olan bu gösterim matris gösterimidir.Örneğin not gate kapısını ele alalım ve matriste göstermeye çalışalım.

	0	**1**
0	**0**	**1**
1	**1**	**0**

Yukarıdaki matris, okunması kolay olsun diye bir satır (en üstteki) ve bir sütun (en soldaki) eklenerek verilmiştir. Bu matriste, satırlar, girdiyi, sütunlar ise çıktıyı tutmaktadır. Yani tablomuzu aşağıdaki şekilde yorumlayabiliriz:

	0	**1**
0	**0 girdisi için, 0 çıktısı alınabilir mi?**	**0 girdisi için, 1 çıktısı alınabilir mi?**

Yukarıdaki bu sorulara evet veya hayır cevaplarını vererek evet için 1 ve hayır için 0 yerleştiriyoruz. Örneğin not gate kapısı 0 için 1 sonucu verir ve 0 için 0 sonucu vermez. Dolayısıyla yukarıdaki doğruluk çizelgesinin matris gösterimini aşağıdaki şekilde yapmak yeterlidir.

0	1
1	0

Yukarıdaki bu matrise bakıldığı zaman, bu matrisin doğruluk çizelgesi (truth table) kolaylıkla anlaşılabilir.

Matris gösteriminin kuantum kapıları için kullanılması durumunda, aslında qubit değerlerinin matrise yerleştirilmesinden bahsediliyor demektir.

Örneğin, $\alpha|0> + \beta|1>$ şeklinde yazılan bir kubit gösterimini vektör olarak modellemek istersek

α
β

Görüldüğü üzere, kubitin tersi alınmıştır. Burada dikkat edilecek bir husus, matriste kullanılan α ve β değerlerinin karmaşık sayılar (complex numbers) olduğudur.

Kuantum Kapılarının bir özelliği, bu kapılarda kullanılan matrisin, vahid masfuf (uniter matrix) olmasıdır.

2.1.5.1 Hadamard Kapısı

Hadamard kapısı, kuantum bilgisayarlarında sıklıkla kullanılan bir kapıdır ve bir qubiti süperpozisyon durumuna sokmak için kullanılır. Bu kapı, klasik bilgisayarlarla karşılaştırıldığında farklı bir özelliği temsil eder ve belirli bir durumdaki qubitin hem 0 hem de 1 durumlarında olma olasılığını eşit bir şekilde dağıtır.

Hadamard kapısı, özellikle kuantum algoritmalarında ve kuantum süperpozisyonunu etkili bir şekilde kullanmak için tasarlanmış devrelerde yaygın olarak kullanılır. Süperpozisyon durumu, qubitler arasında paralel işlemler gerçekleştirmek ve belirli algoritmaların avantajlarını elde etmek için kritik bir bileşendir.

2.1.5.1 Pauli X kapısı

Pauli X kapıları, kalsik değil kapısının (not gate), kuantum için uyarlanmış halidir. Yani yazının başında anlatılan ve girişi tersine döndürmeye yarayan kapılar olarak düşünülebilir. Bu durumda matrisi aşağıdaki şekilde olacaktır.

$$X=\sigma_x=\sigma_1=\begin{bmatrix}0 & 1\\ 1 & 0\end{bmatrix} \qquad (2.1)$$

Aslında bu kapının özelliği Bloch Küresini (Bloch Sphere) X ekseni etrafında pi radyan kadar döndürmesi ve |0> değerini |1> ve |1> değerini |0> yapmasıdır.

2.1.5.3 Pauli Y kapısı

Pauli X kapısına benzer olarak bu kapı da Blok Küresi (Bloch Sphere) üzerinde döndürme işlemi yapmaktadır. Ancak bir önceki kapıdan farklı olarak bu defa Y ekseni üzerinde döndürme işlemi yapılır.

$$\boldsymbol{Y} = \begin{bmatrix}0 & -i\\ i & 0\end{bmatrix} \qquad (2.2)$$

2.1.5.4 Pauli Z kapısı

Pauli X ve Y kapılarına benzer şekilde Bloch Küresi üzerinde döndürme işlemi yapılır. Bu defa isminden de anlaşılacağı üzere döndürme işlemi Z ekseni üzerinde olur.

$$Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \qquad (2.3)$$

2.1.5.1 Faz kaydırma kapısı (Phase shift gate)

Bu kapının özelliği, 00, 01 ve 10 için değişiklik yapmamak ama 11 durumu için |1> girdisinin $e^{i\Theta}|1>$ girdisine dönüştürmesidir. Yani |1> için, Θ derece döndürme işlemi yapılmaktadır.

$$R = \begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix} \qquad (2.4)$$

2.2 Kuantum Bilgisayarların Geleneksel Kriptografiye Etkileri

Kuantum bilgisayarlar, geleneksel bilgisayarların kullanmış olduğu klasik bit değerlerine dayalı hesaplama modelinden farklı bir şekilde çalışırlar. Kuantum bilgisayarlar, kuantum mekaniği prensiplerini kullanarak qubit adı verilen kuantum bitleri üzerinde işlem yaparlar. Bu özel bilgi birimleri, geleneksel bitlerin sadece 0 veya 1 değerlerini alabilmesinin aksine aynı anda hem 0 hem de 1 değerlerini alabilirler. Bu durum, kuantum paralelizmi olarak adlandırılır ve kuantum bilgisayarların belirli türde hesaplamalarda paralel olarak çok daha hızlı çalışabilme potansiyeline sahip olduğu anlamına gelir.

2.2.1 Çözme Kapasitesi Artışı

Kuantum bilgisayarların çözme kapasitesindeki artış, özellikle Shor'un kuantum algoritması aracılığıyla bazı matematiksel problemlerin hızlı bir şekilde çözülmesinden kaynaklanır. Shor'un algoritması, büyük sayıları çarpanlarına ayırmak için klasik algoritmaların zaman alacağı problemleri etkili bir şekilde çözebilir. Bu durum, mevcut kriptografik algoritmaların dayandığı matematiksel problemlerin, özellikle RSA ve ECC gibi asimetrik şifreleme algoritmalarının temelindeki sayı teorisi problemlerinin, kuantum bilgisayarlarla daha hızlı bir şekilde çözülebileceği anlamına gelir.

Örneğin, RSA şifrelemesi, büyük asal sayıların çarpanlarına ayrılması zorluğuna dayanır. Ancak Shor'un algoritması, bu tür sayıları hızlı bir şekilde çarpanlarına ayırabilir, bu da RSA şifrelemesinin temel güvenliğini tehlikeye atar. Aynı şekilde, ECC (Elliptic Curve Cryptography) gibi diğer asimetrik şifreleme yöntemleri de Shor'un algoritması tarafından etkilenebilir.

Bu çözme kapasitesindeki artış, mevcut şifreleme yöntemlerinin güvenliğini azaltabilir ve bu da özellikle kritik bilgilerin korunması için kullanılan iletişim sistemlerinde ciddi güvenlik sorunlarına neden olabilir. Bu nedenle, kuantum bilgisayarların çıkışıyla birlikte, kriptografi alanında kuantum güvenli algoritmaların geliştirilmesi ve uygulanması önemli bir araştırma ve geliştirme alanı haline gelmiştir.

2.2.2 Gizlilik Tehlikesi

Kuantum bilgisayarların geleneksel kriptografiye olan etkilerinden biri de gizlilik tehlikesidir. Bu tehlike, özellikle asimetrik şifreleme (public-key cryptography) algoritmalarının kuantum bilgisayarlar tarafından çözülebilir hale gelmesiyle ilgilidir. İşte bu konuda daha fazla detay:

RSA ve ECC Gibi Asimetrik Şifreleme Algoritmalarının Tehdidi: Kuantum bilgisayarlar, Shor'un algoritması gibi özel algoritmalar kullanarak asimetrik şifreleme algoritmalarında kullanılan matematiksel problemleri, örneğin büyük sayıların çarpanlarına ayırma problemi, hızlı bir şekilde çözebilirler. Bu durum, RSA ve ECC gibi popüler asimetrik şifreleme algoritmalarının temelindeki matematiksel problemlerin klasik bilgisayarlarla kıyaslandığında çok daha hızlı bir şekilde çözülebileceği anlamına gelir.
Anahtar Uzunlukları ve Güvenlik Seviyeleri: Geleneksel olarak, RSA veya ECC gibi algoritmaların güvenliği, kullanılan anahtar uzunluklarına dayanır. Ancak kuantum bilgisayarların çözme kapasitesindeki artış, belirli anahtar uzunluklarını daha savunmasız hale getirir. Klasik bilgisayarlar için güvenli olan anahtar uzunlukları, kuantum bilgisayarlar için daha kısa bir sürede çözülebilir hale gelebilir.
Gizli İletişim Tehlikesi: Kuantum bilgisayarlarla çözülebilen algoritmaların kullanılmasıyla, geçmişte güvenli bir şekilde iletilmiş olan şifreli mesajlar veya veriler, kuantum bilgisayarlar tarafından çözülebilir. Bu da geçmişteki gizli iletişimlerin güvenliğini tehdit eder.
Bu gizlilik tehlikesiyle başa çıkabilmek için, kuantum güvenli algoritmaların geliştirilmesi ve uygulanması gerekmektedir. Bu algoritmalar, kuantum bilgisayarlar tarafından çözülemez veya çözülmesi çok zor matematiksel problemlere dayanmalıdır. Quantum Key Distribution (QKD) gibi kuantum güvenlik protokolleri de geleneksel şifreleme yöntemlerinin yerini alabilir ve daha güvenli bir iletişim sağlayabilir.

2.2.3 Quantum Key Distribution (QKD)

Quantum Key Distribution (QKD), kuantum mekaniği prensiplerini kullanarak güvenli bir şekilde anahtar paylaşımı sağlamayı amaçlayan bir kriptografik protokoldür. Temel olarak, QKD, kuantum fiziğindeki belirli özellikleri kullanarak, iki taraf arasında paylaşılan bir anahtarı algılamak veya paylaşmak için izin veren bir iletişim yöntemidir.

QKD'nin temel prensibi şu adımları içerir:

Kuantum Mekaniği İlkeleri: QKD, kuantum mekaniği prensiplerinden faydalanır. Özellikle, Heisenberg belirsizlik ilkesi ve kuantum süperpozisyonu gibi kavramlar kullanılır.
Kuantum Durumları İle Anahtar Paylaşımı: İki taraf arasında bir iletişim kurulduğunda, belirli kuantum durumları (örneğin, fotonların polarizasyon durumları) üzerinden bilgi taşıyan kuantum bitleri veya qubit'ler kullanılır.
Foton Gönderimi ve Algılama: Gönderen taraf, kuantum durumlarını temsil eden fotonları yollar. Alıcı taraf, bu fotonları alır ve kuantum durumunu ölçer.
Heisenberg Belirsizlik İlkesi Kullanımı: Gönderilen ve alınan fotonların polarizasyon durumu gibi özellikleri, Heisenberg belirsizlik ilkesi nedeniyle tam olarak ölçülemez. Bu durum, bir saldırganın bu bilgileri izlemesini zorlaştırır.
Anahtar Paylaşımı ve Güvenlik: Gönderen ve alıcı, kuantum durumlarını kullanarak bir anahtar oluşturur. Bu anahtar daha sonra şifreleme için kullanılabilir. Kuantum mekaniği prensiplerine dayandığı için, QKD'nin güvenliği, bir saldırganın anahtarın paylaşımını izlemesini veya kopyalamasını tespit etmeye dayanır.
QKD'nin temel amacı, geleneksel şifreleme yöntemlerine kıyasla daha güvenli bir anahtar paylaşımı sağlamaktır. Ancak, QKD'nin kullanımı şu anda sınırlıdır ve bazı pratik zorluklarla karşılaşmaktadır. Örneğin, kuantum durumlarını iletmek ve algılamak için özel donanım gereklidir ve bu da maliyeti artırabilir. Ancak, bu alanda devam eden araştırmalar ve teknolojik gelişmelerle birlikte, QKD'nin daha geniş çapta kullanılabilir hale gelmesi beklenmektedir.

2.2.4 Kuantum Güvenli Algoritmaların Geliştirilmesi:

Kuantum bilgisayarların geleneksel kriptografiyi tehdit etmesiyle birlikte, kuantum güvenli algoritmaların geliştirilmesi önemli bir araştırma ve geliştirme alanı haline gelmiştir. Bu algoritmalar, kuantum bilgisayarların çözme kapasitelerine karşı dirençli olacak şekilde tasarlanır ve kriptografik güvenliği sağlamak için kuantum mekaniği prensiplerini kullanır. İşte kuantum güvenli algoritmaların geliştirilmesiyle ilgili bazı temel konular:
Hash Fonksiyonları ve Şifreleme Algoritmaları: Kuantum bilgisayarların hash fonksiyonlarını ve şifreleme algoritmalarını çözebilme potansiyeli, geleneksel algoritmaların yerini alacak ve güvenliği tehlikeye atacak bir risk oluşturur. Bu nedenle, kuantum güvenli hash fonksiyonları ve şifreleme algoritmalarının geliştirilmesi önemlidir.
Kuantum Anahtar Dağıtımı (QKD): QKD, kuantum güvenli algoritmalar arasında öne çıkar. Bu protokol, kuantum mekaniği özelliklerini kullanarak güvenli bir şekilde anahtar paylaşımı sağlar. QKD'nin geliştirilmesi ve yaygınlaştırılması, kuantum bilgisayarların tehdidine karşı dayanıklı bir iletişim sağlamak adına önemlidir.
Gelişmiş Kuantum Rastgele Sayı Üretimi: Güvenli kriptografik protokollerin temelinde rastgele sayılar bulunur. Kuantum bilgisayarların deterministik olmayan doğası göz önüne alındığında, kuantum güvenli rastgele sayı üretimi üzerine odaklanan algoritmaların geliştirilmesi önemlidir.
Quantum-Safe Kriptografik Protokollerin Standartlaştırılması: Kuantum güvenli algoritmaların standartlaştırılması, farklı sistemler ve uygulamalar arasında

uyumluluk sağlamak için önemlidir. Bu, endüstri standardı haline gelmiş güvenli algoritmaların benimsenmesini hızlandırabilir.
Bu alanlardaki çalışmalar, gelecekteki kriptografik ihtiyaçları karşılamak ve bilgi güvenliğini korumak adına kritik öneme sahiptir. Standart kriptografik algoritmaların yerini alacak ve kuantum bilgisayarlar gibi yeni tehditlere karşı dayanıklı olan güvenli algoritmaların geliştirilmesi, bilgi güvenliği alanında önemli bir adımdır.

2.3 Güvenlik Standartlarının Evrimi ve Kuantum Güvenliği

Güvenlik standartları, bilgi güvenliği alanındaki teknolojik gelişmeler ve tehdit değişiklikleriyle paralel olarak sürekli evrim geçirir. Kuantum bilgisayarların ortaya çıkmasıyla birlikte, kriptografi standartları üzerinde de önemli değişiklikler ve güncellemeler beklenebilir.

2.3.1 Post-Kuantum Kriptografisi ve Standartlaştırma

Post-Kuantum Kriptografisi (PQC), kuantum bilgisayarlar gibi gelecekteki güçlü hesaplama teknolojilerine karşı dirençli kriptografik algoritmaların tasarlanması ve geliştirilmesi alanını ifade eder. Bu algoritmalar, kuantum bilgisayarlar tarafından etkili bir şekilde çözülemeyecek veya avantaj sağlayamayacak şekilde oluşturulur. Standartlaştırma ise bu yeni algoritmaların geniş bir kullanım ve uygulama alanına yayılmasını sağlamak amacıyla belirli kuruluşlar tarafından yapılan süreçleri ifade eder.

2.3.1.1 Standartlaştırma Kuruluşları ve İnisiyatifler

Kriptografik standartlar ve güvenlik protokollerinin belirlenmesi ve yaygınlaştırılması için birçok standartlaştırma kuruluşu ve inisiyatif bulunmaktadır. Bu kuruluşlar, endüstrinin ve toplumun bilgi güvenliğini artırmak, uyumlu ve güvenli çözümler geliştirmek amacıyla çalışmaktadır. Önemli standartlaştırma kuruluşları ve inisiyatifler:
National Institute of Standards and Technology (NIST): ABD'deki NIST, bilim ve endüstri alanlarında standartlar oluşturmak ve teşvik etmekle görevli bir federal kuruluştur. NIST, kriptografik algoritmaların ve güvenlik standartlarının belirlenmesi konusunda öncü bir rol oynamaktadır. Post-Kuantum Kriptografisi için düzenlediği yarışma ile bu alandaki standartların belirlenmesine katkıda bulunmuştur.
European Telecommunications Standards Institute (ETSI): ETSI, Avrupa'da telekomünikasyon endüstrisinde standartlar oluşturan bir kuruluştur. Kriptografik protokoller ve güvenlik standartları konusunda çalışmalar yürütmektedir.
International Organization for Standardization (ISO): ISO, dünya genelinde standartları belirlemek ve bunların küresel olarak kabul görmesini sağlamak amacıyla faaliyet gösteren bir kuruluştur. ISO/IEC JTC 1 SC 27, bilgi güvenliği standartlarını belirlemekle görevlidir.

Internet Engineering Task Force (IETF): IETF, internet protokollerini ve standartlarını belirlemek için çalışan bir topluluktur. Güvenlik protokollerinin geliştirilmesi ve yaygınlaştırılması konusunda önemli bir rol oynamaktadır.
Cloud Security Alliance (CSA): CSA, bulut bilişim güvenliği konusunda standartlar oluşturmak ve bu alanda iyi uygulamaları teşvik etmek amacıyla faaliyet gösteren bir kuruluştur.
OpenID Foundation: OpenID, kimlik doğrulama ve yetkilendirme standartlarını belirleme ve destekleme konusunda faaliyet gösterir. Bu, kullanıcı kimlik bilgilerinin güvenli ve standardize edilmiş bir şekilde yönetilmesini sağlamak için önemlidir.
Trusted Computing Group (TCG): TCG, güvenli bilgi işlem platformları ve güvenlik protokollerine odaklanan bir kuruluştur. TPM (Trusted Platform Module) gibi güvenlik donanımlarının standartlaştırılmasına katkıda bulunmuştur.

Bu kuruluşlar ve inisiyatifler, kriptografik algoritmalar, güvenlik protokolleri ve bilgi güvenliği ile ilgili diğer konularda standartların belirlenmesi, geliştirilmesi ve yaygınlaştırılması için çeşitli çalışmalar yürütmektedir. Bu standartlar, endüstri genelinde güvenlik ve uyumluluk sağlamak için önemli bir rol oynamaktadır.

2.3.1.2 Yarışma ve Değerlendirme

NIST (National Institute of Standards and Technology), post-kuantum kriptografisi alanında yeni algoritmaların belirlenmesi ve standartlaştırılması amacıyla bir yarışma düzenlemiştir. Bu yarışma, post-kuantum kriptografisi alanındaki en güvenli ve uygulanabilir algoritmaların seçilmesi için bir platform sağlamaktadır. İşte NIST'in post-kuantum kriptografisi yarışma sürecinin ana hatları: NIST, post-kuantum kriptografisi yarışmasının başlamasıyla birlikte, topluluktan ve araştırmacılardan post-kuantum kriptografisi için yeni algoritmaları önermelerini isteyen bir duyuru yapar. Bu duyuru, geniş bir katılımı teşvik etmek ve çeşitli algoritmaların sunulmasını sağlamak amacı taşır. Araştırmacılar, kendi geliştirdikleri post-kuantum kriptografik algoritmalarını NIST'e sunarlar. Bu algoritmalar genellikle dijital bir formatta, önerilen standartlar ve kriptografik dayanakları ile birlikte sunulur. NIST, sunulan algoritmaları uzmanlar ve kriptografi topluluğundan oluşan bir inceleme kurulu tarafından değerlendirilmesi için yayımlar. Bu süreçte, algoritmaların matematiksel dayanakları, dayanıklılık, etkinlik ve uygulanabilirlik gibi çeşitli faktörler dikkate alınır. Değerlendirmeler sonucunda, önerilen algoritmalar hakkında açık bir tartışma süreci başlar. Araştırmacılar, algoritmalarını iyileştirebilir ve geliştirebilirler. İnceleme ve değerlendirme sürecinin ardından, NIST finalist algoritmaları seçer. Bu algoritmalar, post-kuantum kriptografisi standartları olarak kabul edilmeye adaydır. NIST, finalist algoritmalarını belirleyerek, bunları post-kuantum kriptografisi standartları olarak tanımlar. Bu standartlar, endüstri genelinde güvenlik sağlama ve uyumlu bir geçiş süreci oluşturma amacını taşır. Post-kuantum kriptografisi alanında güvenli ve etkili algoritmaların belirlenmesi ve standartlaştırılması için bir çerçeve sağlar. Ayrıca, kriptografik topluluğun geniş bir katılımını teşvik eder ve çeşitli bakış açılarını içerir, bu da standartların güvenilirliğini artırır.

2.3.1.3 Algoritmaların Seçilmesi ve Standartlaştırılması:

Algoritmaların seçilmesi ve standartlaştırılması süreci, genellikle bir dizi dikkatlice planlanmış adım içerir. Bu süreç, post-kuantum kriptografisi gibi yeni alanlarda daha da karmaşık hale gelebilir. Algoritmaların seçilmesi ve standartlaştırılması süreci:
Güvenlik: Algoritmanın kuantum bilgisayarlar dahil olmak üzere gelecekteki bilgisayar gücüne karşı dayanıklılığı.
Etkinlik: Algoritmanın performansı ve işlem hızı.
Uygulanabilirlik: Algoritmanın çeşitli uygulama senaryolarında nasıl performans gösterdiği.
Dayanıklılık: Yapılan saldırılara karşı direnç.
Araştırmacıların ve Topluluğun Katılımı:
Yarışmalar veya açık çağrılar gibi yöntemlerle araştırmacılardan ve topluluktan algoritmaların sunulmasını sağlamak.
Dış İnceleme ve Değerlendirme:
Dış uzmanlardan oluşan bir inceleme kurulu tarafından algoritmaların matematiksel dayanakları ve performansı değerlendirilir. Açık tartışma forumları ve konferanslar aracılığıyla topluluğun görüşleri alınır. Değerlendirmeler sonrasında araştırmacılara geri bildirim sağlanır.
Araştırmacılar, algoritmalarını geliştirmek için bu geri bildirimleri kullanabilir.
İnceleme kurulu ve standartlaştırma kurulu, en iyi performans gösteren ve güvenilir bulunan finalist algoritmalarını seçer. Seçilen finalist algoritmalar, belirli bir standart haline getirilir.
Standart, belirli bir standartlaştırma kuruluşu veya otorite tarafından yayımlanır. Endüstri ve diğer uygulayıcılar, yeni standartlara uyum sağlama ve mevcut sistemleri güncelleme sürecine geçer.
Eğitim ve Farkındalık:
Yeni standartlar hakkında eğitim ve bilinçlendirme süreçleri başlatılır.
Toplum ve endüstri, güvenli ve etkili kullanım için bilinçlendirilir.
Bu süreç, algoritmaların güvenlik standartlarına uygun bir şekilde belirlenmesi ve geniş bir kullanıcı tabanına yayılması için önemlidir. Post-kuantum kriptografisi gibi geleceğe yönelik alanlarda, standartlaştırma süreci, güvenliği sağlamak ve uyumlu geçiş süreçlerini yönetmek açısından kritik bir rol oynar.

3. Mevcut Güvenlik Standartlarının Post-Kuantum Dünyasında Yetersiz Kalışı

Mevcut güvenlik standartlarının post-kuantum dünyasında yetersiz kalışı, kuantum hesaplama teknolojisinin gelişmesiyle ortaya çıkan bir sorundur. Kuantum hesaplama, klasik bilgisayarların yapamadığı veya çok uzun sürede yaptığı bazı matematiksel

problemleri çok hızlı bir şekilde çözebilen bir teknolojidir. Bu teknoloji, kriptografi gibi alanlarda devrim yaratacak potansiyele sahiptir. Ancak, aynı zamanda, mevcut kriptografik protokollerin güvenliğini de tehdit etmektedir. Çünkü, kuantum hesaplamalar, şifreli verileri kırmak için kullanılabilecek algoritmalar geliştirmeyi mümkün kılmaktadır. Bu nedenle, post-kuantum dünyasında güvenliği sağlamak için yeni kriptografik standartlar ve protokoller geliştirilmesi gerekmektedir.

Post-kuantum kriptografi, kuantum hesaplamalara dayanıklı olan kriptografik algoritmaları inceleyen bir bilim dalıdır. Bu alanda, hem simetrik hem de asimetrik şifreleme yöntemleri araştırılmaktadır. Simetrik şifreleme, aynı anahtarın hem şifreleme hem de deşifreleme işlemlerinde kullanıldığı bir yöntemdir. Asimetrik şifreleme ise, farklı anahtarların şifreleme ve deşifreleme işlemlerinde kullanıldığı bir yöntemdir. Asimetrik şifreleme, genellikle kimlik doğrulama, dijital imza, anahtar dağıtımı gibi işlemlerde kullanılmaktadır.

Post-kuantum kriptografide, simetrik şifreleme yöntemlerinin kuantum hesaplamalara karşı daha dayanıklı olduğu düşünülmektedir. Bununla birlikte, simetrik şifreleme yöntemlerinin güvenliği, anahtar uzunluğuna ve anahtar yönetimine bağlıdır. Bu nedenle, post-kuantum dünyasında simetrik şifreleme yöntemlerinin kullanılması için anahtar uzunluğunun artırılması ve anahtar yönetiminin iyileştirilmesi gerekmektedir.

Asimetrik şifreleme yöntemleri ise, kuantum hesaplamalara karşı daha zayıf olduğu bilinmektedir. Çünkü, kuantum hesaplamalar, asimetrik şifreleme yöntemlerinin temelini oluşturan matematiksel problemleri çözebilmektedir. Örneğin, Shor algoritması, kuantum hesaplamalar ile büyük sayıların asal çarpanlarına ayrılmasını sağlayan bir algoritmadır. Bu algoritma, RSA gibi asimetrik şifreleme yöntemlerinin güvenliğini tehlikeye atmaktadır. Bu nedenle, post-kuantum dünyasında asimetrik şifreleme yöntemlerinin kullanılması için yeni matematiksel problemler ve algoritmalar geliştirilmesi gerekmektedir.

Post-kuantum kriptografide, çeşitli asimetrik şifreleme yöntemleri önerilmiştir. Bunlardan bazıları şunlardır:

Izgara tabanlı kriptografi: Izgara problemlerine dayanan kriptografik algoritmaları içerir. Izgara problemleri, çok boyutlu ızgaralarda noktaların konumlarını bulmayı veya değiştirmeyi içeren matematiksel problemlerdir. Bu problemler, kuantum hesaplamalar ile çözülememektedir.
Koda tabanlı kriptografi: Hata düzeltici kodlara dayanan kriptografik algoritmaları içerir. Hata düzeltici kodlar, verilerin iletimi veya depolanması sırasında oluşabilecek hataları tespit etmek ve düzeltmek için kullanılan matematiksel yöntemlerdir. Bu yöntemler, kuantum hesaplamalar ile kırılamamaktadır.
Çok değişkenli kriptografi: Çok değişkenli polinomlara dayanan kriptografik algoritmaları içerir. Çok değişkenli polinomlar, birden fazla değişken içeren cebirsel ifadelerdir. Bu ifadeler, kuantum hesaplamalar ile çözülememektedir.

Kapsayıcı kriptografi: Kapsayıcı eğrilere dayanan kriptografik algoritmaları içerir. Kapsayıcı eğriler, özel bir geometrik şekil olan eliptik eğrilerin genelleştirilmesidir. Bu eğriler, kuantum hesaplamalar ile kırılamamaktadır.
Post-kuantum kriptografide, bu ve benzeri yöntemlerin güvenliği, performansı, uygulanabilirliği ve uyumluluğu üzerinde çalışılmaktadır. Bu yöntemlerin, mevcut güvenlik standartlarının yerini alması veya onlarla birlikte kullanılması için, hem teorik hem de pratik açıdan test edilmesi ve değerlendirilmesi gerekmektedir.

Post-kuantum kriptografi, kuantum hesaplama teknolojisinin gelişmesiyle ortaya çıkan bir zorluk ve fırsattır. Bu alanda, hem akademik hem de endüstriyel araştırmalar devam etmektedir. Post-kuantum kriptografi, hem sivil hem de askeri amaçlar için önemli bir güvenlik unsuru olacaktır. Bu nedenle, post-kuantum kriptografiye yatırım yapmak ve desteklemek, geleceğin güvenliği için hayati bir önem taşımaktadır.

3.1 RSA ve ECC Algoritmalarının Zayıflıkları

RSA ve ECC algoritmaları, asimetrik şifreleme yöntemleri olarak bilinir. Asimetrik şifreleme, farklı anahtarların şifreleme ve deşifreleme işlemlerinde kullanıldığı bir yöntemdir. RSA algoritması, büyük asal sayıların çarpımına dayanır. ECC algoritması ise, eliptik eğrilerin matematiksel özelliklerine dayanır. Bu algoritmaların, kuantum hesaplamalara karşı zayıflıkları vardır. Çünkü, kuantum hesaplamalar, asimetrik şifreleme yöntemlerinin temelini oluşturan matematiksel problemleri çözebilmektedir. Örneğin, Shor algoritması, kuantum hesaplamalar ile büyük sayıların asal çarpanlarına ayrılmasını sağlayan bir algoritmadır. Bu algoritma, RSA algoritmasının güvenliğini tehlikeye atmaktadır. Benzer şekilde, Pollard rho algoritması, kuantum hesaplamalar ile eliptik eğriler üzerindeki logaritma problemini çözen bir algoritmadır. Bu algoritma, ECC algoritmasının güvenliğini tehlikeye atmaktadır. Bu nedenle, RSA ve ECC algoritmalarının, kuantum hesaplamalara dayanıklı olmayan matematiksel problemlere dayandığı söylenebilir.

RSA ve ECC algoritmalarının zayıflıkları, sadece kuantum hesaplamalar ile sınırlı değildir. Bu algoritmaların, uygulama, tasarım, parametre seçimi, anahtar yönetimi, saldırgan modeli gibi çeşitli faktörlere bağlı olarak başka zayıflıkları da olabilir. Örneğin, RSA algoritmasında, anahtar uzunluğu, şifreleme hızı, güvenlik seviyesi gibi parametrelerin doğru seçilmesi gerekmektedir. Aksi takdirde, RSA algoritması, kaba kuvvet, ortak bölen, Wiener, Coppersmith gibi saldırılara karşı savunmasız olabilir. ECC algoritmasında ise, eliptik eğri seçimi, koordinat sistemi, nokta çarpımı, nokta sıkıştırma gibi işlemlerin doğru yapılması gerekmektedir. Aksi takdirde, ECC algoritması, kaba kuvvet, indirgeme, Weil eşleniği, MOV, Semaev, Smart gibi saldırılara karşı savunmasız olabilir.

RSA ve ECC algoritmalarının zayıflıkları, güvenli iletişim için önemli bir sorundur. Bu nedenle, bu algoritmaların güvenliğini artırmak için çeşitli yöntemler geliştirilmiştir. Örneğin, RSA algoritmasının güvenliğini artırmak için, anahtar uzunluğunu artırmak, Çin Kalan Teoremi, Montgomery Çarpımı, Kare-Kök Algoritması gibi hızlandırma teknikleri kullanmak, OAEP, PSS, RSA-KEM gibi şifreleme ve imza şemaları kullanmak, CRT, Blinding, Fault Detection gibi saldırı önleme teknikleri

kullanmak mümkündür. ECC algoritmasının güvenliğini artırmak için ise, güvenli eliptik eğriler seçmek, proje, Jacobian, Chudnovsky gibi hızlı koordinat sistemleri kullanmak, endomorfizm, GLV, GLS gibi hızlandırma teknikleri kullanmak, ECIES, ECDSA, ECDH gibi şifreleme ve imza şemaları kullanmak, Side Channel, Fault Injection, Lattice gibi saldırı önleme teknikleri kullanmak mümkündür.

RSA ve ECC algoritmalarının zayıflıkları, kriptografi alanında sürekli araştırılan ve geliştirilen bir konudur. Bu algoritmaların, hem teorik hem de pratik açıdan test edilmesi ve değerlendirilmesi gerekmektedir. Bu algoritmaların, hem sivil hem de askeri amaçlar için önemli bir güvenlik unsuru olduğu unutulmamalıdır. Bu nedenle, RSA ve ECC algoritmalarına yatırım yapmak ve desteklemek, geleceğin güvenliği için hayati bir önem taşımaktadır.

3.2 Kuantum Salındığındaki Kriptografik Algoritmaların Güvenliği

Kuantum salındığındaki kriptografik algoritmaların güvenliği, kuantum bilgisayarların gelişmesiyle ortaya çıkan bir konudur. Kuantum bilgisayarlar, klasik bilgisayarlardan farklı olarak kuantum mekaniğinin yasalarını kullanarak bazı matematiksel problemleri çok hızlı bir şekilde çözebilen bilgisayarlardır. Bu bilgisayarlar, kriptografi gibi alanlarda devrim yaratacak potansiyele sahiptir. Ancak, aynı zamanda, mevcut kriptografik protokollerin güvenliğini de tehdit etmektedir. Çünkü, kuantum bilgisayarlar, şifreli verileri kırmak için kullanılabilecek algoritmalar geliştirmeyi mümkün kılmaktadır. Bu nedenle, kuantum salındığındaki kriptografik algoritmaların güvenliği, hem sivil hem de askeri amaçlar için önemli bir sorundur.

Kuantum salındığındaki kriptografik algoritmaların güvenliği, iki temel yöntemle sağlanmaya çalışılmaktadır. Bunlardan ilki, kuantum hesaplamalara dayanıklı kriptografik algoritmalar geliştirmektir. Bu algoritmalar, kuantum bilgisayarların çözemediği veya çok zor çözdüğü matematiksel problemlere dayanmaktadır. Bu alanda, hem simetrik hem de asimetrik şifreleme yöntemleri araştırılmaktadır. Simetrik şifreleme, aynı anahtarın hem şifreleme hem de deşifreleme işlemlerinde kullanıldığı bir yöntemdir. Asimetrik şifreleme ise, farklı anahtarların şifreleme ve deşifreleme işlemlerinde kullanıldığı bir yöntemdir. Asimetrik şifreleme, genellikle kimlik doğrulama, dijital imza, anahtar dağıtımı gibi işlemlerde kullanılmaktadır. Kuantum hesaplamalara dayanıklı kriptografik algoritmaların güvenliği, performansı, uygulanabilirliği ve uyumluluğu üzerinde çalışılmaktadır. Bu algoritmaların, mevcut güvenlik standartlarının yerini alması veya onlarla birlikte kullanılması için, hem teorik hem de pratik açıdan test edilmesi ve değerlendirilmesi gerekmektedir.

Kuantum salındığındaki kriptografik algoritmaların güvenliği, ikinci bir yöntem olan kuantum anahtar dağıtımı ile de sağlanmaya çalışılmaktadır. Kuantum anahtar dağıtımı, kuantum mekaniğinin yasalarını kullanarak iki taraf arasında güvenli bir şekilde anahtar paylaşımı yapmayı amaçlayan bir yöntemdir. Bu yöntem, kuantum mekaniğinin temel özelliklerinden olan süperpozisyon ve ölçüm yapma prensiplerini kullanmaktadır. Süperpozisyon, bir kuantum sisteminin birden fazla durumda aynı anda bulunabilmesi anlamına gelir. Ölçüm yapma ise, bir kuantum sisteminin

durumunu belirlemek için yapılan işlemdir. Bu işlem, kuantum sisteminin süperpozisyon durumunu bozar ve belirli bir duruma indirger. Kuantum anahtar dağıtımı, bu prensipleri kullanarak, iki taraf arasında rastgele bir anahtar oluşturur ve bu anahtarın gizliliğini ve bütünlüğünü korur. Bu yöntem, kuantum hesaplamalara karşı dayanıklı olduğu gibi, klasik hesaplamalara karşı da dayanıklıdır. Kuantum anahtar dağıtımının güvenliği, teorik olarak kanıtlanmıştır. Ancak, pratikte, bu yöntemin uygulanması, teknik ve mali zorluklar içermektedir. Bu nedenle, kuantum anahtar dağıtımının, yaygın bir şekilde kullanılması için, hem fiziksel hem de yazılımsal açıdan geliştirilmesi gerekmektedir.

Kuantum salındığındaki kriptografik algoritmaların güvenliği, kuantum bilgisayarların gelişmesiyle ortaya çıkan bir zorluk ve fırsattır. Bu alanda, hem akademik hem de endüstriyel araştırmalar devam etmektedir. Kuantum salındığındaki kriptografik algoritmaların güvenliği, hem sivil hem de askeri amaçlar için önemli bir güvenlik unsuru olacaktır. Bu nedenle, kuantum salındığındaki kriptografik algoritmaların güvenliğine yatırım yapmak ve desteklemek, geleceğin güvenliği için hayati bir önem taşımaktadır.

3.3 Mevcut Kripto Sistemlerinin Post-Kuantum Dünyasında Geçerliliği

Mevcut kripto sistemlerinin post-kuantum dünyasında geçerliliği, kuantum bilgisayarların gelişmesiyle ortaya çıkan bir sorundur. Kuantum bilgisayarlar, klasik bilgisayarlardan farklı olarak kuantum mekaniğinin yasalarını kullanarak bazı matematiksel problemleri çok hızlı bir şekilde çözebilen bilgisayarlardır. Bu bilgisayarlar, kriptografi gibi alanlarda devrim yaratacak potansiyele sahiptir. Ancak, aynı zamanda, mevcut kriptografik protokollerin güvenliğini de tehdit etmektedir. Çünkü, kuantum bilgisayarlar, şifreli verileri kırmak için kullanılabilecek algoritmalar geliştirmeyi mümkün kılmaktadır. Bu nedenle, mevcut kripto sistemlerinin post-kuantum dünyasında geçerli olup olmadığı, hem sivil hem de askeri amaçlar için önemli bir sorudur.

Mevcut kripto sistemleri, genellikle simetrik veya asimetrik şifreleme yöntemleri olarak sınıflandırılabilir. Simetrik şifreleme, aynı anahtarın hem şifreleme hem de deşifreleme işlemlerinde kullanıldığı bir yöntemdir. Asimetrik şifreleme ise, farklı anahtarların şifreleme ve deşifreleme işlemlerinde kullanıldığı bir yöntemdir. Asimetrik şifreleme, genellikle kimlik doğrulama, dijital imza, anahtar dağıtımı gibi işlemlerde kullanılmaktadır.

Mevcut kripto sistemlerinin post-kuantum dünyasında geçerliliği, kuantum bilgisayarların bu yöntemleri kırma kapasitesine bağlıdır. Kuantum bilgisayarlar, asimetrik şifreleme yöntemlerinin temelini oluşturan matematiksel problemleri çözebilmektedir. Örneğin, Shor algoritması, kuantum bilgisayarlar ile büyük sayıların asal çarpanlarına ayrılmasını sağlayan bir algoritmadır. Bu algoritma, RSA, ECC, ElGamal gibi asimetrik şifreleme yöntemlerinin güvenliğini tehlikeye atmaktadır. Bu

nedenle, mevcut asimetrik şifreleme yöntemleri, post-kuantum dünyasında geçerli olmayacaktır. Simetrik şifreleme yöntemleri ise, kuantum bilgisayarların çözemediği veya çok zor çözdüğü matematiksel problemlere dayanmaktadır. Örneğin, Grover algoritması, kuantum bilgisayarlar ile bir veritabanında arama yapmayı hızlandıran bir algoritmadır. Bu algoritma, AES, DES, RC4 gibi simetrik şifreleme yöntemlerinin güvenliğini azaltmaktadır. Ancak, bu yöntemlerin güvenliği, anahtar uzunluğuna ve anahtar yönetimine bağlıdır. Bu nedenle, mevcut simetrik şifreleme yöntemleri, post-kuantum dünyasında geçerli olabilir, ancak anahtar uzunluğunun artırılması ve anahtar yönetiminin iyileştirilmesi gerekmektedir. Mevcut kripto sistemlerinin post-kuantum dünyasında geçerliliği, hem teorik hem de pratik açıdan test edilmesi ve değerlendirilmesi gereken bir konudur. Bu konuda, hem akademik hem de endüstriyel araştırmalar devam etmektedir. Ayrıca, post-kuantum kriptografi adı verilen, kuantum hesaplamalara dayanıklı kriptografik algoritmalar geliştirmek için çeşitli yöntemler önerilmiştir. Bu yöntemler, hem simetrik hem de asimetrik şifreleme yöntemlerini içermektedir. Bu yöntemlerin, mevcut kripto sistemlerinin yerini alması veya onlarla birlikte kullanılması için, hem teorik hem de pratik açıdan test edilmesi ve değerlendirilmesi gerekmektedir.

Mevcut kripto sistemlerinin post-kuantum dünyasında geçerliliği, kuantum bilgisayarların gelişmesiyle ortaya çıkan bir zorluk ve fırsattır. Bu alanda, hem akademik hem de endüstriyel araştırmalar devam etmektedir. Mevcut kripto sistemlerinin post-kuantum dünyasında geçerliliği, hem sivil hem de askeri amaçlar için önemli bir güvenlik unsuru olacaktır. Bu nedenle, mevcut kripto sistemlerinin post-kuantum dünyasında geçerliliğine yatırım yapmak ve desteklemek, geleceğin güvenliği için hayati bir önem taşımaktadır.

3.4 Güvenlik Standartlarının Gelecekteki Yönelimleri ve İhtiyaçlar

Post kuantum kriptografi alanında güvenlik standartlarının gelecekteki yönelimleri ve ihtiyaçlar, kuantum bilgisayarların geleneksel kriptografik sistemleri tehdit etmesi nedeniyle önemli bir araştırma konusudur. Post kuantum kriptografi, kuantum bilgisayarların saldırılarına karşı dayanıklı olan kriptografik algoritmaları ve protokolleri içerir. Post kuantum kriptografi, aşağıdaki alt alanlara ayrılabilir:

Kuantum anahtar dağıtımı: Kuantum mekaniğinin temel prensiplerini kullanan, alıcı ve gönderici arasında gizli bir anahtar oluşturmak ve paylaşmak için bir yöntem. Kuantum anahtar dağıtımı, Heisenberg'in belirsizlik ilkesine dayanır ve herhangi bir dinleme veya müdahale girişimini tespit edebilir.
Kuantum sonrası şifreleme: Kuantum bilgisayarların çözemeyeceği matematiksel problemlere dayanan, geleneksel bilgisayarlarla uygulanabilen kriptografik algoritmalar. Kuantum sonrası şifreleme, uzun anahtar imzaları, hibrit kriptografi yaklaşımları, ızgara tabanlı, kod tabanlı, çok değişkenli, örgü tabanlı, imza tabanlı ve izomorfizm tabanlı gibi farklı teknikler kullanır.

Kuantum sonrası güvenlik protokolleri: Kuantum sonrası şifreleme algoritmalarını kullanan, veri iletişimi, kimlik doğrulama, dijital imza, güvenli çoklu parti hesaplama, sıfır bilgi kanıtı gibi güvenlik hizmetleri sağlayan protokoller. Kuantum sonrası güvenlik protokolleri, mevcut güvenlik standartlarıyla uyumlu olmak ve performans, güvenilirlik, ölçeklenebilirlik gibi kriterleri karşılamak için geliştirilmektedir.
Post kuantum kriptografi alanında güvenlik standartlarının gelecekteki yönelimleri ve ihtiyaçları, kuantum bilgisayarların gelişimi, kuantum sonrası kriptografik algoritmaların analizi ve testi, kuantum sonrası kriptografik çözümlerin uygulama ve entegrasyonu gibi konuları kapsamaktadır. Bu alanda, akademik, endüstriyel ve devlet kuruluşları arasında işbirliği ve bilgi alışverişi önemlidir. Ayrıca, kuantum sonrası kriptografi alanında ulusal ve uluslararası standartlar belirlemek ve uygulamak için çalışmalar devam etmektedir

Post kuantum kriptografi alanında güvenlik standartları belirleme çalışmaları, kuantum bilgisayarların geleneksel kriptografik sistemleri kırabileceği gerçeğiyle karşı karşıya kalan araştırmacılar, endüstriler ve devletler tarafından yürütülmektedir. Bu çalışmaların amacı, kuantum bilgisayarların saldırılarına karşı dayanıklı olan kuantum sonrası kriptografik algoritmaları ve protokolleri geliştirmek, test etmek, standartlaştırmak ve uygulamaktır. Bu alanda, ulusal ve uluslararası kuruluşlar arasında işbirliği ve koordinasyon önemlidir.

Post kuantum kriptografi alanında güvenlik standartları belirleme çalışmalarının önde gelen kuruluşlarından biri, Ulusal Standartlar ve Teknoloji Enstitüsü (NIST)'dir. NIST, 2016 yılında kuantum sonrası kriptografi standartları oluşturma sürecini başlatmış ve bu süreçte akademik, endüstriyel ve devlet kuruluşlarından gelen 69 aday algoritmayı değerlendirmiştir. NIST, 2020 yılında bu algoritmaları 15'e indirmiş ve bunları üçüncü turda daha fazla test etmek üzere seçmiştir. NIST, 2022 yılında kuantum sonrası kriptografi standartlarını ilan etmeyi planlamaktadır.

Post kuantum kriptografi alanında güvenlik standartları belirleme çalışmalarına katılan diğer kuruluşlar arasında, Avrupa Birliği (EU), Avrupa Telekomünikasyon Standartları Enstitüsü (ETSI), Uluslararası Elektroteknik Komisyonu (IEC), Uluslararası Standartlar Örgütü (ISO), Uluslararası Telekomünikasyon Birliği (ITU), Uluslararası Kuantum Güvenliği Ağı (IQNet) gibi uluslararası kuruluşlar, ayrıca Çin, Japonya, Güney Kore, Kanada, Almanya, Fransa, İngiltere gibi ülkelerin kendi ulusal kuruluşları sayılabilir.

Post kuantum kriptografi alanında güvenlik standartları belirleme çalışmalarına örnek olarak, aşağıdaki projeler ve girişimler verilebilir:

Thales, kuantum sonrası kriptografi alanında aktif olarak araştırma ve geliştirme (Ar-Ge) çalışmaları yürütmektedir. Thales, kuantum sonrası kriptografi alanında yeniliği teşvik etmek ve bilgi alışverişini sağlamak için akademik kurumlar, araştırma kuruluşları ve endüstri ortaklarıyla aktif olarak işbirliği yapmaktadır. Thales'in katıldığı projeler ve girişimler arasında, ilk başarılı kuantum sonrası telefon

görüşmesine pilotluk yapmak, PQC imza tokenları, Lightway post-kuantum koruma, WolfSSL ile post-kuantum şifreleme gibi örnekler bulunmaktadır.
PQCRYPTO, Avrupa Birliği tarafından finanse edilen ve kuantum sonrası kriptografi alanında araştırma ve eğitim yapan bir konsorsiyumdur. PQCRYPTO, kuantum sonrası kriptografi alanında güvenli, verimli ve pratik algoritmalar geliştirmeyi ve bunları yazılım ve donanım uygulamalarına entegre etmeyi amaçlamaktadır. PQCRYPTO, kuantum sonrası kriptografi alanında standartlar oluşturmak için NIST ile işbirliği yapmaktadır.
Open Quantum Safe (OQS), kuantum sonrası kriptografi alanında açık kaynaklı yazılım geliştiren bir proje ve girişimdir. OQS, kuantum sonrası kriptografi algoritmalarını ve protokollerini test etmek, değerlendirmek ve uygulamak için araçlar ve kütüphaneler sunmaktadır. OQS, kuantum sonrası kriptografi alanında standartlar oluşturmak için NIST ile işbirliği yapmaktadır.

NIST'in kuantum sonrası kriptografi standartları oluşturma süreci, aşağıdaki adımları içeriyor:

İlk adım: NIST, 2016 yılında kuantum sonrası kriptografi standartları oluşturma sürecini başlatarak, akademik, endüstriyel ve devlet kuruluşlarından kuantum sonrası kriptografik algoritmaların önerilmesini istedi1. NIST, bu algoritmaların güvenlik, verimlilik ve uygulanabilirlik açısından değerlendirileceğini ve sonunda kuantum sonrası şifreleme ve dijital imza standartları belirleyeceğini duyurdu.
İkinci adım: NIST, 2017 yılında 69 aday algoritmanın başvurusunu aldı ve bunları ilk turda değerlendirmeye aldı2. NIST, bu algoritmaları farklı kategorilere ayırdı: kuantum sonrası anahtar kurulumu, kuantum sonrası şifreleme, kuantum sonrası dijital imza ve kuantum sonrası hash tabanlı imza.
Üçüncü adım: NIST, 2019 yılında ilk turda değerlendirilen 69 algoritmadan 26 tanesini ikinci turda daha fazla test etmek üzere seçti2. NIST, bu algoritmaları daha detaylı bir şekilde güvenlik, verimlilik, uygulanabilirlik, uyumluluk ve esneklik açısından inceledi ve geri bildirimler topladı.
Dördüncü adım: NIST, 2020 yılında ikinci turda değerlendirilen 26 algoritmadan 15 tanesini üçüncü turda son testlere tabi tutmak üzere seçti2. NIST, bu algoritmaları daha da optimize etmek, güvenlik analizlerini güncellemek, performans ölçümlerini yapmak ve uygulama senaryolarını göstermek için çalışmalar yaptı.
Beşinci adım: NIST, 2022 yılında üçüncü turda değerlendirilen 15 algoritmadan son seçimleri yaparak, kuantum sonrası kriptografi standartlarını ilan etmeyi planlıyor2. NIST, bu standartları belirlerken, kuantum sonrası kriptografi alanındaki gelişmeleri, geri bildirimleri, ihtiyaçları ve beklentileri dikkate alacak.

SONUÇ

Kuantum kriptografisi, günümüzdeki bilgi güvenliği standartlarına getirdiği devrim niteliğindeki değişikliklerle, gelecekteki dijital iletişim sistemlerini şekillendirecek önemli bir yapı taşı olmaya adaydır. Bu yenilikçi teknoloji, klasik

kriptografinin karşılaştığı bazı temel zorlukları aşarak, bilgi güvenliği alanında çığır açan bir çözüm sunmaktadır. Gelecekte, kuantum kriptografisinin gelişimi ile birlikte, şifreleme algoritmaları üzerindeki klasik tehditlerin ötesine geçilerek daha güvenilir bir dijital dünya inşa edilebilecektir.

Ancak, bu potansiyel avantajlara rağmen, kuantum kriptografisinin benimsenmesiyle birlikte yeni güvenlik zorlukları ve standartlarının ortaya çıkması kaçınılmazdır. Bu nedenle, gelecekteki güvenlik standartlarını belirlemek ve sürdürmek için küresel bir işbirliği ve standardizasyon çabası gereklidir. Kuantum kriptografisi, bilgi güvenliği ekosistemini dönüştürme potansiyeline sahip olabilir, ancak bu dönüşümü etkili bir şekilde yönetmek ve sürdürmek, endüstri, araştırma ve düzenleyici kurumlar arasında koordinasyon ve işbirliği gerektirir. Gelecekteki güvenlik standartları, bu teknolojinin getirdiği yenilikleri ve meydan okumaları kucaklayarak, dijital dünyamızı daha güvenli ve dirençli hale getirmek adına sağlam bir temel oluşturacaktır.

Kuantum kriptografisinin güvenlik paradigmasındaki bu devrim, özellikle kuantum anahtar dağıtımı ve kuantum güvenli şifreleme gibi temel teknolojilerin geliştirilmesiyle mümkün olmuştur. Ancak, bu teknolojilerin günlük uygulamalarda geniş çapta kullanılabilir hale gelmesi için bir dizi teknik, ekonomik ve politik engelin aşılması gerekmektedir. Standartlar oluşturulmalı, cihazlar geliştirilmeli ve endüstriler arasında kapsamlı bir uyum sağlanmalıdır. Kuantum kriptografisi, sadece bireysel kullanıcıların değil, aynı zamanda devletlerin ve büyük şirketlerin de bilgi güvenliği stratejilerini kökten değiştirebilir. Ancak, bu teknolojinin getirdiği avantajlarla birlikte, bilgi güvenliği uzmanlarının, etik uzmanlarının ve hukukçuların da aktif bir rol oynaması gerekmektedir. Özellikle, kuantum bilgisayarlarının güvenlik alanında nasıl bir tehdit oluşturabileceği ve bu tehditlere karşı nasıl savunma mekanizmaları geliştirilebileceği konularında derinlemesine çalışmalar ve düzenlemeler gerekmektedir.

Sonuç olarak, kuantum kriptografisi, bilgi güvenliğimizi daha da güçlendirecek ve gelecekteki dijital iletişimimizi daha güvenli kılacak potansiyel bir teknolojidir. Ancak bu potansiyeli gerçekleştirmek ve güvenlik standartlarını etkin bir şekilde belirlemek, küresel bir çaba ve uzun vadeli bir strateji gerektirecektir. Bu teknolojiyi başarıyla benimsemek ve yönetmek, dijital geleceğimizi daha güvenli, şeffaf ve dirençli bir şekilde inşa etmemize olanak tanıyacaktır."

KAYNAKÇA

1- Bennett, C. H., & Brassard, G. (1984). Quantum cryptography: Public key distribution and coin tossing. Proceedings of IEEE International Conference on Computers, Systems and Signal Processing, 175-179.

2- Gisin, N., Ribordy, G., Tittel, W., & Zbinden, H. (2002). Quantum cryptography. Reviews of Modern Physics, 74(1), 145-195.

3- Shor, P. W. (1997). Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. SIAM Journal on Computing, 26(5), 1484-1509.

4- Şahinoğlu, G. (2018). Kriptoloji ve Kuantum Kriptografisi. Türk Bilgisayar ve Matematik Eğitimi Dergisi, 9(2), 363-378.

5- Ekert, A. K. (1991). Quantum cryptography based on Bell's theorem. Physical Review Letters, 67(6), 661-663.

6- Lo, H. K., & Chau, H. F. (1997). Unconditional security of quantum key distribution over arbitrarily long distances. Science, 283(5410), 2050-2056.

7- Akgül, G., & Yanardağ, M. (2014). Kuantum Kriptografisi: Temeller ve Uygulamalar. Bilgi Güvenliği Dergisi, 5(1), 27-43.

8- Büyükköse, S. (2019). Kuantum Bilgisayarlar ve Kriptografi Üzerine Etkileri. Fen Bilimleri Enstitüsü Dergisi, 6(1), 123-136.

9- Scarani, V., Bechmann-Pasquinucci, H., Cerf, N. J., Dušek, M., Lütkenhaus, N., & Peev, M. (2009). The security of practical quantum key distribution. Reviews of Modern Physics, 81(3), 1301.

10- Gisin, N., & Thew, R. (2007). Quantum communication. Nature Photonics, 1(3), 165-171.

11- Öztürk, N., & Çetinkaya, C. (2020). Kuantum Kriptografisi ve Güvenlik Uygulamaları. Bilgisayar Bilimleri ve Mühendisliği Dergisi, 8(2), 287-298.

12- Mosca, M., & Ekert, A. (1999). The hidden subgroup problem and eigenvalue estimation on a quantum computer. Proceedings of the 30th Annual ACM Symposium on Theory of Computing, 596-604.

13- Atalay, T., & Kılıç, İ. H. (2017). Kuantum Bilgisayarlar ve Kuantum Kriptografisi. Bilgi Güvenliği Dergisi, 8(2), 49-60.

14- Scarani, V., & Renner, R. (2008). Quantum cryptography with finite resources: Untrusted devices. Physical Review Letters, 100(20), 200501.

15- National Institute of Standards and Technology (NIST). (2021). Post-Quantum Cryptography Standardization. [Online] https://csrc.nist.gov/projects/post-quantum-cryptography