T.C.
İSTANBUL AYDIN ÜNİVERSİTESİ
LİSANSÜSTÜ EĞİTİM ENSTİTÜSÜ

MAKİNE ÖĞRENMESİ ALGORİTMALARININ KAD/QKD ARTIK BİT'LERİNİN GERİ KAZANIMINDA KULLANIMI

DOKTORA TEZİ

Faruk TAKAOĞLU

Bilgisayar Mühendisliği Anabilim Dalı
Bilgisayar Mühendisliği Programı

HAZİRAN, 2022

T.C.
İSTANBUL AYDIN ÜNİVERSİTESİ
LİSANSÜSTÜ EĞİTİM ENSTİTÜSÜ

MAKİNE ÖĞRENMESİ ALGORİTMALARININ KAD/QKD ARTIK BİT'LERİNİN GERİ KAZANIMINDA KULLANIMI

DOKTORA TEZİ

Faruk TAKAOĞLU
(Y1615.610007)

Bilgisayar Mühendisliği Anabilim Dalı
Bilgisayar Mühendisliği Programı

Tez Danışmanı: Prof. Dr. Naim Mahmood Musleh AJLOUNI
Eş Danışman: Prof. Dr. Ali Güneş

HAZİRAN, 2022

ONAY FORMU

ONUR SÖZÜ

Doktora tezi olarak sunduğum "Makine Öğrenmesi Algoritmalarının KAD/QKD Artık Bit'lerinin Geri Kazanımında Kullanımı" adlı çalışmanın, tezin proje safhasından sonuçlanmasına kadarki bütün süreçlerde bilimsel ahlak ve geleneklere aykırı düşecek bir yardıma başvurulmaksızın yazıldığını ve yararlandığım eserlerin Bibliyografya'da gösterilenlerden oluştuğunu, bunlara atıf yapılarak yararlanılmış olduğunu belirtir ve onurumla beyan ederim. (15/06/2022)

Faruk TAKAOĞLU

ÖNSÖZ

Gerçekleştirme imkânı bulduğumuz bu tez çalışmasında günümüz ve geleceğin teknolojisi olan kuantum hesaplama teknolojisi, bir başka deyişle kuantum bilgisayarlarında, kuantum anahtar dağıtımı noktasında görülen artık bitlerle ilgili bir iyileştirme yapılması sağlanmıştır. Yapay zekâ çalışma konusunun alt başlığı olan makine öğrenmesi algoritmalarından faydalanılarak kuantum anahtar dağıtımında görülen artık bitlerin geri kazanımında olumlu sonuçlar elde edilmiştir. Bu sürecin gerçekleştirilmesinde çok büyük emekleri olan başta doktora tez danışmanı hocam kıymetli Prof. Dr. Naim Mahmood Musleh Ajlouni'ye özel teşekkürlerimi sunmak istiyorum. Tez konusu seçimi sürecinden başlayarak son aşamaya kadar çalışmama kıymetli görüşleriyle katkılar sağlayan çok değerli hocalarım Prof. Dr. Zafer ASLAN ve Dr. Ali Hamitoğlu'na teşekkürlerimi sunmak istiyorum. Lisans, Yüksek Lisans ve Doktora eğitimimi tamamlama imkânı bulduğum İstanbul Aydın Üniversitesi Bilgisayar Mühendisliği Bölümünün kıymetli Bölüm Başkanı Prof. Dr. Ali Güneş hocama tüm yükseköğretim sürecimde vermiş olduğu destekler için teşekkür ve saygılarımı sunmak istiyorum. Son olarak kıymetli aileme bu süreçte göstermiş oldukları destekler için çok teşekkür ediyor, hazırlamış olduğum doktora tezimi anneme ithaf ediyorum.

Haziran, 2022 Faruk TAKAOĞLU

MAKİNE ÖĞRENMESİ ALGORİTMALARININ KAD/QKD ARTIK BİT'LERİNİN GERİ KAZANIMINDA KULLANIMI

ÖZET

Tez çalışmamızda kuantum anahtar dağıtımı protokollerinde görülen anahtar paylaşımı esnasında kaybedilen bit miktarlarında azaltma bir başka deyişle iyileştirme yapılması amaçlanmıştır. Geçen 2 yıllık süreçte kuantum anahtar dağıtımı algoritmaları ayrıntılı bir şekilde incelenmiştir. Seçilen protokollerin kuantum anahtar dağıtımında karşılaştıkları kayıp ya da artık diye adlandırılabilecek bitleri hesaplanmış ve bunların yapay zekâ algoritmalarıyla azaltılması, iyileştirilmesi amaçlanmıştır. Makine öğrenmesi algoritmaları tez çalışması sürecinde tek tek incelenmiş ve kuantum anahtar dağıtımı protokollerine uygulanmıştır. Elde edilen sonuçlar tezimizin ilgili bölümlerinde paylaşılmıştır. Uyumsuz olan makine öğrenmesi algoritmaları sebepleriyle birlikte paylaşılmıştır. Olumlu sonuçlar elde edilen algoritmalar ve başarı yüzdelerine göre daha iyi olanları ön plana çıkartılmış ve paylaşılmıştır. Ayrıca tez çalışmamızda blokzincir teknolojisi de dikkate alınmıştır. Artık bitlerin geri kazandırılmasında makine öğrenmesi algoritmalarının yanı sıra yenilikçi çözümlerden de faydalanılmıştır. Blokzincir teknolojisi kuantum anahtar dağıtımı protokollerinde görülen veri iletim kanalı olarak kullanılmış ve hattan kaynaklanan kayıpların önüne geçilmiştir. Bu sayede tezimizde makine öğrenmesi algoritmaları sayesinde daha verimli ve iyileştirilmiş sonuçlar elde edilirken blokzincir teknolojisinin kullanılması durumunda da artık bitlerde daha da iyileştirme elde edildiği görülmüştür.

Anahtar Kelimeler: Kuantum Anahtar Dağıtımı, BB84, E91, Makine Öğrenmesi

USE OF MACHINE LEARNING ALGORITHMS IN RECOVERY OF KAD/QKD ARTICLE BITS

ABSTRACT

In our thesis, it is aimed to reduce the amount of bits lost during key sharing seen in quantum key distribution protocols, in other words to improve. In the last 2 years, quantum key distribution algorithms have been studied in detail. The bits that can be called lost or residual that the selected protocols encounter in quantum key distribution are calculated and it is aimed to reduce and improve them with artificial intelligence algorithms. Machine learning algorithms were examined one by one during the thesis work and applied to quantum key distribution protocols. The results obtained are shared in the relevant sections of our thesis. Incompatible machine learning algorithms are shared with their reasons. Algorithms with positive results and better ones according to their success rates were highlighted and shared. In addition, blockchain technology was also taken into account in our thesis. In addition to machine learning algorithms, innovative solutions have also been used to recover bits. Blockchain technology was used as the data transmission channel seen in quantum key distribution protocols and the losses caused by the line were prevented. In this way, while more efficient and improved results are obtained thanks to machine learning algorithms in our thesis, it has been seen that further improvement in bits is achieved in the case of using blockchain technology.

Keywords: Quantum Key Distribution, BB84, E91, Machine Learning

İÇİNDEKİLER

Sayfa

ÖNSÖZ ..... **iii**
ÖZET ..... **v**
ABSTRACT ..... **vii**
İÇİNDEKİLER ..... **ix**
KISALTMALAR ..... **xi**
ÇİZELGELER LİSTESİ ..... **xiii**
ŞEKİLLER LİSTESİ ..... **xv**
I. GİRİŞ **1**
A. Literatür Taraması 6
B. Problem Tanıtımı 26
C. Önerilen Yöntem 27
D. Tezin Bilime Katkısı 27
II. BİLGİ GÜVENLİĞİ VE KRİPTOLOJİ **29**
A. Kriptoloji 30
B. Şifreleme Anahtarı Problemleri 33
C. Kuantum Anahtar Dağıtımı 35
1. Kuantum Terminolojisi 36
2. Güncel Sınırlamalar ve Problemler 41
D. Kuantum Anahtar Dağıtımı Protokolleri 43
1. BB84 Protokolü 43
2. E91 Protokolü 47
3. B92 Protokolü 49
4. Diğer Protokoller 50
E. Kuantum Anahtar Dağıtımı Protokolleri Avantajları ve Dezavantajları 52
F. Kuantum Anahtar Dağıtımı Protokolleri Çıkarımları 53
G. Kuantum Anahtar Dağıtımı Protokollerine Önerilen Makine Öğrenmesi Çözümü 54

1. Genel Açıklama 55
2. Yapay Zeka Mimarisi 55
3. Veritabanı Mimarisi 57
4. kNN Yöntemi 58
5. Naïve Bayes Yöntemi 62
6. Karar Ağacı Yöntemi 65
7. Diskriminant Analizi Yöntemi 69
8. Diğer Yöntemler 73
9. Yapay Sinir Ağları 75
H. Test ve Sonuçlar 83
1. kNN Sonuçları 83
2. Naïve Bayes Sonuçları 95
3. Karar Ağacı Sonuçları 97
4. Diskriminant Analizi Sonuçları 99
5. Yapay Sinir Ağı Sonuçları 100
I. Yapay Zekâ Tahmin Yöntemlerinin Kullanımı ve Elde Edilen Çıkarımlar 103
III. ÖNERİLEN ANAHTAR DAĞITIMI YÖNTEMİ 107
A. Blokzincir Genel Tanımı 107
B. Önerilen Blokzincir Tabanlı Sonuç 112
C. Çıkarımlar 115
IV. ANALİZ VE TARTIŞMA 117
V. SONUÇ VE ÖNERİLER 121
VI. KAYNAKÇA 123
ÖZGEÇMİŞ 135

KISALTMALAR

.txt : Text (Metin)

AES : Advanced Encryption Standard (İleri Şifreleme Standardı)

AHCI : Arts and Humanities Citation Index (Sanat ve Beşerî Bilimler Atıf Dizini)

BPP : Bits Per Pixel (Piksel Başına Bit Sayısı)

BTC : Bitcoin

CNN : Convolutional Neural Network (Evrişimli Sinir Ağı)

CP-ABE : Ciphertext-Policy Attribute-Based Encryption (Şifreli Metin İlkesi Öznitelik Tabanlı Şifreleme)

DCT : Discrete Cosine Transform (Ayrık Kosinüs Dönüşümü)

DES : Data Encryption Standard (Veri Şifreleme Standardı)

DWT : Discreate Wavelet Transform (Ayrık Dalgacık Dönüşümü)

ETH : Ethereum

GAN : General Adversarial Network (Üretken Düşman Ağları)

IoT : Internet of Things (Nesnelerin İnterneti)

KB : Kilobayt

LFSR : Linear Feedback Shift Register (Doğrusal Geri Besleme Kaydırma Kaydı)

MB : Megabayt

MSE : Mean Squared Error (Ortalama Kare Hatası)

NCC : Normalized Cross Correlation (Normalleştirilmiş Çapraz Korelasyon)

NFC : Near Field Communication (Yakın Alan İletişimi)

nm : Nanometre

OMR : Optical Mark Recognition (Optik İşaret Tanıma)

OTA : Ozyavas-Takaoglu-Ajlouni

OTP : One Time Pad (Tek Seferlik Şerit)

PEKS : Public Key Encryption with Keyword Search (Anahtar Kelime Arama ile Açık Anahtar Şifreleme)

PoW : Proof-of-Work (İş Kanıtı)

PoW-BC : Proof-of-Work-and-Block-Compression (İş Kanıtı ve Blok Sıkıştırma)

PSNR : Peak Signal Noise Ratio (Tepe Sinyal Gürültü Oranı)

Qbit : Kubit

RBML : Rule Based Machile Learning (Kural Tabanlı Makine Öğrenimi)

RSA : Rivest-Shamir-Adleman

SCI : Science Citation Index (Bilim Alıntı Endeksi)

SCI-E : Science Citation Index Expanded (Science Citation Index Genişletildi)

SGX : Software Guard Extension (Yazılım Koruma Uzantısı)

SSCI : Social Sciences Citation Index (Sosyal Bilimler Atıf İndeksi)

SSMI : Structural Smilarity Index Measure (Yapısal Benzerlik İndeksi Ölçüsü)

UIQI : Universal Image Quality Index (Evrensel Görüntü Kalitesi İndeksi)

URL : Uniform Resource Locator (Tekdüzen Kaynak Bulucu)

VANET : Vehicular Ad Hoc Network (Araç Özel Ağı)

YÖK : Yükseköğretim Kurulu

ÇİZELGELER LİSTESİ

Sayfa

Çizelge 1 E91 örnek polarizasyon filtresi ve sonucu.....49
Çizelge 2 B92 örnek polarizasyon filtresi ve sonucu 50
Çizelge 3 Naive Bayes kernel distribution sonucu 96
Çizelge 4 Naive Bayes MN distribution sonucu 96
Çizelge 5 Naive Bayes MN-Non negative sonucu 96
Çizelge 6 Naive Bayes MVMN distribution sonucu 97
Çizelge 7 Karar ağacı Gini katsayısı = 1 ile hesaplama sonuçları.....98
Çizelge 8 Karar ağacı Gini katsayısı = 2 ile hesaplama sonuçları.....98
Çizelge 9 Karar ağacı Gini katsayısı = 3 ile hesaplama sonuçları.....98
Çizelge 10 Karar ağacı Gini katsayısı = 4 ile hesaplama sonuçları.....99
Çizelge 11 Discriminant Analysis Diag-Quadratic sonuçları 99
Çizelge 12 Makine öğrenmesi metotları karşılaştırılması.....105

ŞEKİLLER LİSTESİ

Sayfa

Şekil 1 Polarizasyon filtreleri ve ürettikleri değerler 44
Şekil 2 BB84 örneği 45
Şekil 3 BB84 tabanlı genel sistem mimarisi 46
Şekil 4 kFold ve partioning benzeri bölümleme örneği 58
Şekil 5 Görselleştirme örneği 59
Şekil 6 kNN genel sistem diyagramı 61
Şekil 7 Naive Bayes genel sistem diyagramı 63
Şekil 8 Karar ağacı genel şeması 68
Şekil 9 X ekseninde boyut indirgeme örneği 70
Şekil 10 Diagonal eksende boyut indirgeme örneği 70
Şekil 11 Kümeler arası mesafe görsel örneği 71
Şekil 12 Diskriminant analizi genel şeması 72
Şekil 13 SVM margin örnekleri 75
Şekil 14 ReLU görseli 79
Şekil 15 TanH fonksiyonu görseli 79
Şekil 16 Sigmoid fonksiyonu görseli 80
Şekil 17 YSA tasarımı 83
Şekil 18 1K Chebychev sonuçları 84
Şekil 19 10K Chebychev sonuçları 84
Şekil 20 100K Chebychev sonuçları 85
Şekil 21 1M Chebychev sonuçları 85
Şekil 22 1K CityBlock sonuçları 86
Şekil 23 10K CityBlock sonuçları 86
Şekil 24 100K CiyBlock sonuçları 87
Şekil 25 1M CityBlock sonuçları 87
Şekil 26 1K Euclidean sonuçları 88
Şekil 27 10K Euclideean sonuçları 88

Şekil 28 100K Euclidean sonuçları 89
Şekil 29 1M Euclidean sonuçları 89
Şekil 30 1K Hamming sonuçları 90
Şekil 31 10K Hamming sonuçları 90
Şekil 32 100K Hamming sonuçları 91
Şekil 33 1M Hamming sonuçları 91
Şekil 34 1K Jaccard sonuçları 92
Şekil 35 10K Jaccard sonuçları 92
Şekil 36 100K Jaccard sonuçları 93
Şekil 37 1M Jaccard sonuçları 93
Şekil 38 1K sEuclidean sonuçları 94
Şekil 39 10K sEuclidean sonuçları 94
Şekil 40 100K sEuclidean sonuçları 95
Şekil 41 1M sEuclidean sonuçları 95
Şekil 42 YSA 20K veri 10 epoch sonucu 100
Şekil 43 YSA 20K veri 100 epoch sonucu 101
Şekil 44 20K veri 1000 epoch sonucu 101
Şekil 45 YSA 50K veri 10 epoch sonucu 102
Şekil 46 YSA 50K veri 100 epoch sonucu 102
Şekil 47 YSA 50K veri 1000 epoch sonucu 103
Şekil 48 BB84 protokolü için blokzincir sistemi önerisi 113
Şekil 49 E91 protokolü için blokzincir sistemi önerisi 114
Şekil 50 B92 protokolü için blokzincir sistemi önerisi 114

I. GİRİŞ

Bilgisayar teknolojisi ortaya çıkışının ardından sürekli ve hızlı bir şekilde gelişmeye ve kullanım alanlarında genişlemeye devam etmiştir. Bilgisayar teknolojisinde kullanılan donanımlar hacim olarak her geçen gün ufalmaya ve maliyet olarak da makul seviyelerde üretilmeye devam etmektedir. Birçok kullanıcının evinde, iş yerinde hatta telefonların ufak birer bilgisayara dönüşme eğiliminden dolayı ceplerinde kişisel bilgisayarlar taşınmaktadır. Kullanım yeri ve amacı fark etmeksizin bilgisayarlar da ortak olduğu söylenebilecek en temel husus bilgisayar işlemcilerinin üretildiği materyaldir. Silikon (Silisyum maddesi) bazlı işlemciler diye ifade edilen ve günümüzde bilgisayarda kullanılan işlemcilerin üretildiği madde olan silikon çeşitli süreçlerden geçtikten sonra işlemci haline dönüşmektedir. İlk üretilen bilgisayarlar ile günümüzde satın alınabilecek bilgisayarlar mukayese edildiğinde boyut ve hız olarak oluşan fark çok ciddi oranlardadır. Tüm bu farkın temel sebebi katlanarak artan bilgisayar bilimleri, bilgisayar donanımı, elektrik-elektronik biliminde görülen gelişme hızının çok fazla olmasıdır. Tüm bu etkenler üst üste geldiğinde 1960'lı yıllarda hayatlarımıza giren bilgisayarların günümüzde çantamızda hatta cebimizde taşınabilir hale gelmesini sağladığı söylenebilir.

Silikon bazlı işlemciler Intel şirketinin kurucularından olan Gordon Moore'un kendi soy ismini verdiği Moore Yasasına göre değerlendirilmektedir. Bu yasaya göre bilgisayar mikroişlemcileri içindeki transistor sayısının her iki yılda bir iki katına çıkacağı ve işlemcilerin de boyutlarında küçülmeler olacağı ifade edilir. 2 kez revize edilen ve en son tezimizde ifade edildiği şekilde 2 yılda bir 2 kat artacak açıklaması bir yasa olarak kabul edilmiştir. Moore ayrıca işlemci maliyetlerinin aynı kalacağı yahut azalacağını ifade etmiştir (Moore, 1965). Moore'un açıklamaları günümüze kadar geçerliliğini ana hatlarıyla korumayı başarmıştır. İçinde bulunduğumuz 2022 yılında etkisi azalsa dahi devam eden küresel COVID salgını sebebiyle çip maliyetleri artmış ve doğal olarak tüm dünyada görülen enflasyon doğal olarak teknolojik cihazlarda

maliyet artışlarına sebebiyet vermiştir. Ancak son dönem dikkate alınmadan önerilen Moore Yasası dikkate alındığında gerçekten de işlemci boyutları ufalırken bilgisayar hızlarının arttığı görülmüştür.

Silikon işlemcili bilgisayarlarda transistorlar yapılmak istenen hesaplamaların gerçekleştirilmesinde görevli olan donanım birimleridir. Bir nevi bilgisayarların hücreleri durumundadır. Çok küçük olan transistorlar yaklaşık olarak 14 nanometrelik (nm) bir boyuta sahiptirler. Berkeley Üniversitesinde yürütülen çalışmalar transistor boyutunun 5 nanometrelik yapılara düşmesinin önünü açacak yöndedir. Ancak 14 nm'lik bir transistor dikkate alındığında ve gerçek hayattaki başka hücre boyutları incelendiğinde ilginç sonuçlar görülecektir. Örneğin bir HIV virüsü 120 nm iken bir beyaz kan hücresi 7000 nm'lik bir boyuttadır. Anlaşılacağı üzere günümüzde silikon bazlı geliştirilen bu işlemciler için ufalabilecek boyut ve doğal olarak artabilecek hız miktarında Moore Yasasına göre tamamlanmak üzeredir. Bu sebeple alternatif hesaplama yöntemleri ve yeni bilgisayarlar üzerine çalışmalar sürdürülmektedir (Avis ve Jang, 2022). Mekanik olarak daha ufak parçaların geliştirilemeyeceği durumuna gelindiği kabul edilirse, bilgisayarlardan daha fazla performans alabilmek için yıkıcı inovasyon olarak nitelendirilen teknolojik alanlarda gelişmelerin hızlandırılması gerekmektedir. Bu alanlardan biri ve en ön planda olanı kuantum teknolojileridir. Araştırmacılar kuantum mekaniği ve fiziğini temel alarak yeni nesil bilgisayarlar üretmek amacıyla çok sayıda çalışma yürütmüşlerdir. (Mor ve Renner, 1983) çalışmalarında Moore Kanunu da dikkate alınarak günümüzde gelinen eşiğin geçilmesi durumunu öngörerek kuantum hesaplama teknolojisi bir diğer deyişle kuantum bilgisayarlar üzerine akademik anlamda ilk çalışmayı yürüten kişilerden olmuşlardır.

Günümüzde kullanılan silikon bazlı işlemcili bilgisayarların en ufak veri birimi bitlerdir. Kuantum bilgisayarlarında ise iki farklı değerden birine ayarlanabilen kübitler kullanılmaktadırlar. Kübiter manyetik alan özellikleri ve fotonik dairesel hareketleri ile yorumlanabilmektedir. Fotonlar üzerinden çalışmalar devam etmekte olup, bilgi edinimi ve paylaşımı için bu üretilen fotonların polarizasyon denilen yönlü optik filtre mekanizmalarından geçirilmeleri gerekmektedir. Bu işlem sonrasında fotonlar hakkında yorum yapabilir hale gelinir. Bu süre zarfına kadar fotonlar anlık olarak 0 veya 1

olabilecek herhangi bir konumda bulunabilir ve bu duruma fotonların süperpozisyonu denilmektedir. Bu özellik kuantum bilgisayarların günümüz bilgisayarlarından ayrıştığı en önemli noktadır (Bohr, 1928).

Günümüz bilgisayarlarında 4 bit içeren bir bilgi durumunu ele alalım. Dört bit tek seferde 0 ve 1 olmak üzere temelde 24 farklı durumda bulunabilmektedir. Bu işlemin sonucunda 16 muhtemel kombinasyon elde edilir ve bunlardan sadece 1 tanesi kullanılabilir. Ancak kuantum bilgisayarlarında süperpozisyon halinde dört kübit (QBit) aynı anda bu 16 kombinasyonun tamamında bulunabilir. Her yeni bir Qbit eklenilmesinde bu durum üstel fonksiyon değerinde artmaktadır. ‘0 bitlik bir dizin günümüz bilgisayarlarında 220 işlemi sonucundan elde edilen 1.048.576 değerden sadece bir tanesini tutabilecek iken, kuantum bilgisayarlarında bu durum 1.048.576 değerin tamamına karşılık gelmektedir, bu avantaj fotonların süperpozisyon ve kuantum özelliğinden kaynaklanmaktadır (Friedman vd., 2000).

Kuantum bitleri, foton davranışları, süperpozisyon durumu ne kadar sezgisel ve kafa karıştırıcı bir durum olarak gözükse de kuantum fiziğinde sezgisel olmayan bir başka önemli özellik olan foton dolanıklığı konusu bulunmaktadır. Birbirileri ile bağlantısı bulunan fotonların ne kadar uzakta olurlarsa olsunlar, birinin durumunun değişmesi durumunda diğerinin tersinir bir pozisyona geçmesi halidir. Bu durum sayesinde dolanık fotonlardan sadece birini ölçerek diğer foton hakkında otomatik olarak bilgi sahibi olunabilmektedir (Collini vd., 2010).

Kuantum bilgisayarları temel olarak fotonların manipülasyonu ve süper pozisyon halinde olmaları durumlarını kullanarak, birden fazla fotonda aynı anda çoklu ihtimaller ile hesap sonuçları alabilmek ve elde edilmesi gereken sonuca ulaşabilmeyi sağlar. Normal bilgisayarlarda karşılaştırma ve sonuç elde etme işlemleri sıralı bir kontrol işlemi içerdiği için kuantum bilgisayarlara göre bu konularda oldukça zayıf kalmaktadırlar (Engel vd., 2007).

Kuantum bilgisayarların altyapısal olarak üstünlükleri bulunmasına karşı yakın bir zamanda evimizdeki bilgisayarların yerini hemen alabilecekleri düşünülmemelidir. Fiyat performans analizleri ve kullanılabilirlik alanları halen daha güncel kullanımda olan bilgisayarlarımızın alanında değildir. Veri

bilimcilerin sıkça kullandıkları ve üzerine bilimsel araştırmaların popüler olduğu veri tabanı araması algoritmalarında kullanılmasına çalışılmaktadır. Günümüz bilgisayarlarında veri tabanı sorgu işlemleri veri tabanı üzerine tek tek test edilmek zorunda kalınabilir, ancak kuantum bilgisayarlar aynı işlemi yapmak için normal cihazların kullandığı zamanın karekökünde bu işlemi gerçekleştirebilirler. Normal işlemler için bu çok önemli bir fark olarak gözükmese bile büyük veri tabanlarında bu tarz işlemlerin yapılması oldukça önem arz etmektedir. 100.000.000 birim zaman içerecek bir sorgu işleminin 10.000'de yapılıyor olması durumu buna örnek olarak gösterilebilir.

Kuantum bilgisayarların önemli oldukları bir diğer alan ise bilgi güvenliği sektörüdür. Şu an için tüm şifreleme algoritmaları ve yöntemlerini tehlikeye sokacak bir durumda olmayan kuantum cihazları ve işlem güçleri polinomal şifre havuzu içeren yöntemlerin ürettikleri geniş şifre havuzlarına karşı etkilidir. Kişisel bilgilerinizi koruyan temel unsur haberleşme hatlarında akan verilerin okunamayacak bir formatta iletilmesidir. Bu işlem esnasında alıcı ve verici arasında iletilen bilgiyi elde etmek isteyen üçüncü şahıslara karşı veriyi okunamayacak formatta tutmak için güvenilir şifreleme algoritmaları kullanmak gerekmektedir. Ancak şifreleme algoritmalarının tam anlamı ile güvenilir olması için herkes tarafından bilinen açık bir yöntem olmasına rağmen algoritmik karmaşıklığının aşılamaz olmasıdır. Herkes tarafından bilinen bir yöntemin/algoritmanın güvenilirliği en temel olarak kullanılan açık ve özel anahtarlardan gelmelidir. Açık ve kapalı anahtar mekanizması, bunların rastgele olmaları ve kullanım sistemleri genel olarak bir şifreleme algoritmasının temelini meydana getirir. Şifrelerin rastgele olması durumu ayrı özel bir araştırma konusu olmasının yanında şifrelerin iletişimin iki tarafını oluşturan kesimlerin birbirilerine uzak mesafelerden güvenli bir şekilde paylaşılabilir olması ayrı bir araştırma konusudur. Her iki araştırma konusunda kuantum sistemlerinin normal sistemlere göre üstünlükleri bulunmaktadır. Günümüzde kullanmakta olduğumuz anahtar/şifre üretme sistemleri en temelinde yapay rastgele sayı üreteçleri kullanmaktır, bu üreteçlerin tam anlamı ile rastgele ve tahmin edilemez değerler ürettiği düşünülmemektedir. Ancak kuantum anahtar üretim sistemlerinde kullanılan fotonların yukarıda bahsedilen süperpozisyon halinde bulunmaları sebebi ile polarize edilmeden bu fotonlar hakkında

herhangi bir bilgi sahibi olmak bilimin bulunduğu noktada imkânsız olarak gözükmektedir. Fotonların polarize edilmesi yöntemi ile elde edilen sayılar diğer yöntemlerin hepsine göre çok daha fazla rastgele değerler üretmektedir ve dolayısı ile daha güvenilirdir (Croitoru ve Isar, 2022).

Diğer bir araştırma konusu olan alan anahtarların iletişim tarafları arasında güvenli bir şekilde paylaştırılması işlemidir. Günümüzde simetrik ve asimetrik anahtar paylaşımlı sistemler bulunmakta ve kullanılması düşünülen sistemlere uygunluğuna göre tercih edilmektedirler. Asimetrik anahtar paylaşımı sistemlerinde bir açık bir özel anahtar çifti kullanılmalıdır. Açık anahtar genellikle gönderilen mesaj içerisinde iki tarafın bildiği bir konumda saklanırken özel anahtarlar paylaşılmaz. Ancak "man in the middle" gibi anahtarlar kullanılarak iletişim kanalı arasına giren üçüncü şahıslar bu tarz şifreleme algoritmalarını ve sağladıkları güvenliği aşabilmektedirler. OTP-One Time Pad gibi mesaj uzunluğu kadar şifre üreten algoritmalar gönderilecek olan mesajın boyutunun uzaması ile kullanılabilirliklerini ve askeri kullanımları hariç kullanımlarının efektif olmaktan çıkarmakta ve tercih edilememektedir. Kuantum teknolojileri kullanılarak tarafların anahtarlarını belirtecek değerleri karşılıklı olarak paylaşmadan, birbirileri ile fiziksel olarak görüşmelerine gerek kalmaksızın, çift anahtar kullanmasını gerektirmeyen sistemleri 1984, 1991, ve 1992 yıllarında başarılı örnekler kullanarak oluşturulmuştur. Bu yöntemler ilerleyen bölümlerde BB84 (Bennett ve Brassard, 1984), E91 (Ekert, 1991) ve B92 (Bennett, 1992) başlıkları altında anlatılacaktır. Kuantum anahtar dağıtımı ağları kullanılarak ve bu ağların içerisine klasik haberleşme ağlarını da dahil ederek başarılı örnekler oluşturmak mümkündür.

Ancak güncel olarak kullanılan teknolojiler ve güvelik unsurlarının temelini oluşturan anahtar üretimi ve dağıtımı sistemlerinin kuantum sistemlerine göre dezavantajları bulunduğu gibi, kuantum sistemlerinin de güncel kullanılan sistemlere göre belirli dezavantajları bulunmaktadır. Bu dezavantajlara tezin ilerleyen bölümlerinde değinilecektir. Doktora çalışmamızın temel olarak ele aldığı konu kuantum anahtar dağıtımı sistemlerinin önemli dezavantajlarından biri olan artık bit'lerin çok olması ve bunların azaltılması üzerine çalışmaktır. Bunun için makine öğrenmesi ve sınıflandırma algoritmaları kullanılmış ve yapılan işlemlerin sonuçları ilgili

bölümlerde gösterilmiştir. Ayrıca tezimizden üretilen ve yayın aşamasında olan Kuantum Blokzincir Anahtar Dağıtımı isimli makale çalışmamızda kuantum anahtar dağıtımında blokzincir teknolojisi kullanılarak gerçekleştirilmeye çalışılmıştır. BB84, E91 ve B92 protokolleri ile uyumlu çalışabilen bir sistem önerilmiştir. Tez çalışmamızın ilerleyen bölümlerinde blokzincir teknolojisinden ve önermiş olduğumuz yöntemden bahsedilecektir.

A. Literatür Taraması

Literatür çalışması bölümünde kuantum anahtar dağıtımı, şifreleme, blokzincir ve makine öğrenmesi konuları üzerinde gerçekleştirilen çalışmalar incelenmiştir. Makine Öğrenmesi Algoritmalarının KAD/QKD Artık Bit'lerinin Geri Kazanımında Kullanımı isimli tezimizde önerilen çalışmanın daha iyi anlaşılabilmesi için yukarıda belirtilen konu başlıklarının çalışıldığı akademik yayınların incelenmesi ve teknolojik ve akademik olarak gelinen noktanın daha iyi anlaşılması gerekmektedir.

(Takaoğlu vd., 2022) çalışması doktora tezimizden türetilmiş olup, yapay zekâ algoritmaları üzerine yürütülmüş olunan araştırmalar neticesinde elde edilen bilgi birikiminin genetik algoritmalar ve insansız hava araçları üzerine önerilen yöntemde kullanılmasını sonucunda gerçekleştirilmiştir. Gerçekleştirilen çalışmanın araştırma makalesine çevrilmiş hali SCI-E indeksli MDPI Symmetry (Q2) dergisinde yayınlatılmıştır.

(Bennet ve Brassard, 1984) çalışmasında kuantum fiziği mekaniğinden faydalanarak ilk kuantum anahtar dağıtımı protokolü olan BB84'u tanıtmıştır. Bu sayede Alice ve Bob arasında kuantum fiziği kuralları sayesinde gerçek anlamda güvenli anahtar paylaşımı gerçekleştirilmiştir.

(Sun vd., 2021) yapmış oldukları çalışmada Logicontract ismini verdikleri kuantum-güvenli blokzincir sistemlerini akıllı sözleşmeler kullanarak gerçekleştirmektedirler. Geliştirmiş oldukları yöntem birçok alanda uygulanabilir yapıdadır. Kuantum sonrası dönemde güvenilir bir yapıya sahiptir. Bunu kafes bazlı açık anahtarlı şifreleme ve imza yöntemlerini kullanarak sağlamaktadır.

(Ko ve Jung, 2021) çalışmalarında kuantum hesaplama temelli siber güvenlik teknolojileri ve algoritmalarının gelişimini ele almışlardır. IBM Qiskit kuantum simülatörünü kullanarak AES (Advanced Encryption Standard) şifreleme algoritmasını kullanarak şifreleme ve şifre çözme adımları görüntü dosyaları üzerinde uygulamışlardır. Ayrıca AES algoritmasını satır kaydırma aşamasında değiştirmişlerdir. Bunu yapmalarının sebebi kuantum hesaplamaya daha uygun hale getirilmesinin sağlanmasıdır. Elde ettikleri sonuçları çalışmalarında paylaşmışlardır.

(Naresh vd., 2020) çalışmalarında akıllı şehirlerde kullanılan çoklu ajan sistemlerinin e-sağlık hizmetlerinde kullanımı üzerinde durmuşlardır. Kuantum Diffie-Hellmand anahtar dağıtımı algoritmasını genişleterek dinamik grup anahtar mutabakatı üzerine bir araştırma gerçekleştirmişlerdir. Sağlık sektöründe grup anahtar dağıtımının çok önemli olduğunun paylaşıldığı bu çalışmada elde edilmek istenen sonuç; kuantum sonrası dönem için güvenli, akıllı şehir uygulamalarında kullanılabilecek bir çözüm önerisi sunulmasıdır. Çalışma incelendiğinde önerilen yöntemin umut vaat ettiği söylenebilir.

(Mesnager vd., 2020) yapmış oldukları çalışmalarında eşik temelli kuantum sonrası dönem için çoklu gizli paylaşım yöntemini dağıtık blokzincirlerde depolamayı gerçekleştirmişlerdir. Geliştirmiş oldukları yöntem ile blokzincir sistemlerindeki veri depolama boyutlarında iyileştirme elde ettikleri ileri sürülmüştür. Doğrulama ve gizli iletişim hususunda blokzincir sistemlerini kullanmış olmalarının sağladığı katkılardan faydalanmışlardır.

(Ampatzis ve Andeonikos, 2021) çalışmalarında kuantum anahtar paylaşımını simetrik karıştırılmış Bernstein-Vazirani algoritması temel alınarak gerçekleştirmeyi önermişlerdir. Yeni bir fikir olarak önerilen bu çalışma bizim de tez çalışmamızda hazırlamış olduğumuz bir diğer indeksli makale çalışması olan kuantum blokzincir anahtar dağıtımı algoritmasında olduğu gibi kuantum anahtar dağıtımını farklı şekillerde kullanmayı amaçlayan bir çalışmadır. Araştırmacılar çalışmalarında elde ettikleri sonuçları makalelerinde paylaşmışlardır.

(Cochran ve Gauthier, 2021) yapmış oldukları çalışmada kübit temelli saat senkron sistemini bayezyen yaklaşımla kuantum anahtar dağıtımına

uygulamışlardır. BB84 algoritmasını kullanarak test ettikleri yöntemlerinin başarılarını paylaşmışlardır. %95'lik bir senkronizasyon başarı oranı elde etmişlerdir. Kuantum anahtar dağıtımının farklı kullanım yöntemlerinin anlaşılması açısından önemli bir çalışmadır.

(Liu vd., 2021) çalışmalarında uydular arasında kablosuz bağlantıların termal terahertz kaynaklarına dayalı olarak sürekli değişken kuantum gizli bilgi paylaşımı önerilmiştir. Çalışmaları uydular arası kuantum iletişim ağının verimli bir şekilde kurulmasına katkı sağlamaktadır.

(Alshowkan vd., 2013) çalışmalarında üç taraflı yeni bir kuantum anahtar dağıtımı mimarisi önerilmektedir. Alice ve Bob olarak tabir edilen ikili veri gönderim taraflarına ek olarak güvenli merkez adı altında üçüncü bir taraf eklenmesini önermektedir. Bu güvenli merkez kimlik doğrulaması ve anahtar anlaşması aşamasında katkı sağlayacak şekilde planlanmıştır. Teorik olarak önermiş oldukları bu yeni algoritma ayrıntılı olarak açıklanmıştır. Daha önce de ifade edildiği üzere, tezimizden üretilen bir diğer yayın olan kuantum blokzincir anahtar dağıtımı algoritması bu fikre yakın bir çalışmadır. Güvenli merkez diye ekledikleri mekanizma yerine bizim makale çalışmamızda önermiş olduğumuz özel blokzincir mimarisinin eklenmesi aynı etkiyi daha yüksek başarı oranlarıyla sağlayacaktır. Ayrıca sistem güvenliği açısından da blokzincir eklentisi çok daha faydalı bir katkı sağlayacaktır. Araştırmacıların önermiş oldukları bu çalışma 2013 yılında yayınlanması ve 2014 yılında blokzincir teknolojisinin yeni yeni kavram olarak isimlendirilmeye başlandığı düşünüldüğünde blokzincir eklentisinin yapılamamış olması çok normal bir durumdur.

(Zeng ve Zhang, 2000) çalışmalarında kuantum anahtar dağıtımı sürecinde kimlik doğrulaması üzerinde durulmuştur. Kuantum fiziği kuralları gereği veri iletimi sürecinde gerçekleşebilecek saldırı faaliyetlerine karşı gerçek bir korumadan söz edilir. Ancak gerçek uygulamalarda veri iletimi saldırganlar tarafından dinlenmeye çalışıldığında, aynı veri iletiminin bir tarafıymış gibi kendini alıcı ya da gönderici olarak taklit eden saldırıların tespiti için kullanılabilecek bir algoritma ihtiyacı bulunduğu paylaşılmıştır. Önermiş oldukları yöntemin bu ihtiyacın giderilmesinde çözüm olarak kullanılabileceği ve güvenli olduğu makalelerinde ayrıntılı bir şekilde açıklanmıştır.

(Hwang vd., 2007) yapmış oldukları çalışmalarında üç taraflı güvenli bir kuantum anahtar dağıtımı algoritması önermişlerdir. Üçüncü taraf olarak geliştirilen eklentide rastgele sayı ve oturum anahtarı üretilmektedir. Önermiş oldukları algoritmanın güvenli olduğunu teorik olarak açıklamışlardır.

(Wootters ve Zurek, 1982) çalışmalarında kuantum durumu bilinmeyen bir kübit'in kopyalanamayacağını bir başka deyişle polarizasyon temelleri bilinmeyen bir kübit kopyalanamaz fikrini literatüre katmışlardır. Klonlama-yok teoremi olarak bilinen bu çalışma kendisinden sonra yapılan birçok çalışmaya katkı sağlamış ve kuantum teknolojisinin gelişmesine büyük katkılar sağlamıştır.

(Cao vd., 2020) yapmış oldukları çalışmalarında kuantum anahtar dağıtım ağının iki taraflı olarak kullanımının aksine daha esnek ve genişletilebilir bir mimari önermişlerdir. Önermiş oldukları yöntemin uygulanabilirliğini ve güvenlik açısından çok başarılı olduğunu yapmış oldukları örnek üzerinden teorik olarak açıklamışlardır.

(Mailloux vd., 2017) çalışmalarında yem durumu etkin kuantum anahtar dağıtımı sistemlerinin modelleme, simülasyon ve performans analizleri üzerinde durmuşlardır. BB84 ve yem durumu protokolleri, foton numara bölme saldırısına karşı test edilmiştir. Elde ettikleri sonuçları ayrıntılı bir şekilde çalışmalarında paylaşmışlardır.

(Mihara, 2012) çalışmasında kuantum steganografisi üzerine çalışmıştır. Steganografi veri gizleme bilimidir. Bilgisayar teknolojileri sayesinde dijitalleşen verinin yine bilgisayar analiz algoritmalarından gizlenmesi için geliştirilen yöntemler bütününe dijital steganografi denilmektedir. Yazar çalışmasında gizlemek istediği metin dosyasını kullanılan kapak verisinin içeriğinde değişikliğe sebebiyet vermeyecek şekilde gerçekleştirmeyi amaçlamıştır. Bu doğrultuda önermiş olduğu yöntemi ayrıntıları ile tanıtmış ve elde edilen sonuçları paylaşmıştır.

(Armanuzzaman vd., 2017) çalışmalarında güvenli ve verimli veri iletim tekniği önermişlerdir. Bu teknik kuantum anahtar dağıtımı algoritması kullanılarak geliştirilmiştir. One-Time-Pad, OTP şifreleme algoritması ve Huffman kayıpsız sıkıştırma algoritması kullanılmıştır. OTP şifreleme

algoritmasında kullanılması gereken şifrelenecek veri uzunluğunda oluşturulacak rastgele anahtar seçiminin yapılmasında kuantum anahtar dağıtımından faydalanmışlardır. Ancak kuantum anahtar dağıtımıyla seçilen anahtarın belirlenmesinde gerçek kuantum anahtar üreticisi kullanılmamıştır. Yazılımsal olarak üretilen anahtar bitleri kuantum anahtar dağıtımı mekaniği kullanılarak Alice ve Bob arasında iletilmiş ve OTP şifrelemesi gerçekleştirilmiştir. Yapılan işlem esasen BB84 algoritmasına çok benzemektedir.

(Wang vd., 2019) çalışmalarında kuantum anahtar dağıtımı sürecinin yazılım tanımlı ağlar kullanarak kontrol ve yönetilebileceği üzerinde durulmuştur. Yazılım tanımlı ağlar bu bağlamda ayrıntılı olarak incelenmiş ve okuyuculara süreç ve protokoller hakkında bilgiler ve yapılan simülasyon sonuçları paylaşılmıştır.

(Tsai vd., 2021) yapmış oldukları çalışmalarında kuantum anahtar dağıtım ağlarında görülen sorunlar, zorluklar ve güvenlik konusunda gelecek çalışma konuları hakkında bir araştırma yürütmüşlerdir. Çok sayıda alakalı makalenin incelendiği bu çalışma, paylaşmış olduğu kıyaslamalar sayesinde tespit etmiş olunan önemli noktaları ayrıntılı bir şekilde açıklamıştır.

(Zhang, 2019) çalışmasında kuantum öncesi ve sonrası kriptoloji için kara delik tuş takımı sıkıştırma ve ölçeklenebilir OTP algoritması ile bilgi korumalı güvenlikli analitik kuantum zekâ yaklaşımını önermiştir. Önerilen yöntemin teorik ispatı ayrıntılı bir şekilde paylaşılmıştır.

(Wang ve Li, 2021) gerçekleştirdikleri çalışmalarında TEDL olarak isimlendirdikleri, derin öğrenme temelli metin şifreleme metodu önermişlerdir. Amaçları geleneksel şifreleme yöntemlerinde görülen anahtar uzayı ve anahtar güncellemelerinde karşılaşılan sorunların giderilmesidir. Derin öğrenme sayesinde geliştirmiş oldukları mimari sayesinde güvenlik, anahtar uzayı ve anahtar güncellemeleri gibi konularda başarılı sonuçlar elde etmişlerdir.

(Peechara ve Sucharita, 2021) çalışmalarında kaos teorisinden faydalanarak asenkron iki yönlü şifreleme yöntemi geliştirmişlerdir. Bu geliştirdikleri yöntemi bulut hesaplaması için uygulamışlardır. Önerdikleri yöntemle üretilen anahtarların tam anlamıyla rastgele olduğunu p-değeri testini

uygulayarak ispatlamışlardır. Ayrıca veri iletim sistemlerinde bu yöntemin çok büyük kolaylıklar sağlayacağı ifade edilmiştir.

(Aliev vd., 2020) yapmış oldukları çalışmalarında ölçeklenebilir grup anahtar yönetim sistemi önermişlerdir. Bu yöntem ile araçlar arasında güvenli iletişim sağlanması amaçlanmıştır. Matris temelli bir grup anahtar üretimi yöntemi kullanmışladır. Bu yöntem sayesinde sistemin daha hızlı bir şekilde çalışması sağlanmıştır.

(Choudhary vd., 2020) çalışmalarında MAKE-IT ismini verdikleri kimlik doğrulama ve anahtar değişim protokolünden oluşan ve bu yöntemi sanayi için nesnelerin interneti konusunda uygulamaktadır. Algoritmalarının enerji tüketimini azalttığı ve güvenlik açısından üst düzeyde olduğu çalışmada ayrıntılarıyla ifade edilmiştir. Anahtar paylaşımı konusunda özüt algoritmaları ve şifreleme tekniklerinden yararlanılmıştır.

(Stulman ve Stulman, 2019) çalışmalarında güvenli anahtar değişimi için dalgalı topolojiden faydalanarak özel ağlarda güvenlik sağlamayı öngörmüşlerdir. Anahtar değişimini çoklu parçaya bölüp gerçekleştirmeyi amaçlamışlardır. Esasen yapmış oldukları çalışma (Shamir, 1979)'in anahtar değişim algoritmasına benzemektedir. İletilmek istenen gizli veri parçalara bölünüp farklı aracılar ile alıcı tarafına iletilerek ve birleştirilerek elde edilir.

(Belghazi vd., 2019) yapmış oldukları çalışmalarında nesnelerin internetinin yaygın olduğu akıllı ortamlarda cihazlar arası iletişimin güvenli sağlanabilmesi için kablosuz internet güvenliğinin anahtar değişimi algoritması kullanılarak gerçekleştirilmesi amaçlanmıştır. Kare kod ile yenilikçi bir anahtar paylaşımı yöntemi geliştirmişlerdir. Diffie-Hellman anahtar paylaşımı algoritması ve SHA256 özüt algoritmasından faydalanılmıştır. Algoritmaları sayesinde hafıza kullanımı azaltılmış ve veri bütünlüğü ve güvenliği sağlanmıştır.

(Furtak, 2020) çalışmasında bir konsept önerilmiştir. Bu konseptte kriptolojik anahtar üretimi ve yenilenmesi öngörülmüştür. Nesnelerin interneti ağlarında bulunan düğümleri kapsayan bu çalışmada fiziki Güvenilir Platform Modülünden yararlanılmıştır. Önermiş oldukları konsept teorik olarak ayrıntılı bir şekilde tanıtılmıştır.

(Ejaz vd., 2020) çalışmalarında simetrik şifreleme sistemleri için güvenli anahtar bağımlı dinamik bir ikame yöntemi önermişlerdir. Geliştirdikleri yöntemin Amerikan Ulusal Standartlar ve Teknoloji bürosunun belirlemiş oldukları testlere göre yeterlilik gösterildiği ve sistemlerinin güvenli ve emsal algoritmalara göre çok daha başarılı olduğu ifade edilmiştir. Çalışmalarında ayrıntılı olarak önerilen yöntem tanıtılmış ve yapılan testler paylaşılmıştır.

(Escribano Pablos vd., 2020) önermiş oldukları çalışmada kuantum sonrası grup anahtar değişimini Kyber isimli çalışmadan faydalanarak geliştirmişlerdir. Algoritmalarında dört aşamalı bir mimari bulunmaktadır. Bu yöntemde kuantum rastgele kâhin modelinden faydalanılmıştır. Çalışmalarının ilerleyen süreçte kuantum sonrası imzalara ki masraflı bir süreçtir, gerek kalmadan doğrulama sürecini gerçekleştirebileceğini ifade etmektedirler.

(Lizama-Perez ve López, 2021) çalışmalarında kuantum sonrası dönem için ters çevrilemez bir açık anahtar sertifikası sistemi önermişlerdir. Kuantum sonrası dönem için ölçeklenebilir bir açık anahtar mimarisi olmadığına dikkat çeken araştırmacılar bu bağlamda kendi yöntemlerini tanıtmışlardır.

(Melhem ve Kish, 2019) çalışmalarında Kirchhoff-Tasası-Johnson-Gürültü anahtar dağıtımı algoritmasına yeni bir saldırı geliştirmişlerdir. Geliştirmiş oldukları statik döngü akımı saldırısına karşı Kirchhoff-Tasası-Johnson-Gürültü anahtar dağıtımı algoritmasının başarısız kalması durumu ayrıntıları ile paylaşılmıştır. Kullanılan anahtar paylaşım algoritmalarına yürütülebilecek saldırıların anlaşılması ve anahtar paylaşım algoritmalarının güvenlik açıklarının görülmesi açısından önemli bir çalışmadır.

(Goumidi vd., 2021) yapmış oldukları çalışmalarında uygulanabilirliği kolay ve güvenli bir kimlik doğrulama ve anahtar dağıtımı yöntemi önermişlerdir. Çalışmalarında geliştirmiş oldukları yöntemi uygulamak için seçtikleri ortam araçlar için geliştirilmiş olan bulut hesaplama platformudur. AVISPA isimli yazılımı kullanarak geliştirmiş oldukları yöntemi analiz etmişler ve elde ettikleri sonuçları paylaşmışlardır.

(Mawlood Hussein vd., 2020) çalışmalarında geliştirmiş oldukları dağıtık anahtar dağıtımı algoritması ile nesnelerin interneti kablosuz sensor ağı güvenliğini akıllı tarım uygulamalarında sağlamaya çalışmışlardır. Eliptik eğri

şifrelemesi ve Diffie-Hellmann anahtar paylaşımı algoritmalarından faydalanarak kendi algoritmalarını geliştirmişlerdir. Elde ettikleri sonuçları ve ölçeklenebilirlik değerlerini çalışmalarında paylaşmışlardır.

(Chen vd., 2019) çalışmalarında kablosuz sensor ağlarında kullanılmak üzere takip edilemez veri iletim şeması önermişlerdir. Verilerin paketler halinde gönderimini ve bu süreçlerin gerçekleştirilmesinde gizli anahtar mekanizması geliştirerek sağlamışlardır. Geliştirmiş oldukları algoritmanın ayrıntılı açıklamasının paylaşıldığı çalışmalarında ayrıca dinleme ve geri takip gibi saldırılara karşı kendi yöntemlerinin güvenlik sağladığını göstermişlerdir.

(Yuan vd., 2020) yapmış oldukları çalışmalarında anahtar yönetim sistemi önermişlerdir. Bu yöntem heterojen kablosuz sensor ağları için geliştirilmiştir. Yöntemlerini eşleştirme gerektirmeyen kimlik tabanlı dijital imza algoritmasından esinlenerek geliştirmişlerdir. Bu yöntemleri sayesinde sisteme yöneltilebilecek saldırılara karşı bir güvenlik katmanı kazandırılmıştır. Sistem performansı değerlendirmesine göre ise geliştirmiş oldukları algoritma tüm ağ güvenliğinin sağlanması için hem enerji tasarrufu sağlarken hem de kabul edilebilir oranda depolama alanından fedakârlık yapmaktadır.

(Park vd., 2021) çalışmalarında medikal verilerin paylaşımında blokzincir temelli Proxy yeniden şifrelenmesine dayalı güvenli bir sistem önerisinde bulunmuşlardır. Önermiş oldukları sistem tam anlamıyla blokzincir sistemini kullanmadığı için ve dış sunucular bulunması sebebiyle şifreleme yolunu seçerek sistem güvenliğini arttırmayı öngörmüşlerdir. Karma bir sistem önerisi bulunulan bu çalışma hem şifreleme hem de blokzincir entegresi sayesinde medikal verilerin güvenli bir şekilde paylaşılması için alternatif bir çözüm önerisi sunmuştur.

(Lin, 2019) çalışmasında sosyal ağ servisleri için uygun yeni bir çift doğrulamalı şifreleme yöntemi önermiştir. Araştırmacıların önermiş oldukları yöntem sayesinde özel anahtar paylaşımı yapılmasına gerek kalmadan şifreleme ve şifre çözme işlemi yapılabilmektedir. Bu yöntem üçlü iletişim ortamları için hazırlanmıştır. Bilindiği üzere Skype, Line, Facebook Messenger gibi uygulamalar üçlü iletişim ortamına sahip uygulamalardır. Bu sebeple geliştirilen

yöntemin günümüz uygulamalarınca uygulanabilir yapıda olduğu ifade edilmiştir.

(Yoon vd., 2020) çalışmalarında SPEKS ismini verdikleri özel yazılım güvenlik eklentisi temelli, anahtar kelimesi araması kullanılarak açık anahtar şifreleme yöntemini önermişlerdir. Bu yöntem performans açısından alışılageldik yöntemlere nazaran daha iyi sonuçlar vermiştir. Özellikle sorgu işleme maliyetinde O(x)'den O(1)'e düşme görülmüştür (x şifrelenmiş veri sayısı). Ayrıca hesaplama süresi ortalama %80 oranında azaltılmıştır.

(Kim vd., 2020) yapmış oldukları çalışmalarında üçlü şifre doğrulama anahtar değişim protokolünü inceleyerek geliştirilmiş yeni bir protokol önermişlerdir. Sağlık alanında kablosuz iletişimde kullanılmak üzere geliştirilmiş ve test edilmiştir. Sistemlerinin dışarıdan gelebilecek saldırılara olduğu gibi içeriden gelebilecek saldırılara da dayanıklı olması sağlanmıştır. Geliştirmiş oldukları yeni protokol eskisinden farklı olarak biyometrik temelli verimli şifre doğrulama anahtar değişim protokolü olmuştur. Sistemin nasıl geliştirildiği ve güvenilirliği ile ilgili ayrıntılı bilgiler çalışmalarında paylaşılmıştır.

(Alvares vd., 2017) çalışmalarında hafifletilmiş anahtar değişimi için algoritma önermişlerdir. Kullanılan yöntemlerin çoğunda ciddi bir işlem gücü gerektiren algoritmalar bulunması ve bu yöntemlerin mobil uygulama gibi alanlarda uygulanabilirliğinin zor olması sebebiyle uygulaması hafif yöntemler üzerine odaklanılmıştır. Çeşitli şifreleme algoritmaları üzerinde durulmuş, bu algoritmaların performans analizleri yapılmış ve güvenlik çerçevesi oluşturulmuştur. Daha çok alan yazın çalışması gibi hazırlanmış bu çalışma şifreleme ve anahtar paylaşımı algoritmalarını ayrıntılı olarak incelemesi ve test etmesi açısından tezimiz için önem taşımaktadır.

(Mihalkovich vd., 2020) çalışmalarında değişken olmayan bir grup üzerinden tanımlanan anahtar değişim protokolü önermişlerdir. Bu protokolü geliştirirken deterministik olmayan bir polinoma dayalı tam karar problemi esas alınmıştır. Kuantum dönemi sonrası için herhangi bir kuantum kriptanaliz yönteminin deterministik olmayan polinom problemlerinin tespiti için hazırlanmadığı ifade edilmiştir. Ancak kuantum sonrası dönemde sahip

olunacak işlem gücüne deterministik olmayan polinom problemlerinin dayanıklı olması beklenmemektedir. Bu sebeple sistemlerinde güvenlik katmanı olarak sadece bu eklentiye güvenilerek hareket edilmemiştir.

(Liu vd., 2019) çalışmalarında araç özel ağları için güvenli ve verimli bir grup anahtar mutabakatı yöntemi önermişlerdir. Çalışmalarında toplu kimlik doğrulama yöntemi ve araçlar arasında gizli anahtar paylaşım yöntemi kullanmışlardır. Önermiş oldukları yöntem ayrıntılı bir şekilde çalışmalarında tanıtılmış olup sistem güvenliği teorik olarak ispatlanmıştır.

(Lee ve Lee, 2018) yapmış oldukları çalışmalarında dinamik grup kimlik doğrulaması ve anahtar paylaşım algoritması önermişlerdir. Nesnelerin interneti akıllı ölçüm ortamlarında kullanılabilmesi için eşik gizli paylaşımı tekniği temel alınarak geliştirilmiştir. Geliştirilen dinamik grup kimlik doğrulaması ve anahtar paylaşımı algoritmanın teorik açıklama ve ispatı çalışmalarında ayrıntılı bir şekilde paylaşılmıştır.

(Roy ve Khatwani, 2017) yapmış oldukları araştırmalarında kriptanaliz, eliptik eğri şifrelemesi temelli bir doğrulama ve anahtar paylaşımı protokolleri önermişlerdir. Önermiş oldukları protokolleri ayrıntılı bir şekilde açıklamışlardır. Çalışmada ele alınan konu başlıklarının tamamı tezimiz ile alakalı konular olması sebebiyle önem arz etmektedir. Ayrıca kendi sistemlerine yöneltmiş oldukları saldırı yöntemlerinin incelenmesi açısından da değerli bir çalışmadır.

(Liang vd., 2021) çalışmalarında eliptik eğri şifreleme yöntemini esas alarak asimetrik hiperkaotik resim şifreleme yöntemi önermişlerdir. Asimetrik bir şifreleme yöntemi geliştirme ihtiyacını resim şifrelemesinde çokça kullanılan simetrik şifreleme algoritmalarının anahtar paylaşımlarının açık kanaldan yapılamaması olarak göstermişlerdir. Bu doğrultuda asimetrik bir şifreleme yöntemi geliştirilmiştir. Önermiş oldukları yöntemi ayrıntılı olarak çalışmalarında tanıtmış ve çeşitli saldırılara tabii tutatak yöntemin güvenilirliğini ispatlamışlardır.

(Rivero-García vd., 2017) çalışmalarında kimlik temelli doğrulama ve anahtar değişimi algoritması kullanarak hastaların veri yönetim sistemini koruma altına almayı önermişlerdir. Mobil cihazlar ve yakın alan iletişim

bileklikleri kullanılarak önermiş oldukları sistemi test etmişlerdir. Elde ettikleri sonuçlar çalışmalarında ayrıntılı bir şekilde paylaşılmıştır.

(Lin vd., 2021) önermiş oldukları algoritmada kaos temelli senkron dinamik anahtarlar ve bu anahtarların resim şifrelemesinde iyileştirilmiş AES şifreleme algoritmasının kullanımını tanıtmışlardır. AES tarafında yapılan iyileştirme; statik anahtarın dinamik hale getirilmesi ve açık kanallar vasıtasıyla iletimine gerek kalmaması olarak ifade edilmiştir. Önermiş oldukları algoritmayı çeşitli test ve analizlere tabii tutarak elde ettikleri sonuçlar çalışmalarında paylaşılmıştır.

(Meng ve Li, 2021) çalışmalarında blokzincir destekli kimlik odaklı bir şifreleme yöntemi temel alınarak sanayi nesnelerin internetinde bulunan sensor ve çalıştırıcılarda kullanılmak üzere bir veri paylaşım mekanizması önermişlerdir. Çok katmanlı bu çalışmada güvenli ve güvenilir bir iletişim linki oluşturulmaktadır. Sisteme erişimi olan kimliklerin güvenilir olduğu kontrol edilmektedir. Son olarak sistemde kullanılabilecek farklı yapıdaki cihazlara uyumlu olması sağlanmaktadır. Araştırmacılar çalışmalarında önermiş oldukları mekanizmayı ayrıntılı olarak tanıtmış ve çeşitli testlere tabii tutarak elde ettikleri sonuçları paylaşmışlardır.

(Boakye-Boateng ve Lashkari, 2019) çalışmalarında tek seferlik pedler (One-Time-Pad) şifreleme algoritmasını genel nesne yönelimli trafo merkezi olayında güvenlik katmanı olarak kullanmayı önermişlerdir. Bu alanda yapmış oldukları çalışmayı teorik olarak ayrıntılı olarak açıklamışlardır. Ancak önerilen sistem geliştirilmeye ve üzerinde çalışmaya ihtiyaç duyulan bir yapıdadır. Çalışmanın simetrik şifreleme algoritmalarından olan ve kuantum sonrası dönem için teorik olarak güvenli kabul edilen OTP algoritmasını kullanması açısından tezimizde incelenmeye değer görülmüştür.

(Wu vd., 2021) yapmış oldukları çalışmalarında serbest uzay kuantum anahtar dağıtımı yöntemi için kirişlerin polarizasyon filtreleri özellikleri üzerine kaynak parametrelerinin etkileri incelenmiştir. Araştırmacılar çalışmalarında Huygens-Fresnel ilkesi ve çapraz spektral ile kavisli optiklerin bağımlı polarizasyon etkilerinin depolarizasyon ve dönüşünü incelemişlerdir. Yapılan

simülasyonlarda türbülans etkisinin neden olduğu polarizasyonun iyi foton tutarlılığını korurken güçlü bir şekilde azaltılabileceğini göstermiştir.

(Zhang vd., 2021) çalışmalarında referans çerçeve kalibrasyonunda makine öğrenimi destekli ve ölçüm cihazından bağımsız kuantum anahtar dağılımı protokolü önermişlerdir. Önermiş oldukları algoritmayı 100 km ile 250 km fiber tek modlu hatlar üzerinde denemekte oldukları ifade edilmiştir. Algoritmaları sayesinde aktarım verimliliğinin yüksek oranlarda arttırıldığı paylaşılmıştır.

(Wang vd., 2021) çalışmalarında serbest alan ölçüm cihazı kullanarak bu cihaz ile ilişkili türbülans kanalı altında yapmış oldukları modülasyon ile retro-reflektörlü bağımsız kuantum anahtar dağıtımı protokolü önermişlerdir. Önermiş oldukları protokol sönüm korelasyon katsayısının artması durumunda ve türbülans yoğunluğunda artış görülmesi durumunda iyileştirici ve sistemi koruyucu bir özellik taşımaktadır. Yapmış oldukları klasik saldırıların analizlerinden elde ettikleri sonuçları çalışmalarında paylaşmışlardır.

(Wen vd., 2021) yapmış oldukları çalışmada sürekli değişen kuantum anahtar dağıtımı algoritmalarında iyileştirilmiş dilim eşleştirme protokolü geliştirmişlerdir. Protokolleri geliştirilirken ham veriler üzerine rastgele bir ortogonal işlem uygulayarak nicelenmiş diziler için geliştirilmiş bir hale getirilmiştir. Protokolleri sayesinde %95 başarı oranı gösteren mutabakat sonuçları elde edilmiştir. Protokolün teorik ve analiz açıklamaları çalışmalarında ayrıntılı bir şekilde paylaşılmıştır.

(Lu vd., 2021) yapmış oldukları çalışmalarında frekans yan kanalları kullanılarak gönderen ve göndermeyen ikiz alan kuantum anahtar dağıtımı analiz edilmiştir. Yapılan analizlerde foton kaynağının pratik güvenliğinin önemini ortaya koymuştur. Protokolün pratik uygulamasında cihaz seçimi için elde edilen sonuçların referans olarak kullanılabileceği belirtilmiştir.

(Li vd., 2021) çalışmalarında yerel-yerel osilatör habercili hibrit lineer amplifikatör kullanılarak gerçekleştirilen sürekli değişken kuantum anahtar dağıtımı protokolü önerilmiştir. Önermiş oldukları protokolün test sonuçlarından amplifikatörlerin kullanılmasının, yerel yerel salınım tabanlı

sürekli değişken kuantum anahtar dağılımı sistemlerinin temel hızları ve iletişim mesafelerini artırabileceği ifade edilmiştir.

(Mao vd., 2021) çalışmalarında kuantum anahtar dağıtımı protokollerinde yüksek verimli sendrom tabanlı düşük yoğunluklu eşlik kontrolü uzlaşması algoritması önermişlerdir. Bu sayede boşa harcanan sendrom bilgisini tam olarak değerlendirerek mutabakatın bilgi kayıplarını azaltması sağlanmıştır. Teorik olarak ayrıntılı bir şekilde tanıtılan algoritmalarının test sonuçları, bilgi kaybı ve iletişim turlarının sayısında net azaltmalar olduğunu göstermektedir.

(Huang vd., 2021) çalışmalarında makine öğrenme algoritmaları kullanılarak güvenliği arttırılmış sürekli değişken kuantum anahtar dağıtımı protokolü önerilmiştir. Bu sayede sisteme yöneltilebilecek saldırı yöntemleri incelenerek makine öğrenmesi algoritması kullanılarak daha güvenli bir sistem elde edilmesine çalışılmıştır.

(Zhang vd., 2022) yapmış oldukları çalışmalarında kısmen güvenilir rölelere sahip kuantum anahtar dağıtımı ağlarında kullanılmak üzere topoloji soyutlaması tabanlı koruma protokolü önerilmiştir. Bu protokol güvenilir ve güvenilmeyen rölelerle çalışmaktadır ve gizli anahtarların çalışma ve koruma yollarını oluşturmaktadır. Protokolün teorik açıklaması ayrıntılı bir şekilde yapılmış olunup simülasyon sonuçlarında önermiş oldukları yöntemin kararlığı ve güvenilirliğinin yüksek olduğu paylaşılmıştır.

(Cardoso-Isidoro ve Delgado, 2022) çalışmalarında kuantum anahtar dağıtımını asimetrik çift kuantum ışınlamasını kullanarak geliştirmişlerdir. Önermiş oldukları bu yöntem, çift kuantum ışınlama tekniğinin kuantum anahtar dağıtımında kullanılabilirliği test edilmiş, gerçekleşebilecek saldırılar incelenmiş ve emsal yöntemlerle da karşılaştırılarak çalışmalarının farklılıkları açıklanmıştır.

(Cai vd., 2021) çalışmalarında kuantum kör, çoklu imza yönteminin endüstriyel blokzincirleri için uygulanabilirliği araştırılmıştır. Böyle bir çalışmayı yapmalarındaki amaç blokzincir sistemlerinin kuantum dönemi sonrası süreçte karşılaşabileceği kuantum saldırılarına karşı dayanıklı hale getirilmesidir. Araştırmacılar teorik olarak yapmak istedikleri işlemleri ayrıntılı

bir şekilde anlatmış ve önermiş oldukları eklentinin sağlayabileceği güvenlik artılarını açıklamışlardır.

(Gozzard vd., 2021) çalışmalarında uydu kuantum anahtar dağıtımı uygulamalarının yer tabanlı lazerlerde karşılaşabilecek kesintilere karşı güvenlik açıkları üzerinde durmuşlardır. Yapmış oldukları araştırmalar sonucunda karşılaşılabilecek sorunların giderilmesi ve önlem alınabilmesi için tespit ettikleri bilgileri ayrıntılı bir şekilde paylaşmışlardır.

(Xu vd., 2021) yapmış oldukları çalışmada yer-uydu bağlantı linkleri bağlantısı üzerinden sürekli değişken kuantum anahtar dağıtımı protokolü için gürültüsüz zayıflama optimasyonu kullanılarak yöntemini önermişlerdir. Bu yöntem sayesinde sürekli değişken kuantum anahtar dağıtımı protokolünün performansını iyileştirmek için kaynak hazırlamak için sıfır foton kataliz işlemi kullanılarak farklı bir şekilde gürültüsüz zayıflama yapılabilme imkânı elde etmişlerdir. Ayrıntılı bir şekilde konu açıklamasının yapıldığı çalışmada simülasyon sonuçları paylaşılmıştır.

(Jing vd., 2021) yaptıkları çalışmalarında ölçüm cihazından bağımsız sürekli değişken kuantum anahtar dağıtımı protokolünde gürültüsüz doğrusal amplifikatör kullanılarak performansı iyileştirilmiştir. Önerilen yöntemin teorik açıklaması ve simülasyon sonuçları ayrıntılı olarak çalışmalarında paylaşılmıştır.

(Xu vd., 2021) çalışmalarında pasif sürekli değişken kuantum anahtar dağıtımı protokolünde sonlu boyut etkisini dikkate alarak güvenlik analizi yapmışlardır. Simülasyonlarda farklı durumlar göz önüne alınarak testler gerçekleştirilmiş ve elde edilen sonuçlar paylaşılmıştır.

(Zheng vd., 2021) yapmış oldukları çalışmalarında karmaşık iletişim ortamında sürekli değişken ve ölçüm cihazından bağımsız kuantum anahtar dağıtımı protokollerinin güvenlik analizi yapılmıştır. Yapmış oldukları simülasyon ve analizlerin ayrıntılı olarak tanıtıldığı çalışmalarında elde ettikleri sonuçları paylaşmışlardır.

(Ahn vd., 2022) çalışmalarında kuantum korumalı kuantum sonrası dönem için kuantum anahtar dağıtımının dağıtılmış enerji kaynaklarının korunması için bir yöntem önerilmiştir. Bu sayede dağıtık enerji kaynakları kuantum anahtar

dağıtımı ve kuantum sonrası şifreleme algoritmaları kullanılarak korunması sağlanmıştır. Çalışmalarında önermiş oldukları yöntemin ayrıntılı açıklamasına yer verilmiştir.

(Zhu vd., 2022) çalışmalarında B92 protokolü kullanılarak modülasyonlu retro reflektörlü serbest alan kuantum anahtar dağıtımı protokolü önermişlerdir. Analiz ve simülasyon sonuçları incelendiğinde ihtiyaç duyulan çoklu kuantum kuyu modülatörlerinin sayısında düşme olduğu ifade edilmiştir. Ayrıca emsal protokoller düşük modülatör sönme oranı yahut yüksek optik yanlış hizalama durumlarında çalışmazken, araştırmacıların önermiş olduğu protokol çalışmaya devam etmiştir.

(Sun ve Huang, 2022) yapmış oldukları çalışmada pratik kuantum anahtar dağıtım sistemlerinin güvenlik açısından değerlendirilmesi yapılmıştır. BB84 algoritmasının kuantum saldırı ve hackleme durumlarına karşı değerlendirilmesi yapılmış ve kaynak, kodlayıcı, kod çözücü ve dedektör gereksinimleri dikkate alınarak incelenmiştir.

(Xie vd., 2022) çalışmasında sürekli değişken kuantum anahtar dağıtımı için derin sinir ağı algoritması tabanlı bir uzlaşma protokolü üzerinde durulmuştur. Elde edilen protokol yüksek hızla çalışmakta olup analiz sonuçları incelendiğinde karmaşıklığı azalttığı görülmüştür. Önerilen protokolün teorik ayrıntılı açıklaması ve simülasyon ve analiz bölümleri çalışmada paylaşılmıştır.

(Gao vd., 2022) yapmış oldukları çalışmalarında hatalarla öğrenme probleminden kuantum kimlik tabanlı şifreleme yöntemi önermişlerdir. Yöntemlerinin teorik açıklamaları ayrıntılı olarak çalışmalarında paylaşılmıştır. Önermiş oldukları şifreleme yönteminin güvenilirliği yine teorik olarak ispatlanmıştır.

(Wang vd., 2022) çalışmalarında kuantum anahtar dağıtım takımyıldızı ağlarının ağ fizibilitesi üzerinde durulmuştur. Kuantum anahtar dağıtım takımyıldızı ağlarının küresel anlamda kuantum ağını kurabilmenin yegâne yolu olduğu paylaşılan çalışmada araştırmacılar bu alanda yapılan çalışmaların az olması ve farkındalığın arttırılması için kapsamlı bir araştırma ve bilgilendirici açıklamalarda bulunmuşlardır. Yapmış oldukları simülasyonda güneş ışınlarının

kuantum anahtar dağıtım takımyıldızı ağlarının önündeki en büyük engel olduğu görülmüştür.

(Adnan vd., 2022) yapmış oldukları çalışmada 5G ağlarında kuantum anahtar dağıtımını çalışmışlardır. Bu alanda yapılan son teknolojik gelişmeler ve yapılması gereken çalışmalara odaklanmışlardır. Alan yazın şeklinde hazırlanan çalışma sayesinde kuantum anahtar dağıtımının 5G ağlarda nasıl uygulanabileceği kapsamlı bir şekilde tanıtılmış ve yapılan önceki çalışmalara da dikkat çekilmiştir.

(Abushgra, 2022) çalışmasında konvansiyonel sistem ölçümlerine dayalı kuantum anahtar protokollerinin varyasyonlarını ele almış ve ayrıntılı bir literatür taraması gerçekleştirmiştir. Kuantum anahtar dağıtımı protokollerinde kullanılan farklı varyasyonların ayrıntılı olarak değerlendirilmesi sebebiyle tezimizin literatür taramasında kullanılmıştır.

(Takaoğlu vd., 2021) yapmış oldukları çalışmada blokzincir teknolojisi ile steganografi bilimini birleştirerek yeni bir steganografi tekniği önermişlerdir. Blokzincir steganografisi olarak isimlendirdikleri bu çalışmalarında kapak multimedya olarak blokzincir sistemini kullanan araştırmacılar tekrar eden veri gizleme tekniği sayesinde kullanılan kapak multimedyasının boyutunun önemsiz hale gelmesine ve sınırsız veri gizleme imkânı elde edilmesini sağlamışlardır. Yapılan test ve analizlerde önermiş oldukları algoritma sayesinde steganaliz yöntemleri ve gizleme kapasitesi sorunlarına karşı güvenilir bir sistem elde etmişlerdir.

(Akhtar vd., 2021) çalışmalarında blokzincir teknolojisinden faydalanarak elektronik cihazlara gerçek zamanlı ve senkron erişim kontrolü yöntemi önermişlerdir. Blokzincir teknolojisini eklemelerindeki sebep; sistem erişim kontrolü, veri depolaması ve yönetimi, birlikte çalışabilirlik gibi sorunlarda karşılaştıkları sorunların çözümünde katkı sağlıyor olmasıdır. Çalışmalarında önermiş oldukları sistemi elektrikli araçların ve şarj istasyonlarının arasındaki mikro ödeme örneği üzerinden ele almış ve açıklamışlardır.

(Wang ve Li, 2021) yapmış oldukları çalışmada gizlilik koruma sistemi olan Healthchain ismini verdikleri blokzincir temelli bir medikal veri koruma sistemi önermişlerdir. Sağlık alanında blokzincir teknolojisinin eklenmeye

çalışıldığı birçok çalışma bulunmaktadır. Benzer bir çalışma olan bu örnekte de önerilen sistem teorik olarak gizlilik ve güvenlik sorunlarını çözmektedir. Kurumlar arası olabileceği gibi tıbbi kurumların bireysel olarak da sistemlerinde kullanılabileceği bu sistem sadece simülasyon ortamında test edilebildiği için gerçek hayat testlerinden gelen geri bildirimler ve karşılaşılan sorunların incelenebilmesinden uzak bir aşamadadır.

(Horng vd., 2021) çalışmalarında blokzincir temelli geri çevrilebilir veri gizleme yöntemi önerilmiştir. Bu yöntem tıbbi görsellerde kullanılmak üzere geliştirilmiştir. Ancak önerilen yöntem çalışmak için seçtiği görsel boyutlarının yüksek çözünürlüklü ve büyük boyutlarda resimlerden oluşması sebebiyle blokzincir sistemlerinde bulunan veri iletiminde kullanılabilecek bölümler için çok büyük ve doğal olarak uygulanabilir olmayan bir durumdadır.

(Zhang vd., 2021) çalışmalarında gizli iletişim modeli üzerinde çalışmışlardır. Blokzincir teknolojisini bu bağlamda inceleyen araştırmacılar akıllı sözleşmelerden faydalanarak elde etmek istedikleri gizli iletişim sistemini teorik olarak önermişlerdir. Bu sayede sahip oldukları sistemin blokzincir teknolojisi kullanılarak geliştirilmesi sebebiyle yapısal olarak kurcalanmalara karşı dayanıklı yapısı ve sistem uygulanabilirliğinin düşük kompleksli olması imkanına kavuşmuştur.

(Nguyen vd., 2020) çalışmalarında blokzincir teknolojisinden faydalanarak Vietnam için karşılaşılan diploma sahteciliğine karşı bir çözüm önerisi getirilmiştir. Blokzincir teknolojisinin kullanılması ile sertifika ve diplomaların doğrulanabileceği bir sistem önerilmiştir. Ayrıntılı olarak blokzincir teknolojisinin incelendiği bu çalışma Vietnam çapında uygulanabilecek bir sistem önerisi sunması açısından öneme sahiptir.

(Ali vd., 2021) araştırmacılar VisTAS ismini verdikleri sistemlerinde blokzincir temelli görünür yani kamuya açık ve güvenilir bir uzaktan kimlik doğrulama sistemi önermişlerdir. Blokzincir teknolojisinin imkân tanıdığı bu sistem önerisi benzer mimariyi takip ederek farklı alanlarda uygulanabilir yapıdadır. Yazarların önermiş olduğu kimlik doğrulama sistemi sertifika doğrulama sistemine yahut tapu/araç aidiyet sistemine çevrilebilir yapıdadır. Bu bağlamda önerilen sistem farklı alanlarda uygulanabilirliği ve blokzincir

teknolojisinin güzel sunulması sebebiyle tezimizde literatür bölümünde değerlendirilmiştir.

(Yeom vd., 2021) çalışmalarında blokzincir temelli işçi kontrat sistemi önermişlerdir. Ayrıca sistemlerinde şifreli anahtar kelimesi aramasına müsaade edilmektedir. Bu sistemde kullanıcılar sadece kendi kontratlarını görebilecekleri, siber saldırılara karşı dayanıklı, güvenliğin ve gizliliğin üst seviyede olduğu bir sistem elde edilmiştir.

(Pranto vd., 2021) yapmış oldukları çalışmada blokzincir teknolojisi ve akıllı sözleşmeler kullanılarak nesnelerin interneti imkanlarıyla birlikte akıllı tarım uygulamaları için bir öneride bulunulmuştur. Sahada üretilen verilerin nesnelerin interneti sayesinde blokzincire aktarılması ve akıllı sözleşmeler vasıtasıyla ilgili taraflara ulaştırılması amaçlanmıştır. Blokzincir teknolojisi kullanıldığı için sistem güvenliği yüksek, kurcalanamaz ve şeffaf bir sistem elde etmişlerdir.

(Hussein vd., 2019) çalışmalarında biyomedikal verilerin yönetimi için blokzincir temelli bir teknik önermişlerdir. İki blokzincir sistemi geliştirip birlikte çalışması üzerine bir sistem planlamışlardır. Anahtar kelimesi aramasına müsaade edilen ve farklı veri türlerinin sistemde kullanılabildiği güvenli ve hızlı çalışan bir sistem önermişlerdir. Test ve analiz bölümünde önermiş oldukları sistemin simülasyon sonuçları ayrıntıları ile paylaşılmıştır.

(Yu vd., 2021) çalışmalarında yeni bir konsensüs protokolü önermişlerdir. Blok sıkıştırması yöntemi kullanılarak çokça kullanılan işin ispatı algoritması optimize edilmiştir. İşin ispatı algoritmasının blokzincir sistemlerinde önerilen ilk konsensüs protokolü olduğu ifade edilmiştir. Ancak bu konsensüs algoritmasının masraflı ve çok enerji harcayan yapıda olduğu paylaşılmıştır. Araştırmacıların önermiş oldukları yöntemde ise enerji tüketimi açısından daha çevreci bir çözüm üretildiği ifade edilmiştir.

(Zoughalian vd., 2022) çalışmalarında sahtecilik girişimlerinin olmaması için blokzincir temelli güvenliği yüksek bir ilaç dağıtım sistemi önerilmiştir. Sistemleri dağıtılmış verilerin bütünlüğümü sağlamak için sıfır bilgi kanıtı protokolünü kullanmaktadır. Araştırmacıların sistemlerinde her bir düğüme itibar puanı vermiş ve düğüm güvenilirliğini tespit etmeye çalışmıştır, bu

amaçla Markov modeli tanıtılmış ve kullanılmıştır. İlaç sahteciliğinde önerilen sistemin karar verme, gizlilik, bütünlük ve uygulanabilirlikte güvenilir bir yöntem olduğu ifade edilmiştir.

(Takaoğlu vd., 2019) araştırmacılar çalışmalarında blokzincir teknolojisini ayrıntılı olarak açıklamış ve bu teknolojinin uygulanabileceği alanları tespit etmiştir. Ayrıca Türkiye'de belirlenen blokzincir teknolojisinin uygulama alanlarının ne şekilde gerçekleştirilebileceği bilgisi ve tavsiyeler paylaşılmıştır.

(Asif vd., 2022) çalışmalarında akıllı şehirlerde kullanılması için blokzincir temelli kimlik doğrulama ve güven yönetim sistemi önermişlerdir. Nesnelerin interneti ortamında görülen çeşitli güvenlik sorunlarının blokzincir altyapısı sayesinde giderilmesi amacıyla Ethereum blokzincir platformundan yararlanılarak uygun eklentiyi gerçekleştirmişlerdir. Önermiş oldukları algoritmayı test etmişler ve elde ettikleri sonuçları ayrıntılı bir şekilde paylaşmışlardır.

(Lin vd., 2022) yapmış oldukları çalışmalarında nesnelerin interneti için geliştirilen uygulamalar için akıllı sözleşmelerin kullanıldığı konsorsiyum blokzinciri sistemi önermişlerdir. Blokzincir sistemlerinin açık, özel, konsorsiyum şekillerinde geliştirilebilir olduğu ifade edilen araştırmada, blokzincir sisteminde kullanılabilen ve önceden belirlenen özel bir durum her gerçekleştiğinde aynı işlemi yapan ufak kod parçalarına akıllı sözleşme denilen yapıların kullanıldığı ifade edilmiştir. Sistemleri ile ilgili gerekli teorik açıklama ve simülasyon çalışmaları ayrıntılı olarak çalışmalarında paylaşılmıştır.

(Choi vd., 2022) araştırmacılar çalışmalarında Kore için 2030 sürdürülebilir kalkınma hedefleri doğrultusunda eğitimin önemi ve gerçekleştirilebilmesi için blokzincir merkezli eğitim programlarını paylaşmışlardır. 704 ilkokul öğrencisi üzerinde denedikleri sistemlerinin sonuçlarını ayrıntılı olarak çalışmalarında paylaşmışlardır.

(Lee, 2022) yapmış olduğu çalışmada blokzincir teknolojisindeki yeni trendleri konu olarak ele almışlardır. Literatür taraması ağırlıklı yapılan bu çalışmada blokzincir teknolojisi tanıtılmış ve yeni trendler hakkında bilgiler paylaşılmıştır. Blokzincir teknolojisinin ilk ortaya koyduğu başarılı ürün olarak

kabul edilen Bitcoin kripto parasının finans konulu bir çalışma olması ve sonrasında teknolojinin farklı alanlarda uygulanmaya çalışılması ve günümüzde takas edilemez jeton ve kurgusal evren gibi yeni trendlerin dikkat çekmesi üzerine geniş ve açıklayıcı bir çalışma yapılmıştır.

(Kwak vd., 2022) araştırmacılar çalışmalarında EggBlock ismini verdikleri bir platform tanıtımı yapmışlardır. Uç tabanlı nesnelerin interneti sistemlerinde solar enerji tesislerinde üretilen elektrik ticaretini ele alan blokzincir temelli bir sistem tanıtılmıştır. Gerekli açıklamalar ve sistem analizleri ayrıntılı olarak çalışmalarında paylaşılmıştır.

(Shih vd., 2022) çalışmalarında Hyperledger Fabric blokzincir platformunu kullanarak endüstriyel nesnelerin interneti için bir erişim kontrolü protokolü önermişlerdir. Nesnelerin internetinde karşılaşılan sorunların belirtildiği çalışmada kendilerinin önermiş olduğu sistemde bu sorunların nasıl giderilebileceği ayrıntılı olarak açıklanmıştır.

(Chin vd., 2022) yapılan çalışmalarında blokzincir sistemlerinde çokça kullanılan işin ispatı algoritmasında kullanılan algoritma zorluğu ele alınmıştır. Algoritma zorluğunun blokzincir sistemlerinin sürdürebilirliği açısından çok önemli olduğu paylaşılan çalışmada araştırmacılar genetik algoritmalarından faydalanarak işin ispatı algoritması için zorluk belirleme sistemi önermişlerdir. Yapmış oldukları test ve analiz kısımların elde edilen sonuçlar incelendiğinde ciddi oranda iyileştirmeler elde ettikleri görülmektedir.

(Varavallo vd., 2022) çalışmasında takip edilebilir ve sürdürülebilir bir yeşil blokzincir sistemi önerisinde bulunmuşlardır. Günlük süt üretimi yapılan bir tesis örnek edilerek yapılan çalışmada tedarik zinciri blokzincir kullanılarak kayıt altına alınmış ve yenilikçi bir yöntemle bu süreç gerçekleştirilmiştir. Gerekli teorik açıklamalar ve test sonuçlarının analizi çalışmalarında paylaşılmıştır.

(Wang vd., 2022) çalışmasında Çinli araştırmacılar ulusal güvenilir veri depolama altyapısı hakkında araştırma yapmışlardır. Ülke seviyesinde veri kaydı süreçlerinde görülen eksikliklerin ve bunların çözümünde blokzincir teknolojisinden de faydalanarak yenilikçi ve alternatif çözüm önerilerini paylaşmışlardır.

(Lo vd., 2022) çalışmalarında GLASS ismini verdikleri blokzincir temelli bir sistem önermişlerdir. Bu sistemde e-devlet mantığıyla vatandaş merkeziyetçi (ademi merkeziyetçi) dağıtık bir veri paylaşım yapılması öngörülmektedir. Önermekte oldukları sistemin ayrıntılı teorik açıklamalarının yapıldığı, test ve analizlerinin sonuçların paylaşıldığı çalışmaları, blokzincir teknolojisinin bir ülke geneli örneğinde veri paylaşımının gerçekleştirilmesi hususunda sağlamış olduğu yenilikçi katkıları sebebiyle tezimizde incelenmesine karar verilmiştir.

(Meidute-Kavaliauskiene vd., 2022) araştırmacılar yapmış oldukları araştırmalarında blokzincir teknolojisinin kan tedarik zincirinde kullanılması ve karşılaşılan sorunların giderilmesinde katkı sağlaması konusuna odaklanmışlardır. Kan tedarik zincirinde görülen eksikliklerin ayrıntılı bir şekilde tanıtıldığı çalışmada blokzincir teknolojisinin katkı sağlayacağı hususlar ön plana çıkartılmış ve gerekli açıklamalara yer verilmiştir. Farklı uygulama alanlarında blokzincir teknolojisinin uygulanabilirliğinin görülmesi açısından kıymetli bir çalışmadır.

B. Problem Tanıtımı

Bu doktora çalışmasının ait olduğu temel bilim dalı, bilgi ve bilişim güvenliğidir. Bu alan içerisinde şifreleme anahtarları ve anahtar dağıtım senaryoları önemli bir alan kapsamaktadır. Güncel bilime katkıda bulunulmak istenilen alan ise gerçekleştirilmek istenilen işlemlerde meydana gelen performans ve/veya tercih edilebilirliği etkileyen negatif parametrelerin azaltılmasıdır. Bu doktora çalışma konusunda azaltılması düşünülen sorun kuantum anahtar dağıtımı algoritmalarında oluşmakta olan kuantum artık bit'lerdir. Bu bit'lerin azaltılması ile kullanılan yöntemlerin tercih edilirliği arttırılmak istenilmektedir. Kullanılan anahtar dağıtımı algoritmaları sonrasında oluşan artık bit'lerin azaltılması amacı ile önerilen yöntemlerimiz yapay zekâ ve sınıflandırma algoritmaları içermektedir. Test edilen yöntemler BB84 algoritması üzerinden test edilmiştir.

C. Önerilen Yöntem

Tezimizde kuantum anahtar dağıtımı sürecinde görülen artık bitlerin azaltılması ve daha verimli olarak alıcı tarafa iletilmesi üzerine çalışılmıştır. Makine öğrenmesi algoritmaları bu doğrultuda incelenmiş ve test edilmiştir. Elde edilen sonuçlar paylaşılmış ve kullanılması gereken ve kullanılmaması gereken algoritmalar sebepleriyle birlikte izah edilmiştir. Son olarak blokzincir teknolojisini kuantum bit iletimi sürecinde açık kanal yerine kullanmaya çalışılmıştır. Tezin ilgili bölümünde yapılan çalışma paylaşılmış olup ilgili akademik yayın çalışması SCI-E bir dergide yayın aşamasındadır.

D. Tezin Bilime Katkısı

Tez çalışmamızda ele alınan konu kuantum hesaplama ile ilgili olması sebebiyle ve kuantum hesaplama algoritmalarının ortaya atıldığı süreçten bu yana karşılaşılan sorunların giderilmesi hususunda süregelen bir çalışmalar dizisi olması sebebiyle tezimizde üzerinde durulan artık bitlerin azaltılması konusundaki çalışmalarımız bu alanda yenilikçi bir özelliğe sahiptir Gerek makine öğrenmesi algoritmaları sayesinde farklı oranlarda elde edilen başarılı sonuçlar gerekse de blokzincir teknolojisinin kuantum bitlerinin iletiminde kullanılması neticesinde artık bir sorununun hibrit bir şekilde günümüz koşullarında çözümü önerilmiştir. Kuantum bitleri geleneksel sistemlerde fiber kablolarla taşınan foton yani ışıklar olması sebebiyle karşılaşılan artık bit durumu, günümüzde kuantum hesaplama süreçlerinde fotonların ikili sisteme çevrilmesi ve silikon bazlı bilgisayarlarca test edilmesi sebebiyle daha da fazla artık bir oluşmasına sebebiyet vermektedir. Blokzincir teknolojisi ikili yapıya dönüştürülen kuantum bitlerinin kayıpsız bir şekilde alışılageldik kuantum anahtar dağıtımı protokollerinde kullanılmasına imkân tanımaktadır. Bu bağlamda gerçekleştirilen tez çalışmasında, kuantum anahtar dağıtımı protokollerinde makine öğrenmesi algoritmalarının kullanımı sayesinde artık bitlerin azaltılması noktasında daha iyi sonuçlar elde edilmesinin yanı sıra blokzincir teknolojisinden de yararlanarak alternatif bir hibrit kuantum anahtar dağıtımı yöntemi önerilmesi açısından da bilime müspet katkıları olmuştur.

II. BİLGİ GÜVENLİĞİ VE KRİPTOLOJİ

Veri güvenliği bilginin önemli olduğu ve gizlenmesi gerekli bilgilerin öneminin anlaşılmasından bu zamana kadar var olmakta ve gelişmektedir. Bilgi güvenliği ilk olarak bilginin gizlenmesinde başlanmış ve daha sonrasında adım adım gelişerek günümüzdeki halini almıştır. M.Ö. 450-500 yıllarına kadar uzanan bir zamanda yazılı notları bulunan Herodot zamanında bilginin gizlenmesi ile ilgili kaynaklardan bahsedilmektedir. Dolayısı ile bilgi güvenliğinin bu zamanlardan başladığı düşünülebilir. Bilgi gizlenmesi, gizli anlamındaki "steganos" ve yazma anlamındaki "graphein" kelimelerinin birleşmesinden oluşan "staganography"-"steganografi" olarak dilimize geçmiştir. Kelime anlamı olarak gizli yazma anlamına gelmektedir. Sonrasında bilgi güvenliği inceleme çalışmalarından biri olan kriptoloji ile ilgili başarılı örneklere rastlanmıştır. Bu örneklerden biri Roma İmparatoru Gaius Julius Sezar tarafından geliştirildiği düşünülen Sezar şifrelemesidir. Bu yöntemde roma alfabesinde bulunan harfler, 3 harf sonrasındakiler ile değiştirilip kullanılarak metine dökülmüş ve okunması engellenmeye çalışılmıştır. Roma döneminde bu tarz bir şifreleme yöntemi hali hazırda okur yazarlık durumu düşük olan Galya'lılar için belirli bir süre efektif bir çözüm olabileceği düşünülebilir.

Dünya savaşı zamanlarında hem kriptoloji hemde steganografi alanlarında başırılı örnekler ve uygulamalar olmuştur. Bu dönemde mikro yazıların kullanımı ve almanların geliştirmiş oldukları enigma şifreleme cihazı kullanılmıştır. Kriptoloji sistemini kuran ve geliştirdiği algoritma ile verilerin güvenliğini sağlayan kişilere kriptolojist, var olan kripto sistemlerini anlayarak şifreli mesajların çözülmesini sağlayan kişilere ise kriptanalist denilmektedir. Benzer bir durumda steganografi işlemlerinde bulunmaktadır. Steganografi işlemlerini gerçekleştiren kişilere steganograf, var olan sistemlerin ve algoritmaların çözülmesi için çalışan kişilere ise steganalist denilmektedir. Günümüzde tüm bu sistemlerin dijital ortamlarda birlikte kombinasyonlar dahilinde kullanılması ile birlikte var olan bir sistemi ve/veya mesajı savunmaya ve korumaya yönelik işlemler yapan kişiler ve bu güvenlik unsurlarını aşmaya çalışan kişilere "hacker" denilmektedir. Bu kişileri birbirilerinden ayıran

belirteçler ise kullandıkları siyah, beyaz ve gri ön sıfatlarıdır. Benzer şekilde algoritmaların tanıtılması işlemlerinde "hacker" ibaresinin yerine "3.şahıs", "eavesdropper - kulak misafiri " ifadeleri kullanılabilmektedir.

Teknolojinin ilerlemesi ile birlikte fiziksel steganografi ve kriptoloji örnekleri yerini dijital versiyonlarına bırakmıştır. Günümüzde dijital ürünlerin aitlik durumlarında başlanılarak, haberleşme sistemlerinde veri akışları ve tüm bankacılık sistemleri yukarıda bahsedilen bilim dallarının ürünleri ile korunmakta ve güvenlik altına alınmaya çalışılmaktadır.

A. Kriptoloji

Kriptoloji kelimesi dilimize antik Yunan dilinde gizli anlamına gelen "cyrptos" ve yazma anlamına gelen "graphein" kelimelerinin birleşiminden girmiştir. Bu iki kelimenin birlikte kullanımı ile birlikte gizli yazma anlamına gelen kriptoloji kelimesi türeyerek dilimize girmiştir. Steganografi benzer bir şekilde "steganos" saklı, saklanmış anlamına gelen bir kelime kökünün sonuna yazma eki getirilmesi ile oluşturulmuştur. Başlangıçta birbirileri ile benzer işlemler yaptıkları düşünülse bile steganografi bir bilginin gizlenmesi, farkına varılamaması üzerine çalışmakta iken, kriptolojinin temel amacı o bilginin yetkisiz kişiler tarafından farkına varılsa bile okunamayacak şekilde bulundurulması durumudur. İki yönteminde birbirilerine göre avantajları ve dezavantajları bulunmaktadır. Kriptoloji sistemleri steganografi sistemlerine göre nispeten çokça verileri daha güvenilir algoritmalar inşa edip kullanmakta iken, steganografi sistemleri çok daha kısa bilgilerin görünürlük unsurunu ortadan kaldırarak bulunmak istenilen bilginin farkına varılma durumunu engellemektedir. Farkına varılamayan bir unsurun çözülmesi üzerine uğraşmak genel olarak tüm işlemlerin başlangıcında sorunlarımızın çözülmesini sağlayacaktır. Günümüz teknolojilerinde ise bu iki unsuru belirli şartlar altında birlikte kullanmak ve başarılı sonuçlar elde etmek mümkündür.

Tez konumuzun daha yakın olduğu çalışma alanı ise kriptoloji bilimidir. Kriptolojide öncelikle terminolojik birkaç veri paylaşımı yapılması gereklidir. Kriptografi şifreleme algoritmaları ve şifreleme anahtarları kullanılarak veri gizleme işlemidir. Gizlenen verilerin anahtar bilgisine sahip olmaksızın incelenmesi ve çözülmeye çalışılmasına kriptanaliz denilmektedir. "Plain Text" şifrelenecek olan bilgi bloğuna verilen addır. Bu veriyi şifreleyen algoritmaya "Cipher", şifreleme

işlemine “Encrypt” ve bu işlem sonrasında oluşan veriye ise “CipherText” denilmektedir. Şifrelenen metnin çözülmesi işlemi “Decrypt” olarak adlandırılmaktır. Bu işlemden sonra ilk baştaki “Plain Text” elde edilmiş olur.

Şifreleme algoritmaları kullandıkları anahtar değerinin paylaşım türüne göre ikiye ayrılmaktadır. Simetrik şifreleme algoritmaları ve asimetrik şifreleme algoritmaları olarak iki ana gruba ayrılırlar. Simetrik şifreleme algoritmalarının temel avantajı hızlı çalışan sistemler olmasıdır. Bu şifreleme yönteminde taraflarca bilinen bir adet gizli şifre anahtarı taraflarca bilinmektedir. Bu anahtardan şifreleme ve şifre çözümü işlemlerinde faydalanılmaktadır. Simetrik şifrelemenin bilinen örnekleri olarak Blowfish, AES, RC4, DES, 3DES algoritmaları örnek gösterilebilir.

Blowfish şifreleme yöntemi, 23 bit ile 448 bit arasında anahtar uzunluklarına sahiptir. Çalışması için 4096 byte uzunluğunda RAM belleğine ihtiyaç vardır. Bu şartın sağlanamadığı gömülü sistem içeren küçük devrelerde kullanılamazlar.

DES şifreleme algoritması bir sonraki bölümde açıklanacak sebeplerden ötürü tedavülden kaldırılmıştır. Kullanımdan kalktığı zamana kadar en çok kullanılan simetrik şifreleme algoritmalarından bir tanesiydi. Bloklar halinde şifreleme yapan DES algoritması 64Bit içeren veri bloğunu şifrelemek için 56 bit’lik bir anahtar serisi kullanır. Anahtar boyutunun veri bloğuna göre kısa olmasının dezavantaj olmasından sonra daha güçlendirilmiş bir sistem olan 3DES, 3 kez ardı ardına DES şifreleme yapan sistem önerilmiştir. 3DES şifreleme algoritması DES’e göre 3 kat daha yavaştır. AES’in çıkması üzerine NIST raporu ile kullanılmadan kaldırılmıştır. AES’e göre 6 kat daha yavaş çalışan bir algoritmadır.

DES algoritmasının anahtar uzunluğunun mesajdan kısa olmasının oluşturduğu dezavantaj göz önüne alınarak DES’in sağlamlığı üzerine testler arttırılmış olup, bu şifreleme yönteminin kırılabildiği ispatlanmıştır. Daha güncel ve sağlam bir şifreleme sistemi üzerine DES’in zayıf yönleri dikkate alınarak şifreleme algoritması geliştirilmek istenilmiş ve AES simetrik şifreleme algoritması üretilmiştir. DES şifrelemede olduğu gibi bloklar halinde şifreleme işlemi yapar, blok uzunluğu olarak 128, 192 ve 256 bit anahtar uzunluklarında çalıştırılabilmektedir. Kaba kuvvet olarak adlandırılan, tüm anahtar ihtimal havuzunu test eden “brute force” ataklara karşı bir dönem oldukça güvenilir olduğu düşünülmekteydi ancak güncel teknolojide yaşanan son gelişmeler sonrasında kırılabilir olduğu düşünülebilir.

RC4 şifreleme algoritması en az MB/sn seviyesinde hız gerektiren uygulamalarda kullanılmaktadır. Güvenliği üretilen anahtarın ne kadar çok rastgele oluşuna bağlıdır. Anahtar uzunluğu değişebilir ancak genellikle 128 veya 256 bit uzunluğunda bir RC4 şifrelemesi güvenilir olarak kabul görebilir. Günümüzde kullanılan rastgele sayı üreteçlerinin sistem mimarisi ve arka planlarında kullanılan mantık süper bilgisayarlar ve kuantum bilgisayarlar tarafından üretilmediğinden dolayı brute force ataklara karşı güvenilirliği tartışılabilir.

Diğer bir algoritma türü olan Asimetrik Şifreleme Algoritmaları ise farklı olarak iki farklı şifreleme anahtarı kullanmaktadır. Bu anahtarlardan bir tanesi tarafların bildiği ve ulaşılabilir bir açık anahtar verisidir. Bu açık anahtar verisi "Public Key" olarak adlandırılır. Ancak şifrelemenin çözülebilmesi için PublicKey ile matematiksel olarak bağlantılı özel anahtar kullanılması gereklidir. Bu özel anahtar "Private Key" olarak adlandırılır. Açık anahtar kullanılarak şifrelenen dokümanın şifrelenmesinin çözülebilmesi için özel anahtarın kullanılması gerekmektedir. Bu sistemin geliştirilmesindeki temel amaç iletişim kanalının uçlarında yer alan tarafların güvenlik anahtarı dağıtımlarını daha güvenli bir şekilde yapabilmesidir. Bu yöntem internet sistemlerinde haberleşmede güvenliği sağlayıcı ve SSL-Secure Sockets Layer'in gelişmiş hali olan TLS-Transport Layer Security'de kullanılmaktadır. E-posta haberleşmesinde güvenliği sağlamak içn kullanılan PGP-Pretty Good Privacy protokolü buna örnek olarak gösterilebilir. (D-H) Diffie-Hellman anahtar değişimi yöntemi ve bunun yanısıra RSA (Rivest-Shamir-Adleman), ElGamal, DSA (Digital Signature Algorithm) ve ECC (Elliptic Curve Cryptography) asimetrik şifreleme sistemlerine örnek olarak gösterilebilir.

RSA asimetrik şifreleme algoritması çok büyük asal sayıların üzerinden işlem yapma zorluğuna dayanarak geliştiricisi olan üç bilim adamının isimlerinin baş harflerini alarak bilim dünyasına duyurulmuştur. Günümüzde hızlı işlem gerektirmeyen sistemlerde halen daha kullanılabilmektedir. Fazla band genişliği kullanması ve büyük asal sayıları işlem yapmakta kullanmasından dolayı yavaştır ve ağ sistemleri, bankacılık ve benzeri alanlarda tercih edilmemektedir.

ElGamal yöntemi ise Diffie-Hellman anahtar alışverişi yöntemini baz alan açık anahtarlı asimetrik şifreleme yöntemidir. Anahtar üretimi, şifreleme ve şifre çözümü aşamalarından oluşmaktadır. ElGamal GNU Privacy Guard yazılımında, PGP'nin son versiyonlarında ve başka kriptosistemlerde kullanılmaktadır. Bu yöntem soyut

algebra'nın bir alt dalı olan grup teorisinde kullanılan döngüsel veya monojen olarak adlandırılan döngüsel nesneleri ve ayrık logaritma kullanan bir şifreleme algoritmasıdır. DSA algoritmasının temelinde de ElGamal algoritması yer almaktadır.

ECC yönteminde ise simetrik şifreleme tanım olarak sonlu cisimler üzerindeki eliptik eğrilerin cebirsel topolojisinin kullanımını esas alan bir asimetrik şifreleme sistemidir. Bu yöntem avantaj olarak diğer yöntemlere göre nispeten daha ufak boyutlarda anahtar değeri tutar. Genel olarak asimetrik şifreleme sistemlerinde bir anahtar oluşturulduğu zaman açık ve gizli anahtarlar iki veya daha fazla çok büyük asal sayının çarpılması ve/veya bu sayının çarpanlarına ayrılmasının zorluğuna dayanır. Bu algoritmada ise sistem eliptik bir eğrinin bilinen bir noktasına göre ayrık logaritma değerinin hesaplanmasının imkansız olduğu durumu kullanmaktadır. Bu durum eliptik eğrilerin ayrık logaritma problemi olarak adlandırılmaktadır. Eliptik eğrinin boyutu ile problemin zorluğu doğrusal bir ilişki göstermektedir. Eliptik eğrinin boyutu arttıkça problemin zorluğuda artmaktadır. Bu yöntem diğer yöntemlere çözülmesinin zorluğundan dolayı daha küçük şifreleme anahtarı boyutlarına sahip olabilmekte ve buna rağmen diğer başarılı şifreleme algoritmaları ile benzer güvenlik seviyesi sunabilmektedir. Süper bilgisayarlar ve kuantum bilgisayaların da dahil olduğu güncel teknolojilere karşı ECC algoritmasının halen daha güvenilir bir şifreleme yöntemi olabileceğini düşünen belirli otoriteler mevcuttur.

B. Şifreleme Anahtarı Problemleri

Günümüzde hayatımızın birçok alanında şifreleme algoritmaları yer almakta ve aktif bir şekilde kullanılmaktadır. Genel olarak dijitalleşen bir ürün veya hizmet kullanıldığı durumlarda, veri aktarmının olduğu herhangi bir sistemde güvenlik ve güvenilirliğin temel unsuru olarak uygun şifreleme algoritmalarının kullanımı ile sağlanmaktadır. Güvenlik ve güvenilirliğin sarsıldığı veya tehlike düştüğü durumlardan biri şifreleme işleminde kullanılan gizli anahtarların açığa çıkması durumudur. Şifreleme algoritmalarında tarafların bir araya gelmesi ve önceden bir şifre havuzu üzerinde anlaşması mümkün olmadığında ve anlaşılan şifrelerin fiziksel olarak saklanmasının çok güvenli olmadığı düşünüldüğünde uzak mesafelerden tarafların birbirilerini görmeden ve fiziksel olarak şifrelerini bildirmeden, düzenli

olarak sıkça şifrelerini değiştirerek bu algoritmaları kullanabilmeleri oldukça önemlidir. Ancak kullanılan altyapı sistemleri ve teknolojiler iletişim ağlarının dinlenebilmesine imkân sağlamaktadır. İşlem gücü yüksek siper bilgisayarlar ve geliştirilecek kuantum bilgisayarları ile kullanılan çoğu şifrelerin ve algoritmaların gerçersiz kalacağı düşünülmektedir. Hali hazırda "man in the middle" veya "mirrorring- aynalama" yöntemleri ile şifre havuzları hakkında bilgi sahibi olunabilmektedir.

Günümüzde simetrik şifreleme yöntemlerinden AES ve DES algoritmaları güncel olarak kullanılmaktaydı. Daha önceki dönemlerde DES ve 3DES algoritmaları daha popüler olup 2018 yılında NIST'in yayınlamış olduğu bir rapor ile resmen kullanımdan kaldırılmıştır. DES yerine tercih edilmeye başlanılan yöntem olan AES-Advanced Encryption Standart ise, daha uzun boyutlarda şifre anahtalarını kullanabilmektedir. NIST'in talep ettiği özellikler geliştirilecek olan şifreleme sisteminin hem yazılım tabanlı hemde donanım tabanlı sistemlerde kullanılabilir olmasıdır. DES şifreleme sistemleri daha çok donanım tabanlı işlemlerde kullanıldıklarından üst seviye yazılım içeren sistemlerin taleplerini karşılamada yetersiz kalmaktaydı, dolayısı ile geliştirilen AES şifreleme sistemleri donanımsal ve yazılımsal tüm platformlarda çalışmaktadır. DES ve 3DES algoritmları "brute force"- "kaba kuvvet" atak olarak adlandırılan tüm şifreleme anahtarları ihtimal havuzunun test edildiği sistemlere karşı dayanıksız olarak çıkmakta ve aynı zamanda sistemin işleyişini yavaşlatmaktadır.

Şifreleme sistemlerinde karşımıza çıkan temel problemler; gelişen teknolojiye karşı güçlü olmamaları, ürettikleri anahtarların gerçek rastgelelikten uzak olması ve üretilen anahtarların mevcut iletişim kanalları üzerinden güvenli bir şekilde paylaştırılamıyor olmasıdır. Asimetrik şifrelerin geliştirilme mantığı üretilen şifrelerin güvenilir bir biçimde paylaştırılabilir olmasını sağlamaktır. Bu amaçla ilk üretilen yöntem Diffie Helman yöntemi -DH- olmuştur. Bu yöntem iletişimin her iki ucunda bulunan tarafların güvenli olmayan bir kanal üzerinde güvenilir bir şekilde şifreleme anahtarında karar kılarak paylaşabilmesini amaçlamaktadır. Bu yöntem ile temel olarak şifrelemede kullanılan gizli anahtarın taraflar arasında paylaştırılması işlemi yapılmaktadır. Ancak üretilen şifreler halen tam anlamı ile rastgele değildir ve ilerleyen teknoloji sayesinde süper bilgisayarlar ve kuantum bilgisayarlar aracılığı ile başarılı tahmin ve tespit işlemleri gerçekleşebilir.

Süper bilgisayarların ve kuantum bilgisayaların yaygınlaşabileceği bir ortamda var olan teknolojiler ile güvenlik sistemlerinin sağlamlığı ve günvenilirliği ciddi bir şekilde sorgulanacaktır. Gelişen sistemlere ayak uydurarak şifreleme sistemlerinin temelinde yer alan anahtar üretme ve dağıtma sistemlerinde araştırma geliştirme çalışmalarına başlanılmıştır. Bu doğrultuda kuantum anahtar üreteçleri ve anahtar dağıtım senaryoları geliştirilmiştir.

C. Kuantum Anahtar Dağıtımı

Tezin üst bölümlerinde, geçmişten günümüze kadar sırası ile aktarılan veri güvenliği sistemleri, uygulama alanları ve yöntemleri, kullanılan metotlar, bu metotların avantaj ve dezavantajlarından bahsedilmiştir. Son olarak güncel olarak kullanmakta olduğumuz sistemler ve bu sistemlerin zaafları aktarılmıştır. Temel olarak üretilen şifreleme anahtarlarının, şifreleme sistemlerinin güvenilirliğinin test edilebilir olması gerektiğinden herkese açık olması ve test edilerek sonrasında herkes tarafından kullanılmaya başlanmasından dolayı özellikle güvenlik yükünün kullanılan şifreleme anahtarlarına yüklemiştir. Kullanılan şifreleme anahtarlarının rastgele sayılardan oluşması ve tahmin edilemez olması gerekmektedir. Üretilen şifrelerin rastgele olması şartı belirli bir oranda sağlandıktan sonra bu anahtar verilerinin güvenli bir şekilde paylaşılması gerekmektedir. Şifrenin paylaşılması üretilmesi kadar önemli bir husustur. Aynı zamanda kullanılan iletişim altyapısının öğeleri de şifreleme sistemlerinin güvenliğini ölçen önemli bir parametredir. Kullanılan iletişim altyapısında iletişimde taraf olmayan 3. şahısların kolayca hatta girebilmesi ve veri aktarımını dinleyebilmesi ve dahi aktarılan verileri kopyalayabilmesi mümkündür. Bu aşamada halen daha var olan sistemlerin güvenli olarak düşünülüp kullanılmasının sebebi verinin aktarım esnasında ve aktarımından sonra belirli bir süre öneminin korunuyor olabilmesidir. Kriptoanaliz yapan taraflar hatta girip, ilgili verileri kopyalayabiliyor olsalar bile, kullanılan şifreleme algoritmalarının sağladıkları güvenli anahtar havuzu ihtimalleri ve saldırgan tarafın kullandıkları cihazların bu anahtar havuzunu egale edebilecekleri süre verinin ilgili taraflar arasında paylaşılıp gerekli aksiyonların alınmasından sonra verinin hali hazırda sahip olduğu önemi yitirmesine kadar geçen süreyi geçmemektedir. Ancak belirli bir süre sonra kullanılan teknolojiler ve yöntemlerin gelişmesi ile bu kritik süreç içerisinde mesajların çözülebilmesi işlemi gerçekleşebilir. Bunun sebebi olarak

daha öncede bahsedildiği gibi gelişen süper bilgisayarların yaygınlaşması ve kuantum bilgisayarların yaygınlaşması örnek gösterilebilir.

Kuantum cihazların işlem güçlerine karşı kuantum sistemleri kullanılarak gerekli güvenlik aksiyonları alınmaya başlanmıştır. Bu işlemlere örnek olarak fiber hatlar kullanılarak veri aktarımının kuantum fiziğinde yer alan fotonlar ile yapılması gösterilebilir. Fotonlar ilerleyen bölümlerde bahsedileceği gibi kuantum fiziği kurallarına göre kopyalanamazlık özelliğine sahiptirler. Yani foton ile haberleşme yapılan bir sistemde, fotonlar üzerinde herhangi bir değişiklik yapmaksızın ağı dinleyemezsiniz ve fotonları kopyalayamaz- klonlayamazsınız. Benzer bir şekilde bu özelliklerden faydalanarak oluşturulan anahtar dağıtım sistemlerinde kullanılan anahtar uzunluğunun arttırılması ile iletişim hattına girip dinleme işlemi yapmak isteyen bir kişi kolaylıkla varlığını sezdirip, tarafların başka bir iletişim hattına geçmesine sebep olabilir.

Kullanılan kuantum cihazlarının günümüzde kullanılan transistor temelli bilgisayalardan farklı olarak 1 ve 0 kombinasyonları ile değil, fotonun süper pozisyon adı verilen durumundan ötürü belirli bir süreç içerisinde 0 ve 1 arası tahmin edilemez çoklu olasılıklarda değerde olabilecek olmasıdır. Böylelikle normal bilgisayarlardan farklı olarak tekil kıyaslama işlemindan bağımsız olarak birden fazla ihtimali aynı anda işleyebilir ve sonuçlandırabilir. Bu özelliği sayesinde normal bilgisayarların brute force ataklarında harcadıkları süreleri çok daha aşağı sürelere çekmektedir.

1. Kuantum Terminolojisi

Bu alanda kuantum anahtar üretimi ve dağıtımında sıkça kullanılan yöntem, metot ve kuantum terminolojilerine yer verilecektir. Temel olarak kuantum ağlarının ve teknolojilerinin neden daha güvenli olduğunu aktaran kuantum fiziği temelli kuramlardan sadece bahsedilecek, ideal bir kauntum anahtar dağıtımı sisteminde yer alan başlıca elemanlar hakkında bilgilendirme yapılacaktır. Son olarak hali hazırda kurulan ve kullanılan kuantum sistemlerinde karşılaşılan sorunlardan bahsedilecektir.

Belirsizlik İlkesi - Heisenberg Principle, Bu ilke adını mucidi Werner Heisenberg'den almaktadır. W. Heisenberg 1927 yılında, kuantum fiziğine göre bir parçacığın momentım ve konumunun aynı anda net bir doğrulukla ölçülemeyeceğini kanıtlamaya çalışmıştır. Kuantum fiziğinde normal "deterministik" fizikte olduğu

gibi her bir niceliğe denk gelen bir reel sayı bulunmamaktadır. Kuantum fiziğinde reel sayıların yerine bu işlemler için bir matrisler ile ifade edilen işlemciler bulunur. Bu yüzden Heisenberg ölçülen bir değerin varlığının önemli olması gibi aynı zamanda bu varlığın ölçüm sırasınında önemli olduğunu aktarmıştır. Bu yüzden eğer denklemde yer alan işlemcilerin iki tanesinin yer değiştirmesi mümkün olmuyor ise bu iki işlemcinin aynı anda ölçülmesinin olanaklar dahilinde değildir (Örn: momentum ile konumun ve benzer bir şekilde elektromanyetik dalgaların sıklığının bir anda ölçülmesinin imkansız olması gibi, belirli bir süre boyunca tekrar hareketinin gözlemlenmesi gerekir.). Benzer bir şekilde bu iki işlemciden birinin durumu ne kadar kesin bir şekilde ölçülüyor ise diğer işlemcinin belirsizlik durumu bir o kadar artmaktadır.

Kuantum anahtar dağıtımı sistemlerinde de bu ilke kullanılmaktadır. Fotonlar üretildiklerinde kararsız bir yapıdalardır, dalgalar gibi davranabilmektedirler ve günümüz biliminin bulunduğu konumda bu fotonların anlık durumunun ölçülmesi imkan dahilinde değildir. Fotonların içinde bulundukları süperpozisyon adı verilen bu durumdan ölçülerek bir anlam çıkarılması gerekmektedir. Fotonlar yönlü optik polarizasyon filtreleri ile ölçülerek yönlü fotonlar elde edilmesi gerekmektedir. Bu işlem yapılana değin fotonlar belirsizlik durumlarını korumaktadırlar. Kısacası optik olarak bir foton üretecinden çıkan fotonun kararsız halinin değiştirilmeden hakkında bilgi sahibi olunması imkansızdır, foton ölçülene değin belirsizliğini, süperpozisyon halini korur. Dolayısıyla fotonlar hakkında bilgi elde edebilmek için onların polarizasyon filtresinden geçirilerek okunması gerekmektedir. Daha öncesinde oluşturulan ve belirli bir polarizasyon filtresinden geçirilen fotonlar tekrar okundukları zaman ilk okundukları polarizasyon filtrelerinden farklı bir filtreden geçirilmeleri durumunda devinim yaptıkları yönü değişecek ve farklı bir değer ile yüklenebileceği gibi ölçülemez bir duruma gelebilir veyahutta sönümlenebilir. Böylesi durumlarda hattın karşı tarafında ölçüm için foton bekleyen tarafın elde ettiği fotonun değeri ölçüm esnasında bilindiği için daha sonrasında beklediği ölçüm değerini elde edemediğinde, foton gelmediğinde veya sönümlendiğinde hat içerisinde bir dinleyicinin varlığını kolayca saptayabilir. Heisenber Belirsizlik kuramı kuantum anahtar dağıtımı işlemlerinde böylesine kritik bir avantaj sağlamıştır.

Klonlanamaz Teoremi - No-Cloning Theorem, Kuantum fiziği ve deterministik fiziğin ayrıldığı noktalardan bir diğeri kuantum durumunun

kopyalanamaz olması özelliğidir. Fizikte klonlama, her parçacığın etkileşiminin konum, momentum ve enerji seviyelerinin kopyalanabilir olduğu ve diğer kopya parçacıkta tüm bu değerlerin tamamen aynı olabileceği durumunu kabul etmektedir. Kuantum fiziğinde parçacıklar süperpozisyonlar halinde bulunduklarından aynı anda birden fazla durumda olabilir. Bu durum olası tüm durumların aynı anda parçacık üzerinde bulunabildiği, olasılıksal olarak tüm bu ihtimallerin üst üste toplandığı haldir ve bu hallerden birinde değişiklik yapılması parçacığın alabileceği diğer tüm ihtimalleri ek olarak etkileyebilir. Yukarıda bahsedildiği gibi bu işlemler fotonlar üzerinde düşünüldüğünde foton kullanılarak anahtar dağıtımı yapılan sistemlerde işlem yapabilmek için fotonların kopyalanamayacağı çıkarımı yapılabilir. Daha önceden polarize edilerek yönlü bir foton haline getirilen bir fotonun tekrar edilebilir olması durumu ile üretildikten sonraki ilk hali karıştırılmamalıdır. Bu teoreme göre net olarak durumu bilinmeyen fotonların kopyalanamaz olduğu bildirilmektedir. Net olarak durumu hakkında bilgi sahibi olduğunuz fotonların tekrar üretilmesi, üretilen bu fotonların micro dalga tüpleri içerisinden geçirilerek birbirilerine bağıntılı hale getirilmesi gibi işlemler sağlanabilir ancak süperpozisyon durumunda olan bir foton kopyalanamazdır. Ayrıca ışık hızında hareket eden bir foton, bilgi aktarım kablolarında olduğu gibi elektromanyetik alan özelliklerinden faydalanarak hattın dinlenebilmesi gibi durumlardan muhaftır. Fotonların iletidiği fiber hatlara fiziksel olarak müdahale edilmesi, “beam splitter” adı verilen optik bileşenleri ile polarizasyon filtrelerine doğru yönlendirilmesi ve tekrar okunması gerekmektedir.

Kuantum Dolanıklığı, Bu durum oluşturulan fotonların doğal olarak birbirilerine bağlantılı hale gelmeleri ile ilgilidir. Bu durumu simüle etmek için kullanılan özel kristallerin kullanılabildiği gibi fotonlar iletim hatlarında ve üretimlerinden sonra doğal yollar ile de dolanıklık durumuna girebilirler. Dolanıklık durumuna girmiş olan fotonlar evrende birbirilerinden ne kadar uzakta olurlarsa olsunlar birbirilerine göre değerler yüklenirler yani biri hakkında bilgi sahibi olmamız diğerinin değerini bilmemiz için yeterli olmaktadır. Kuantum anahtar dağıtımların dolanıklık durumuna gelmiş yani bağıntılı olmuş fotonlardan biri polarize edildiğinde diğer hakkında da otomatik olarak bilgi sahibi olunmaktadır. Kuantum anahtar dağıtımı sistemlerinde özel kristaller (prizma) kullanılarak elde edilebilen dolanık fotonlar, kuantum bilgisayarlarında fotonların mikrodalga darbeleri “microwave pulse” kullanılarak özel bir hat içerisinde birbirilerine

bağlantılı olmaları sağlanabilir. Dolanık çiftlerden bir tanesi ölçüldüğünde diğeri otomatik olarak zıt konumda yer alacaktır.

Fotonların Süperpozisyon Hali, Bu kavramın açıklanması esnasında genel olarak fotonların çift yarık deneyinde gözlemlendiği hali örnek gösterilir. Deneyde bir foton üreteci fotonları bir delikten "pin-hole" karşı tarafta fotonları algılamamızı sağlayacak bir yüzeye doğru gönderir. Beklenen durum bir delikten karşıya geçildiğinde o alanda bir aydınlanma gözlemlenir. Ancak paralelinde açılan bir delik ile foton bombardımanına tutulduğunda gözlemlenen alanda bir ışık deseni meydana gelmektedir. Bu durum incelenerek deneyin bir sonraki aşamasında deliklerden farklı olarak düzeysel yarıklar kullanılmıştır. Çift yarık ile test yapıldığında delikli durumlardaki gibi benzer bir durum ile karşılaşılmış ve bu deney sonucundan fotonların hem atomik hemde dalgacıklı bir hareket izledikleri çıkarımına ulaşılmıştır. Genel olarak su yüzeyine atılan bir taşın dalgacık şeklinde belirli bir frekansla oluşturduğu desen üzerinden genel bir örnek verilir. İki farklı taşın aynı su yüzeyinde oluşturdukları desenin iç içe geçmesi ile oluşan karmaşık düzen bir süperpozisyon örneği olarak verilebilir. Kuantum fiziğinde ise fotonlar, elektronlar ve protonlar bu tarz karmaşık hareket halinde yol almaktadırlar ve matematiksel olarak kararsız bir hareket izlerler.

Erwin Schrödinger bu olayı açıklamak için meşhur Schrödinger kedisi tanımlamasını yapmıştır. Bu tanımda, Schrödinger bir kediyi ölmek ve ölmemek durumu eşit olan zehirli kutulara koymayı düşünmüştür. Schrödinger bir saatin sonunda kutu kutu açılıncaya kadar kedinin kuantum süperpozisyonuna göre aynı anda hem ölü hemde diri olduğunun söylenebileceğini ve bu durumun netleşmesinin kutunun kapağının açılması ile rastgele karar vererek belirlendiğini aktarmıştır. Schrödinger bu örneği verirken ki amacı kuantumun bu kararsız yapıyı açıklarken o zamanın bilgi birikimine göre saçma bulduğunu göstermekti. Yukarıdaki başlıklarda da anlatıldığı gibi kuantum süperpozisyon durumu fotonun anlık olarak hareketi hakkında net bir bilgi sahibi olamadığımız ancak polarizasyon filtreleri kullanılarak bilgi elde edebildiğimiz karmaşık ve kararsız durumudur.

Kuantum Anahtarları Oluşturmak İçin Gerekli Diğer Bileşenler, Bir kuantum anahtar dağıtımı işlemi yapılabilmesi için öncelikle **bir tekil foton üretecine "SPE-Single Photon Emitter"** sahip olunması gerekmektedir. Foton üretecinin temel işlevi tekil fotonlar üretmektir ve "single-photon source" olarak da

adlandırılırlar. Bu üreteçler özel bir tür lazer türü içermektedir. Bu kaynaklar normal lazerler, geniş band aralığında çalışan akkor ampuller ve termal ışık kaynaklarından farklı olarak Heisenberg belirsizlik ilkesine uygun olarak kuantum karakteristiğini saptamak için tercih edilir. Tek bir kaynaktan çıkan tekil fotonlar "photon anti-bunching" olarak adlandırılan fotonların demetlenmesi olayını engeller, tekil olarak ölçülmelerini ve işlenebilmelerini sağlar. Aksi durumda fotonlar demetlenme denilen bir bağlaşıma girer ve kuantumsal olarak ölçülmeleri zorlaşır.

Demetlenme durumunun ölçülebilmesi ve fotonların yönlendirilmesi için "Beam Splitter" denilen optik ayıraçlar kullanılır. Bu ayraçlar gönderici tarafında tekil fotonların histogramının elde edilebilmesi için kullanılır. Histogramın elde edilebilmesi ile kontrol işlemi sağlanabilir. Histogramın oluşturulabilmesi için ayıraç ile yönlendirilen fotonlar hassas foto diyotlar ile ölçülmektedir.

Üretilen fotonların kontrol işlemleri yapıldıktan sonra optik bir lens takımından geçerek fiber hatlardan oluşan kanala doğru odaklanırlar. Bu kanala kuantum kanalı denilebilir. Kanala girilmeden önce ortam şartlarından oluşabilecek aykırı fotonların oluşunun engellenmesi ve sistemin normalizasyonu için optik band geçiş filtreleri kullanılabilir ve farklı fotonların söndürülmesi sağlanabilir. Kuantum üreteçleri kullanılarak üretilen fotonlar daha sonrasında bir kuantum kanalı üzerinden taraflar arasında iletilir. **Kuantum kanalına** iletilmiş olan fotonlar bu kanalın çıkışında kübit olarak adlandırılır. Kubit olabilmeleri için pozisyonlarının ölçülmüş olması gerekmektedir. Bahsedilen bu ölçüm işlemi için polarizasyon - yönlü optik filtreleri kullanılmaktadır. Yönlü polarizasyon filtreleri doğrusal (Örn:0º ve 90º) ve eksenel (Örn: 45º ve 135º) açılarda olabilirler.

Kübit'lerin üretici tarafından üretilerek alıcı tarafından okunması ile aradaki kullanılan polarizasyon filtrelerinin rastgele seçilmesi ve tarafların birbirilerinin seçtikleri filtreleri bilmemelerinden dolayı çokça yanlış ölçüm yapılabilmektedir. Bu bahsedilen işlemler seçilen sistemin genel mantığından kaynaklanan sorunlar iken aynı zamanda sistemsel ve kontrol dışı işlemlerden kaynaklanan kayıplarda yer almaktadır. Bu sorunlara bir sonraki bölümde değinilecektir. Üreticinin gönderdiği kübit'ler ve alıcının okuyabildiği kübit'ler arasındaki fark ve toplam kübit sayısına göre **QBER - Quantum Bit Error Rate, Kübit Hata Oranı** ölçülerek kurulan anahtar dağıtımı sisteminin başarısı ölçülebilmektedir.

2. Güncel Sınırlamalar ve Problemler

Foton üreteçlerinde yer alan lazer kaynaklarının piyasada erişilen normal lazer kaynaklarından farklı olmasından ötürü uygun yoğulukta lazer üretebilecek kaynakların kullanılması mevcut sistemlerde başlıca yer alan sorunlardan biridir. Kullanılan lazer kaynaklarının her bir "lazer pulse veya photon beam" işleminde foton ürettikleri düşünülmemelidir. Çoğu sistemlerde üretilen pulse'ların birden fazla kez üretim işlemi yaparak şartları sağlayan fotonun kullanılması gerekmektedir. Bu yüzden temelinde lazer olan foton üreteçlerinde lazer yoğunluğu önemli bir kısıtlayıcı parametredir. İyi bir lazer kaynağı seçilememesi durumunda çoklu foton ışıması yapan devreler kurulması gerekecek dolayısıyla masraf artışı ve ataklara geliştirilmekte olan kuantum ataklarına karşı duyarlı hale gelecektir. Foton üretimi işlemlerinde bu bahsedilen sorundan dolayı bir optimizasyon işlemi yapılması gerekmekte ve bu optimizasyon işlemi sistemde yavaşlamalara ve beklemelere sebep olmaktadır. Test için kullanılan, ticari olmayan sistemlerin çoğunda optimize edilmemiş sistemler kullanılmaktadır.

Sinyal olarak iletilen fotonlarında belirli bir mesafede aktarımı sağlanabilmektedir. Normal iletişim kanallarında sinyallerin sönümlenmesinin engellenmesi için amplifier adı verilen sinyal güçlendirici devreler kullanılmaktadır. Kuantum ağlarında ise enteglement- dolanıklık özelliğinden faydalanılarak belirli aralıklar ile fotonlar kuantum modülleri aracılığı ile dolanıklaştırıldıkları diğer fotonlar ile eşlenerek hedefe doğru yönlendirilmektedir. Günümüzde bu veri aktarım mesafesinin attırılması üzerine çalışmalara devam edilmekte ve son olarak 2018 yılında Physical Review Letters dergisinde yayımlanan makaleye göre yeni bir rekor kırılarak 2.5GHz ve yüksek performanslı anahtar paylaşımı 421 km'lik fiber hat üzerinde kuantum anahtar dağıtımı yapılabildiği bildirilmiştir.

Açık anahtar dağıtımı olarak adlandırılan bir başka kuantum anahtar dağıtımı imkânı bulunmaktadır. Uydulara kurulan düzenekler ile yer yüzünde yer alan teleskoplara kuantum anahtar iletimi sağlanabilmektedir. Bu tar kullanım senaryolarında anahtar dağıtım mesafesi herhangi bir opik kablo ve fiber hat kullanılmadan yapıldığından uzun mesafeler boyunca aktarım işlemi yapılabilmektedir. Ancak bu kullanım senaryosunda atmosfer koşulları belirleyici olmakta ve fiber hatlar ile kurulan sistemlerden çok daha uzun mesafelerde aktarım işlemleri yaptıklarından kuantum bit hata oranı yüksek çıkmaktadır. Çin'de yapılan

çalışmalarda 2017 yılında Micius deney setinde 1000 km mesafeden BB84 algoritması test edilmiş olup 3.5 bps'lik bir başarılı anahtar oluşturma performansı sağlanabilmiştir. Micius ile yapılan bir diğer deneyde 1200 km'lik bir mesafeden E91 algoritması test edilmiş ve %4,5 kuantum bit hata oranı elde edilerek kullanılabilir bir seviyede işlem sağlanmıştır. Ancak buna karşılık anahtar oluşturma oranı 0.12 bps olarak düşük bir performans göstermiştir. Mesafelerdeki artışların ve atmosfer katmanlarının dünya ve uydu arasında gerçekleştirilen uzun mesafeli "free-space" kablosuz kuantum anahtar dağıtımı senaryolarında belirleyici olduğu anlaşılmaktadır.

Kuantum anahtar dağıtım temelinde düşünüldüğünde hali hazırda geliştirilmiş olan kuantum anahtar dağıtımı sistemleri günlük kullanımımızda olan iletişim kanallarına entegre olabilmekte, anahtar dağıtımında yer alan tarafların karşılıklı olarak anlaştıkları anahtar bilgilerini birbirilerine klasik iletişim kanalları üzerinden paylaşabildikleri çalışmalar yapılmaktadır. Ancak bu işlemin kuantum kanalları üzerinde yapılması istenildiğinde veri aktarımlarının belirli mesafelerin ötesinde gerçekleştirilebilmesi gerekmektedir. Günümüzde karşılaşılmakta olan güncel sorunlardan bir tanesi olarak bu sorun dikkat çekmektedir. Mevcut fiber optik kablo hatlarının genişletilmesi ve kalite bakımında özelliklerinin aktarılması gerekmektedir.

Kuantum anahtar dağıtımında yer alan foton üreteçleri gönderici tarafında kullanılmakta iken alıcı tarafında eğer anahtar uzlaşısı klasik iletişim hattı üzerinden yapılıyor ise en azından bir foton dedektörünün bulunması gerekmektedir. Kullanılan foto dedektörlerin hassasiyeti ve fotonların geliş açılarına göre hizlanması oldukça önem arzetmektedir. Dedektörün hassasiyeti içerisinde genellikle kullanılmakta olan ölçüm diyotlarının hassasiyeti ile paralel olarak değişmektedir. Hizalama sorunlarının giderilmesi için sabitleyici sistemlerin ve foton aktarımında kullanılan fiber kabloların kılavuzlama işlemlerinin belirli standartlara göre yapılması gerekmektedir.

Foton üreteçlerinde daha önceki bölümlerde bahsedildiği gibi hata düzeltme işlemlerinin yapıldığı modüller ve ölçüm sistemleri yer almalıdır. Lazer üreteçlerinin ürettikleri düşük enerji seviyelerindeki fotonların düzenlenmesi ve hata düzeltme işlemlerine ek olarak lazer uyarıcı modüller eklenmesi ile lazer üretecin zamanlama kontrollerinin yapılmasını içeren çalışmalar mevcuttur.

Sınırlandırıcı parametreler olarak iletişim ağını gürültüsü, hat içerisinde kuantum dolanıklığı olması ve sonrasında foton değerlerinin değişmesi, çeşitli sebeplerden dolayı foton sönümlenmesi sorunlarının hesaba katılması gereklidir. Kuantum anahtar dağıtımı sistemleri başta olmak üzere genel olarak tüm kuantum sistemleri günümüzde kullanılan sistemlerde simüle edilmesi yüksek miktarda bilgisayar gücü gerekmektedir. Dolayısı ile güncel bilim kuantum bilgisayarlarının gelişerek daha çok kullanıma açılması ile daha hızlı yol alacaktır. Kuantum anahtar dağıtımı yöntemlerinde taraflar arası anahtar eşleştirmesi ve karşılıklı olarak uzlaşı protokollerinin gerçekleştirilmesinde çokça sayıda artık kübitler meydana gelmektedir. Doktora çalışmamızın ana konusu bu artık bit'lerin azaltılması üzerinedir.

D. Kuantum Anahtar Dağıtımı Protokolleri

1. BB84 Protokolü

Kuantum anahtar dağıtımı sistemlerinin bilinen ilk başarılı protokol önerisi BB84 algoritmasıdır. Bu algoritma 1984 yılında Charles Bennett ve Gilles Brassard tarafından önerilmiştir. Algoritmanın temel mantığı iletişim kanalında bulunan gönderici, bir diğer adı ile "Alice" ve alıcı "Bob" arasında tasarlanan şifreleme anahtarının kuantum anahtar dağıtımı ağı ile aktarılmasına dayanır. Anahtar dağıtım ağının en önemli bilgisi olan polarizasyon filtre bilgilerinin açığa çıkmaması bu sistemde oldukça önemlidir. Anahtar dağıtım sistemi bu bilginin açığa çıkmaması üzerine kuruludur.

Yukarıdaki bölümlerde aktarıldığı üzere fotonlar üreteçlerden üretildiklerinden sonra süperpozisyon adı verilen kararsız bir yapıda bulunmaktadırlar. Üretilen fotonlardan bilgi çıkarımı yapabilmek için fotonların yön ve doğrultusu bilinen polarizasyon filtreleri ile polarize edilmesi ve yönlü konuma getirilmeleri gerekmektedir. Algoritma daha öncesinde genel olarak yönlü filtre sonrasında elde edilen fotonun sayısal değer olarak karşılığını bildiren bir tablo vermektedir ancak taraflar kendi aralarında bu bilgiyi değiştirerek farklı bir yorumlama tablosu üretebilirler.

Fotonlar, polarizasyon adı verilen optik bir işlemle filtrelenmedikçe anahtar oluşturma algoritmalarında kullanılamaz. Fotonlar filtrelendikten ve optik filtre ile polarize olduktan sonra, yönlü ve amacımız için anlamlı hale gelir.

Polarizasyon süreci dört farklı yönde gerçekleşebilir. Bu dört farklı polarizasyon yönü iki ana grupta toplanmakta ve "+" işareti ile simgelenen "Doğrusal taban" ve "X" ile simgelenen "Ortogonal taban" olarak adlandırılmaktadır. Doğrusal temel, sıfır derece yatay polarizasyon filtresi ve doksan derece dikey polarizasyon filtresidir. Ortogonal taban 45 derece ve 135 derecedir. Şekil 1'de polarizasyon filtreleri ve ürettikleri değerlerle ilgili görsel paylaşılmıştır.

Doğrusal Polarizasyon	**+**	↕ 90º	↔ 0º
		0	**1**
Diyagonal Polarizasyon	**×**	↗ 45º	↖ 135º
		0 veya **+**	**1** veya **−**

Şekil 1 Polarizasyon filtreleri ve ürettikleri değerler

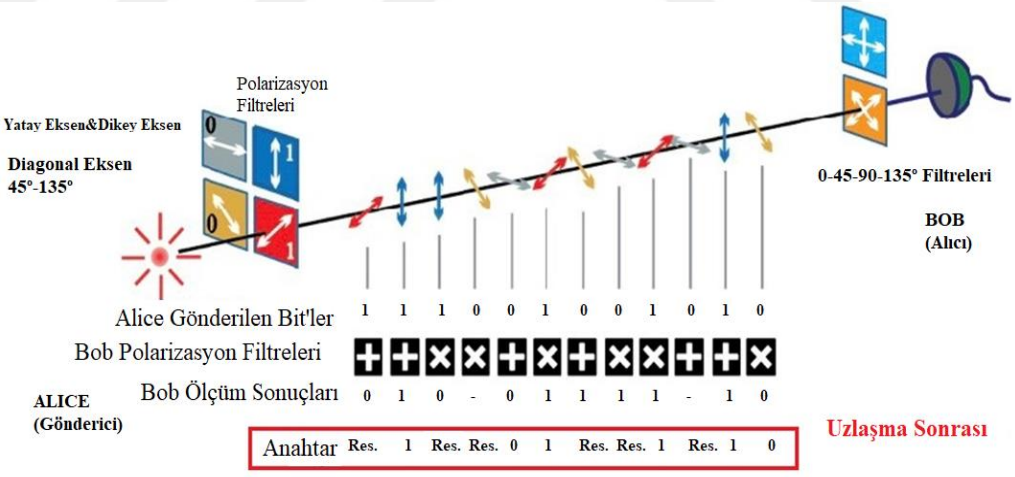
İlk adım, bundan sonra Alice olarak anılacak olan foton vericinin veri değerlerini bir ikili sayı formatında kullanacağıdır. İkinci adımda Alice, polarizasyon filtrelerini rastgele seçecektir. Üçüncü adımda Alice, polarize fotonları kuantum kanalında bundan sonra Bob olarak anılacak olan alıcıya iletir.

Dördüncü adımda Bob, rastgele bir polarizasyon temeli seçer ve gelen fotonları polarizasyon filtreleri kullanarak ölçer. Bob, ölçtükten sonra foton durumları adı verilen foton polarizasyonunun sonuçlarını kaydeder. Bu sonuçları halka açık kanalda Alice ile paylaşır. Beşinci adımda Alice, Bob'un polarizasyon sonuçlarını alır ve eşleşmeleri bulmak için polarizasyon durumlarını kontrol eder. Son adımda Alice, Bob'a kararlaştırılan her polarizasyon filtresi konumu veya indeksi ile cevap verir. Bundan sonra güvenli veya mutabakatlı bir anahtar oluşturulur.

Öte yandan, kuantum kanalında klasik kamu kanalında olduğu gibi bir kulak misafiri olabilir. Kulak misafiri olan Eve, optik bir ışın ayırıcıyla kuantum kanalına girebilir. Fotonlar fiziksel yapıları nedeniyle kopyalanamadığı için, Eve'in kuantum kanalını kesmesi ve rastgele seçtiği polarizasyon filtreleri ile tüm fotonları polarize etmesi gerekmektedir. Fotonlarla ilgili bilgileri filtrelerle ölçmekten başka bilinen bir

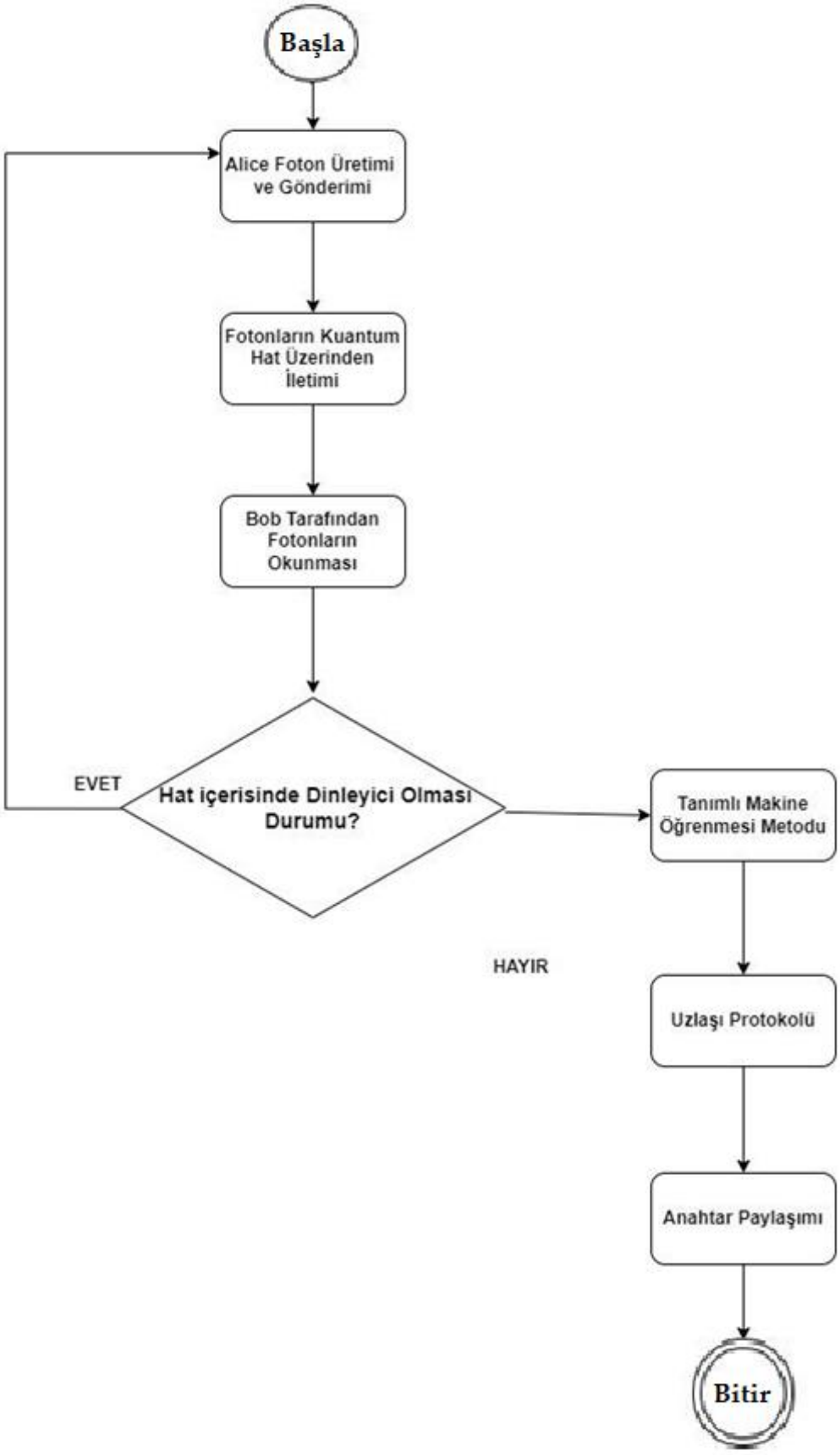
yol yoktur. Fotonlar, ilk ölçüldükleri polarizasyon yönünden farklı bir yönde ölçüldüklerinde, polarizasyon temellerini değiştirirler veya sönümlenirler. Böyle bir durumda her bir foton için araya giren yetkisiz kişinin ölçüm yapması durumunda, BB84 algoritması için 4 adet filtre kombinasyonu bulunduğundan, %75 olasılık ile yanlış tercih yapılabileceğini gösterir. Fotonlar sıralı olarak gönderildiklerinden ve çoklu Kübit'ler olarak gönderildiklerinden her fotonda farkına varılma olasılığı bir önceki olasılık ile çarpılarak toplam farkına varılma durumu hesap edilebilir. Toplamda 64 adet foton iletimi yapıldığı takdirde dinleyici olan kesimin hat içerisinde farkına varılamamasının çok düşük bir ihtimal olabileceği görülebilir. Hat içerisine dahil olan dinleyici Eve, yanlış bir polarizasyon filtresi tercih etmesi durumunda fotonlarda değişikliğe sebebiyet verecektir. Bu değişiklik, Alice ve Bob'un önceki süreçte uzlaştığı beklenen verilerde herhangi bir değişikliğe neden olursa, Alice ve Bob, hattaki bir dinleyici olduklarını anlayacak ve iletişimi sonlandırarak başka bir kanala geçeceklerdir.

Tüm bu adımlar temel olarak BB84 kuantum anahtar dağıtım protokolünü oluşturmaktadır. Şekil 2'de bunun bir örneğini görebilirsiniz. "Res." son satırdaki değerler artık bitleri temsil etmektedir.



Şekil 2 BB84 örneği

Doktora tez çalışmasında BB84 algoritması üzerinden Şekil 3'de paylaşılan bilgiler doğrultusunda bir sistem kurulacaktır. Kuantum anahtar üretimi ve makina öğrenmesi metotlarının kullanımı BB84 algoritması üzerinden test edilecektir.



Şekil 3 BB84 tabanlı genel sistem mimarisi

2. E91 Protokolü

Artur Ekert 1991 yılında foton dolanıklığı özelliğinden faydalanarak E91 adında bir protokol oluşturmuştur. Bu protokol genel olarak birbiri ile ilişkilendirilmiş, dolanıklaştırılmış foton çiftlerini kullanır. Kullanılan fotonlar bilinen bir kaynaktan foton üreteci vasıtası ile üretilen ve dolanıklaştırılarak taraflara iletilen fotonlar olabileceği gibi aynı zamanda hattı dinlemeye çalışan Eve olarak adlandırılan bir dinleyici de olabilir. Dolanıklaştırılarak gönderilen fotonların birer tanesi Alice ve Bob'a iletilir. E91 protokolünde Alice 0º, 45º, 90º yönlerinde kuantum polarizasyon filtresi kullanılırken karşılığında Bob 45º, 90º, 135º yönlerinde polarizasyon filtreleri kullanır. Bu kullanım senaryosunda taraflar ⅓ oranında aynı anahtar düzlemini kullanma olasılığına sahiptirler. Üretilen fotonlar BB84 algoritmasında olduğu gibi taraflar arasında okunmaksızın birbirinden bağımsız bir şekilde tek bir kaynaktan üretilerek taraflara iki bağıntılı/eş foton olarak gönderilirler. Kuantum dolanıklığına sahip fotonlar kullanıldığından dolayı aynı polarizasyon filtresine sahip ölçümlerde tarflar birbirilerinin ölçüm sonuçlarının zıt değerlerine sahip olacaklarını bilmektedir. BB84 algoritmasında aynı polarizasyon filtrelerinde beklenen değerlerden farklı sonuçların tespit edilmesi durumunda hat içerisinde bir dinleyici olduğunun farkına varılmaktadır. E91 algoritmasında bu işleme ek olarak matematiksel bir formül ile hesaplama yapılmakta ve istenilen sayısal değerin elde edilememesi durumunda anahtar dağıtımı yeterli kuantum dolanıklığı sağlanamadığı tespit edilerek anahtar dağıtımı tekrarlanmaktadır. Bu işlem için ölçümü yapılan fotonların ⅔ 'ü kullanılmaktadır. Bu oranda test yapılmasının sebebi zaten halihazırda ⅓'lük oranda anahtar değerlerinin aynı olarak beklenmesidir. Aşağıda paylaşılan ilgili test denklemi Denklem 1 paylaşılmıştır.

$$S = \{P\ +\ +\ (AliceBase(i), BobBase(j))\} + \{P\ -\ -\ (AliceBase(i), BobBase(j))\} - \{P\ +\ -\ (AliceBase(i), BobBase(j))\} - \{P\ -\ +\ (AliceBase(i), BobBase(j))\}$$

(Denklem 1)

S değerinin mutlak değerinin 2'ye küçük eşit olması durumunda yeterli kuantum foton dolanıklığı sağlanamadığı anlaşılır ve prosedür tekrar edilir. Bunun sebebi olarak ortam koşulları düşünülebileceği gibi aynı zamanda hat içerisinde dinleyici olabileceği düşünülebilir. Eğer S değerinin mutlak değerinin $2\sqrt{2}$ değerine

benzer olması durumunda ise hatta istenilen dolanıklık seviyesinin sağlandığı anlaşılır. Bu elde edilen değerden sonra klasik kanal üzerinden Alice ve Bob veri aktarımı yaparak uzlaşma protokolünü gerçekleştirir. Şartları sağlamaları durumunda taraflar klasik kanal üzerinden birbirilerine polarizasyon filtrelerini bildirerek kullanılacak anahtarları netleştirmiş olurlar. Taraflar tam manası ile bir senkronizasyon yakaladıklarından bu ahenki bozan hiçbir ölçüm sonucunu kabul etmeyecek ve protokolü tekrardan başlatacaklardır.

Tarafların birbirilerinin kullandıkları polarizasyon filtrelerinin yönlerini veya açılarını bilmesi imkansızdır, taraflar bu filtreleri rastgele seçmektedir. Ancak tarafların rastgele filtre seçiminde açısal ön kabüller olduğundan benzer filtre doğrultularını denk getirmeleri durumunda %100 doğru sonuçları elde edebileceği kesinliği bir avantaj olarak ön plana çıkmaktadır.

Taraflar klasik haberleşme hattı üzerinden ölçüm sonuçlarını birbirileri ile paylaşarak uzlaşı protokolünü gerçekleştirebilirler. Daha sonrasında elde ettikleri anahtar değerlerini netleştirmiş olurlar. Bu anahtar dağıtımı protokolünün BB84 algoritmasından daha iyi olması sebeplerinden biri tek bir kaynaktan süperpozisyon halinde olan fotonların gönderilmesi ve alıcı-verici tarafları foton ölçümleri yapmamış olmasından dolayı, Eve adı verilen hattı dinleyen kişinin fotonları ölçse bile tarafların anahtarları hakkında bilgi sahibi olmamasıdır. Çünkü tarafların seçtiği polarizasyon filtrelerinin ve Eve'in ölçümlerinin etkilerini klasik hat üzerindeki izlerini takip edebilmesi imkansızdır. BB84 algoritmasında olduğu gibi taraflar fiber kablolar üzerinden foton gönderimi yaparak birbirileri ile haberleşme işlemi gerçekleştirmemektedirler. Fiber hatlar sadece taraflar ve kaynaklar arasında kullanılmaktadır. Eve her iki fiber hattına ulaşıp ölçüm yapsa bile taraflar seçtikleri polarizasyon filtrelerini fotonlar üzerinde ölçüm amaçlı kullanmadıklarından dolayı Eve'in yapacağı ölçüm işleminden değerli bir bilgi elde edilememektedir.

Tarafların E91 kuantum anahtar dağıtımı algoritması için seçtikleri örnek polarizasyon filtre seçimi ve ölçüm sonuçları Çizelge 1'deki gibidir.

Çizelge 1 E91 örnek polarizasyon filtresi ve sonucu

Alice Polarization States	↑	→	→	↗	↗	↗	→	→
Alice Measurement	1	0	0	1	1	1	0	0
Bob's polarization States	↑	↘	↑	↑	↑	↗	↗	↗
Bob Measurement	1	X	X	0	0	1	X	X
Shared Key	1001							

3. B92 Protokolü

Bu protokol temel olarak BB84 algoritmasının sadeleştirilmiş halidir. Alice ve Bob olarak gönderici ve alıcı tarafları iletişim kanalının her iki ucunda konumlanmışlardır. BB84 algoritmasında olduğu gibi Alice foton üretecinden bir seri foton üretecek ve bu fotonları rastgele seçtiği polarizasyon filtrelerinden geçirerek Bob'a iletecektir. Bu algoritmanın BB84 algoritmasından ayrıştığı nokta seçilen polarizasyon filtrelerinin çeşitliliğinden gelmektedir. BB84 algoritmasında 4 farklı polarizasyon filtresi Alice ve Bob tarafından serbstçe rastgele seçilebilir iken B92 algoritmasında tarafların seçebilecekleri polarizasyon filtreleri önceden belirlenmiştir ve bu sınırlı filtreler arasından seçim yapılabilecektir. Tarafların fotonların polarizasyonundan sonra anlamlandırılacağı karşılık değerleri önceden bilinmektedir. Buna göre Alice 0º (yatay) ve 45º açılı yönlü polarizasyon filtreleri kullanır. Bu filtrelerden geçirilen fotonların alacakları değerler sırası ile 0 "sıfır" ve 1 "bir" 'dir. Buna karşılık Bob 90º (dikey) ve -45º veya 135º açılarda polarizasyon filtreleri kullanmak zorundadır. Buna karşılık Bob'un ölçüm yapacağı filtrelerde elde edeceği değerler sırası ile 1 "bir" ve 0 "sıfır" 'dır. Bob, Alice'den gelecek fotonların polarizasyonları ve karşılığında alacağı değerleri bildiğinden 90º'lik polarizasyon filtresi sonucuna 0 değerini atamaz. Polarizasyon ölçümü sonucunda elde edilebilecek bir değer olabilmesi için 45º polarizasyon sonucuna denk gelebilecek 90º'lik ölçüme 1 değeri atar ve diğer polarizasyonun sonucunu 0 "sıfır" olarak netleştirir.

Tarafların B92 kuantum anahtar dağıtımı algoritması için seçtikleri örnek polarizasyon filtre seçimi ve ölçüm sonuçları aşağıdaki gibidir.

Çizelge 2 B92 örnek polarizasyon filtresi ve sonucu

Alice Bit	0	0	1	1	1	0	0	0
Alice Polarization States	0º	0º	+45º	+45º	+45º	0º	0º	0º
Bob's polarization States	90º	-45º	-45º	90º	-45º	-45º	-45º	-45º
Bob Measurement	X	X	X	1	X	0	0	X
Shared Key				100				

4. Diğer Protokoller

Yukarıda anlatılan sistemler genel olarak diğer kuantum anahtar dağıtım sistemlerinin temellerini oluşturan en temel yöntemlerdendir. Bu bölümde bahsedilecek olan diğer sistemler genel olarak yukarıda bahsedilen sistemler temel alınarak geliştirilen sistemlerdir.

Decoy State yöntemi temel olarak BB84 algoritmasını temel almaktadır. Kuantum anahtar dağıtımı sistemlerinde bir adet foton üreteci kullanılarak gönderilen tekil foton sistemleri, kullanılan fiziki kaynakların tek seferde yüksek başarılı bir üretim sağlayamadığı ve birden fazla kez kuantum üretmesi gerektiği temel sorunlardan biridir. Güncel sistemlerde sistemin hızlandırılması için birden fazla kaynaktan foton üretimi sağlayarak anahtar dağıtımı sistemleri hızlandırılmaktadır. Bu tarz sistemler genel olarak **PNS- Photon Number Splitting, Foton Sayı Bölünmesi** olarak adlandırılan sistemlere karşı dayanıksızdır. Bu işlemin çokça sistemde olması ve sisteme dahil olan çokça kimsenin hattı dinlemesi ile birlikte kuantum ağlarının servis dışı bırakılmasına dahi sebep olabilecektir. Kullanılan lazer kaynaklarının çoğunlukla 0.2 yoğunlukta foton üretmektedir ve bu fotonlar anahtar dağıtımında kullanılamaz durumdadırlar. Hat boyunca sönümlenebilir ve ölçüm yapacak kişi tarafında mekanik ve optik sistem kaynaklarının hizalanma ve hasssasiyet olmasından dolayı alınamayacaktır. Benzer şekilde bu lazer kaynakları tek seferde 2 foton üretimi yapabilir. Bu durum PNS atağının temelini oluşturmaktadır. Böyle durumlarda Alice fotonlardan birini polarize ederken diğer fotonu karşı tarafa iletebilir. Eve olarak adnlandırılan hattı bölen kişinin elde edilen bu fazla fotonlar üzerinden istatistiksel olarak anahtar hakkında bilgi sahibi olması mümkündür. Ancak tüm bu sorunlara ve ataklara rağmen BB84 algoritmasında

başarılı bir şekilde anahtar paylaşımı yapılabilmesi mümkündür. Buna karşılık sistemsel olarak üretilen yöntemlerden biri Decoy State yöntemidir. Bu yöntemin temel amacı anahtar dağıtımı için kullanılacak fotonlardan farklı olarak belirli bir sayıda foton bu bit'lerden önce veya sonra üretilip gönderilecek bu bit'lerde yaşanan değişimler takip edilerek Eve'in varlığının farkına varılabilmektedir.

PNS ataklarına karşı BB84 tabanlı geliştirilen bir diğer yöntem ise SARG04 adlı kuantum anahtar dağıtımı protokolüdür. Bu algoritmada öncelikle N bit uzunluğunda bir foton serisi Alice tarafından Bob'a iletilir. Alice kendi tarafında üretilen her bir foton için rastgele 2 farklı polarizasyon filtre grubu seçer. Bu filtreler farklı doğrultulara aittir. Alice kullandığı filtre gurubunu açık kanaldan iletir. Bob bu filtre grubundan birini seçerek gelen fotonu polarize ederek kuantum foton algılayıcısından ölçmeye çalışır. Eğer ölçüm sonucunda bir değer çıkmazsa, yani foton sönümlenirse ölçüm sonucunu bildirir. Bob her sinyal için iki farklı ihtmal ile karşılaşır. Eğer ölçüm sonucu filtre grubundaki durumlardan birine dik ise ölçüm sonucunun aslında diğer gruba ait olduğunu netleştirerek Alice'in seçtiği polarizasyon filtresini netleştirmiş olur. Tersi durumlarda ölçüm filtresi bildirilen filtre grubundan herhangi birine ortogonal değil ise bu işlemin bir sonucu alınmamış olur ve sonuç alamadığını bildiren bir mesaj yayınlar. Bu işlem tekrarlanarak kesin bit'ler seçilmiş olur.

Gönderici olan Alice rastgele test bitleri seçerek bunları konumlarını Bob'a duyurur. Bu işlemlerin iki taraflı ölçüm sonuçları karşılıklı ölçülerek anahar dağıtımı hata oranı test edilri. Eğer beklenenden yüksek bir hata oranı ile karşılaşılır ise hat içerisinde bir dinleyicinin "Eve" olduğu anlaşılarak hat kesilir ve tekrar en baştan işlem senaryosu tekrarlanır.

BB84 algortimasından üretilen bir diğer protokol ise **Six-State Protocol** Algoritmasıdır. Bu algoritmada temel amaç foton polarizasyonunda kullanılan filtre türlerinin arttırılması ve karşmaşıklığın arttırılarak daha fazla yönlü foton gönderimi sağlanarak hata yapma ihtimalinin arttırılmasıdır. Dolayısıyla 0º, 45º, 90º ve 135º dereceli 2 boyutlu koordinat sisteminde yer alan polarizasyon filtrelerine ek olarka 3. bir ek boyut getirilmiş ve o boyut düzleminde iki farklı yön doğrultusu ile 5. ve 6. yönlü polarizasyon filtreleri üretmişlerdir. Böylelikle yönlü fotonların sayısı BB84 yönteminde olduğu gibi 4'ten 6'ya çıkarılmış ve araya girerek hattı dinlemek isteyen Eve'in hata yapma olasılığı arttırılmıştır. Eve böyle bir algoritma kullanılması

durumunda hattı dinlemek için beam splitter kullanarak fotonları 6 farklı polarizasyon filtresinden birini rastgele seçerek okumaya çalışacak ve BB84 yönteminde tek bir foton için başarılı tahmin oranını %25'ten %16'ya indiğinden hata yapma oranı otomatik olarak artacaktır. Sıralı birçok foton iletimi gerçekleştirildiğinde BB84 algoritmasında anlatılığı gibi birbirine bağlı durum ihtimalleri içerdiğinden daha kısa olan foton serisi gönderiminde daha erken varlığı tespit edilecektir.

E. Kuantum Anahtar Dağıtımı Protokolleri Avantajları ve Dezavantajları

Bu yöntemlerin temel sorunu kullanılan optik düzeneklerin, foton üreteçlerinin ve ağ altyapısının temel olarak günümüz ihtiyaçlarını karşılayacak kadar ucuz ve yaygın olmamasıdır. Performans amaçlı çoklu foton üreteçleri kullanılmakta ve genel olarak üreteçlerden tek seferde tek bir foton üretimi elde edilememektedir. Aksine sönümlenen fotonlar ve çift fotonlar tek seferde üretilebilmektedir. Sönümlenen fotonlar sistemin başarısını düşürmekte iken çift olarak üretilen fotonlar sistemi dinleyebilen şahıslar tarafından bir güvenlik zaafiyetine sebep verebilmektedir. PSA atakları bu zaafiyetten faydalanmaktadır. Bu durumda dahi kuantum anahtar sistemlerinin çalışıyor olması ve hattı dinleyenlerin tespit edilebiliyor olması büyük avantajlardan bir tanesidir. Fotonların fiber ağlar içerisinde çok uzun mesafelerde iletilemiyor olması, fotonların şu an kullanılan sistemlerimizde olduğu gibi güçlendirici devrelere ihtiyacı olduğunu ve halihazırda kullanılan sistemlerin iyileştirilerek daha performanslı sistemlerin geliştirilmesi gerektiğini göstermektedir. Geliştirilecek sistemlerin şu an kullanmakta olduğumuz sistemler gibi daha ucuz ve yaygın olması gerekliliği temel aşılması gereken sorunlardan bazılarıdır.

Temel sorunların bir diğeri, free-space kuantum anahtar dağıtımı sistemlerinin uydu-kara haberleşmesinde kullanılan ekipmanların masraflı olmaları ve kontrollü atmosfer koşullarında belirli bir seviyede düzgün çalışabiliyor olmalarıdır. Ancak atmosfer koşullarındaki anlık değişimler göz önüne alındığında bu alanda iyileştirici çalışmalara devam edimesi gerektiği anlaşılabilir.

Kullanılan her kuantum anahtar dağıtımı ve haberleşme sistemi altyapılarının iyileştirilmesi anlaşıldığı gibi aynı zamanda geliştirilen algoritmaların benzer şekilde iyileştirilmesi gerekmektedir. Bu algoritmalarda temel çözülmesi gereken sorun anahtar dağıtımı algoritmalarının sonucunda meydana gelen çokça miktarda artık

kuantum bit'lerinin azaltılması gelebilir. Kuantum anahtar dağıtımı sistemlerinde halen daha klasik haberleşme kanallarının veri aktarımı ve uzlaşı protokollerinde kullanılıyor olması ilerleyen dönemlerde kripto-analiz işlemleri gerçekleştiren kişilerce kullanılabilir zaaflar olarak meydana çıkabilir.

Tüm bu bahsedilen ve olası sorunlara karşılık kuantum anahtar dağıtımı sistemlerinin şuan günümüzde kullanılan şifreleme sistemlerine belli başlı avantajları mevcuttur. Kuantum sistemleri, şuan kullanılmakta olan kriptoloji sistemlerinde yer alan "pseudo-random number generator" yani yapay rastgele anahtar üreteçelerini kullanmamakta yerine temellerini fizik biliminden alan gerçek rastgele sayı ve değerler üretmektedir. Ek olarak kullanılan kuantum foton altyapısı şu an kullanılmakta olan elektronik haberleşme yapısında yer alan kopyalama ve hat dinleme işlemlerine göre çok daha güvenli ve belirli zorluklar içermektedir. Kullanılan fotonlar kuantum fiziğinde yer alan kanunlarca klonlanamaz ve bütünlüğüne fiziksel olarak müdahale edilmeksizin haklarında bilgi sahibi olunamazlar. Kuantum fiziğinin bir diğer özelliklerinden olan dolanıklı kavramı ile haberleşme protokolleri gerçekleştirilmiş olup üretilen fotonların mesafe fark etmeksizin çiftleri hakkında bilgi sahibi olunabilmekteyiz. Özet olarak kuantum anahtar dağıtımı sistemleri, muadili olan yöntemlere göre temellerini kuantum fiziği ve fizik kurallarından almaktadır ve şu an kullanmış olduğumuz anahtar dağıtımı sistemlerinin temeli, ihtimal havuzlarının çözülemez olduğunu iddia eden matematiksel varsayımlar ile temellendirilmektedir.

F. Kuantum Anahtar Dağıtımı Protokolleri Çıkarımları

Kuantum fiziği temelinde gelişen kuantum teknolojileri en temelinde geliştirdiğimiz teknolojik cihazların en temel unsuru olan transistörlerin giderek ufalması ile nesnelerin en küçük haline odaklanmamızı sağlamıştır. Kuantum tabanlı teknolojiler bugünlerde güvenlik tabanında tüm teknoloji dünyasına bakış açımızı değiştirmektedir. Fotonların kuantum tabanlı özelliklerinin ve teknolojiye uyarlayabileceğimiz kuantum fiziği kanunlarının; süperpozisyon, belirsizlik ilkesi ve kuantum dolanıklığı gibi, hayatımızda köklü değişimlere önderlik edebileceği açıkça görülmektedir. Bu değişime bilgi güvenliği ve veri bilimi alanlarında başlamış ulunmaktayız.

Bir önceki bölümde bahsedilenlerden anlaşılabileceği gibi kuantum tabanlı anahtar dağıtımı ve üretimi teknolojilerinin geliştirilmesi gereken birçok donanımsal ve altyapısal eksikleri bulunmaktadır. Ancak içinde bulunduğu durumuna rağmen sağladığı güvenlik ve güvenilirlik parametreleri ile çoğu güncel kriptoloji sistemi ile yarışabilir ve yakın zamanda yerine kullanılabilir duruma gelebilecektir. Diğer bir taraftan kuantum anahtar dağıtımı algortimalarının yazılımlarında yapılabilecek yenilikler temelde donanımsal gelişmeler ile bağlantılıdır. Kullanılacak foton üreteçlerinin iyileştirilmesi ile daha az hatalı foton üretimi sağlanabilir, sönümlenen ve çift olarak gönderilen fotonların sayısı azaltılabilir, böylelikle olası güvenlik sorunları azaltılabilir. Ek olarak geliştirilebilecek foton güçlendirici devreler ve fiber optik ağ sisteminin geliştirilmesi ile daha uzun mesafelerde mcelikle anahtar paylaşımı sağlanabilir. Tüm bu donanımsal yeniliklerden bağımsız olarak yazılımsal olarak geliştirilebilecek sistemler ile birlikte anahtar dağıtımı ve uzlaşma protokolleri esnasında açığa çıkan artık bit'lerin azaltılması için yeni metotlar ve tahmin edici sistemler geliştirilebilir. Bu aşamada hibrid teknoloji içeren çözümler önerilerek kuantum anahtar dağıtımı sistemlerinin daha tercih edilebilir ve kullanılır sistemler olması sağlanabilir.

G. Kuantum Anahtar Dağıtımı Protokollerine Önerilen Makine Öğrenmesi Çözümü

Yukarıda bahsedilen kuantum anahtar dağıtımı senaryolarında gözlemlenebileceği gibi anahtar dağıtımı işlemleri esnasında ve tarafların gerçekleştirdikleri uzlaşı protokolleri esnasında karşılıklı olarak denk gelmeyen artık bit'ler oluşmaktadır. Bu artık bit'lerin azaltılması anahtar dağıtımı sistemlerinin daha efektif ve başarılı veri aktarımı yapabilmesini sağlayabilir. Kuantum anahtar dağıtımı sistemleri gerçek rastgele anahtar değerleri üretmelerine rağmen bu üretme işleminde kullanılan kübit'lerin belirli bir sayıda polarizasyon filtresinden geçtiklerini görebilirsiniz. En karmaşık ve fazla sayıda kübit içeren sistemlere dahi sahip olmamız durumunda bile kullanılan polarizasyon filtreleri bilinen yöntemlerde 6 adeti geçmemektedir. Dolayısıyla oluşturulacak bir veri setinden polarizasyon filtrelerinin makine öğrenmesi metotları ile tahmin edilmeye çalışılması elde edilecek sonuçlar doğrultusunda faydalı sonuçlar verebilir ve artık bit'lerin azaltılmasında

kullanılabilir. Elde edilecek sonuçlar ile kuantum anahtar dağıtımı algoritmalarının performansları arttırılabilir.

1. Genel Açıklama

Bu amaç doğrultusunda doktora çalışmamızda, öncelikle çokça kullanılan kuantum anahtar dağıtımı yöntemlerinden biri olan BB84 algoritması MATLAB platformunda kodlanarak simüle edilmiştir. Daha sonrasında elde edilen sonuçlar ile bir veritabanı oluşturulmuştur. Elde edilen veritabanı üzerinden öncelikle aşağıda bahsedilen tahmin ve sınıflandırma algoritmaları uygulanmış daha sonrasında ise tahmin işlemi için bir yapay sinir ağı tasarlanarak Bob tarafında uygun polarizasyon filtreleri tahmin edilmeye çalışılmıştır.

2. Yapay Zeka Mimarisi

1950'li yıllarda ortaya çıkan yapay zekâ teriminin temeli daha öncesinde zeki sistemler olarak adlandırılan basit otomasyon sistemlerinden beslenmektedir. Bilgisayarların hayatımızda oldukça sıradan gibi gözüken yaygın yer alma şekli, geçmiş zamanlarda herhangi bir sistemin içerisine dahil edilmiş olması ile zeki ve akıllı sistemler olarak adlandırılması için yeterli olabiliyordu. Zamanla zekâ ve akıllı sistem tanımları, teknolojinin gelişmesi ve ilerlemesi ile yeni ve üstün teknolojik ürünleri ön plana çıkarmıştır. Böylelikle eskiden yapay zekâ veya akıllı sistemler olarak tanıtılan ürünlere farklı adlar önerilmiş, ürün ve imalat sanayisinde örnek vermek gerekirse bu ön adlar otomatik sistem veya otomasyon sistemleri gibi isimlendirilmelere gidilmiştir. 1950'li yıllardan sonra yapay zekâ sistemlerinin temel amacı insanın olduğu alanlarda, yapabildiği işlere destek olabilen ve yapması uzun süren işlemlerde insanları taklit ederek daha hızlı işlem yapabilmesini sağlayabilmek olmuştur. Bu amaç doğrultusunda yapay zekâ sistemleri; ham ve anlamlandırılmış verileri içeren, bu verilerden belirli bir organizasyon ve sistem ile bilgi üreten, elde edindiği bilgilerden öğrenme işlemini gerçekleştirebilen, belirli öğrenilmiş problemleri çözme yeteneğine sahip, belirli kesimlerce üretilen teoremlerin ispatında yer alabilen ve ispat aşamalarında kullanılabilen bir teknoloji olarak günümüzde kadar gelmiştir.

Temelde bu sistemler kurulan matematiksel mekanizma ile ham veriden bir bilgi çıkarmakta ve o bilgiyi, kurulan çoklu matematiksel fonksiyonlar içeren modellerde sonuca çevirmektedir. Elde edilen sonuç üzerinden bir öğrenim

oluşturmakta ve bu öğrenimin doğruluğu belirli parametreler ve/veya uzman kişilerce test edilip onaylandıktan sonra sınıflandırma ve kümeleme gibi işlemlerde kullanılmaktadır. Tüm bu sistemlerin en önemli unsuru başlangıç kısmında yer alan ham veri alanıdır. Yapay zekâ sistemlerinin eğitiminde kullanılan bilginin kalitesi ve doğruluğu ürettiği sonucun başarısı ve güvenilirliği ile doğru orantılıdır. Böylesi bir durumda veri ve elde edilme yöntemleri, kullanılan veri kontrol, düzeltme ve iyileştirme yöntemleri de yapay zekâ sistemleri gibi önem kazanmıştır.

Bir bilgiyi elde etmek veya üretmek için geçmişten günümüze kullanılan yöntemler aşağıdaki gibidir:

- Anket düzenleme, uzmanlardan görüş alma, yapılacak işlemin teknik alanına göre kaynak taraması yapmak ve mülakat yöntemi ile belirli bir konuda bilgi elde etmek.
- Örnek olayları inceleyip bilgiyi elde etmek.
- Kurulu cihazlardan ve sensörlerden düzenli ve kontrollü veri depolaması yapmak.

Yukarıda yer alan yöntemler ve benzeri yöntemler ile elde edilen verilerin kontrol edilmesi, içeriğinde yer alan aykırı verilerin belirli kurallar dahilinde ayıklanması gerekmektedir. Örnek olarak anket ve mülakat yolu ile elde edilen verilerde aykırı ve hatalı verilerin elde edilmesi sıkça rastlanılan bir durumdur. Kişi kilosu ile ilgili bir veri alma işleminde şahıslar bilerek veya bilmeyerek hatalı bilgi aktarımında bulunabilirler, bu konu ile ilgili bilgi aktarımı yapmak istemeyebilirler. Böylesi durumlarda istatikstiksel olarak verilerin bir histogramı çıkaraılarak, aykırı ve anormal verilerin gözlemlenmesi ve normalize edilmesi çözüm olarak önerilebilecek sistemlerin başında gelir.

Verinin bir diğer önemi ise verinin kullanımı ile gelişen Yapay Zekâ alt sistemleridir. Eğer geliştirilen bir yapay zekâ sistemi bir konu uzmanı tarafından kontrol ediliyor ve sistemin öğrenme işlemi için kullanması gereken öznitelikler önceden belirlenerek sistemin bu değerler üzerinden öğrenim ve tahmin işlemleri yapması isteniyor ise bu sistemler **Makine Öğrenmesi** olarak adlandırılmaktadır. Bir diğer Yapay Zekâ alt dalı olan **Derin Öğrenme** sistemlerinde ise makine öğrenmesinden farklı olarak sisteme öznitelikler belirlenerek verilmemektedir. Derin

öğrenme sistemlerinde büyük bir veri yığınından öznitelik çıkarımını sistemin kendisi yapmaktadır.

3. Veritabanı Mimarisi

Geliştirilen veritabanı mimarisi BB84 algoritmasının simule edilmesinden sonra oluşmuştur. Veritabanında gönderici Alice ve alıcı Bob tarafında seçilen polarizasyon filtreleri, üretici ve alıcı tarafında elde edilen polarizasyon sonrası okuma sonuçları ve uzlaşı protokolünün sonucunun yer aldığı bir sütun bulunmaktadır. Toplam 5 adet sütunda veriler yer sayısal değer olarak yer almaktadır. BB84 algoritmasında toplamda 4 adet polarizasyon filtresi bulunduğundan her bir polarizasyon yönü için 1'den 4'e kadar rakamlar ile atanmıştır. 0º derece için 1, 45º derece için 2, 90º için 3 ve 135º için 4 değeri ile sütunlarda karşılık yer almaktadır. Her iki tarafta da polarizasyon sonucunda elde edilen değerler 1 ve 0 olarak kayıt edilmiştir. Benzer yöntemlerde polarizasyon sonuçları 0,1 ve negatif pozitif değerler olarak sembolize edilmektedir, ancak Qbit değerlerinden normal bit değelerine dönüşüm yapıldığından tekrar 1 ve 0 değerleri kullanılmaktadır.

Veritabanı yapay sinir ağının ve tahmin yöntemlerinin eğitiminde efektif bir şekilde kullanılmaktadır. Bu yöntemlerin eğitimi esnasında veritabanı verilerinin belirli sabit bir kalıpta ve yöntemsiz kullanılması ilgili algoritmaların "ezberleme" adı verilen sorunla karşılaşmasına sebep olmaktadır. Yöntemlerin verileri ve sonuçlarını ezberlemelerini engellemek için öncelikle veritabanında eğitim ve tahmin işlemleri için kullanılan oranlar farklı kombinasyonlarda denenmiştir. Öncelikle %90 eğitim ve %10 test oranından başlanarak sırası ile bu oranlar %25 test %75 eğitim, %40 test %60 eğitim ve %50 test %50 eğitim olarak kullanılmıştır. Bu eğitim setleri tahmin yöntemlerinde farklı uzunluklarda veri bloklarında da uygulanarak eğitim için kullanılan veri büyüklüğünün eğitim oranına göre değişimi yöntem bazlı kontrol edilmiştir.

Bu işlemlere ek olarak eğitim için ayrılan veri setinin öğrenme işleminde farklı besleme yöntemleri ile kullanılması gerekmektedir. Eğitim için ayrılan veri bloğunun sürekli olarak aynı oranda sisteme besleme için verilmesi tekrardan ağın ve yöntemin veri bloğunu ezberlemesine sebep olabilir. Bunun önüne geçmek için **"kFold"** ve **"partitioning"** benzeri bölümleme yöntemleri uygulanarak eğitimde kullanılması

sağlanmıştır. Bu bölümleme yöntemlerinden **"kFold"**, eğitim için kullanılan veri bloğunun k adet eş parçaya bölerek her bir parçayı sistemi eğitmek için sırası ile kullanır.

Şekil 4 kFold ve partioning benzeri bölümleme örneği

Diğer bir veritabanı bölümlendirme yöntemi olan **"partitioning"** işleminde eğitim için kullanılan veri bloğundan belirlenen sayıda ve belirlenen oranlarda rastgele bölümler çekilerek eğitim için kullanılır. Böylelikle sabit bir bölünme yapılmaksızın eğitim işlemi her bir eğitim tekrarında veri bloğunundan farklı bir bölüm ile eğitilerek ağın ve yöntemin veriyi ezberlemesi engellenmiş olur.

Tezimizin bir sonraki bölümünde tahmin algoritmaları olarak kNN, Naive Bayes, Decision Tree- Karar Ağacı ve Dicriminant Analiz yöntemleri açıklanacaktır. Doktora çalışmasında bu yöntemlerin kullanılan farklı alt dalları ve metotları anlatılacaktır. Bu yöntemlerin ve alt dallarının birbirilerine göre meydana getirdiği farklılıklar Test ve Sonuçlar kısmında aktarılacaktır. Kullanılan yöntemlerin hem birbirileri hem de kendi iç metotlarının performansları farklı veri büyüklüğüne ve farklı eğitim oranlarına göre test edilmiştir.

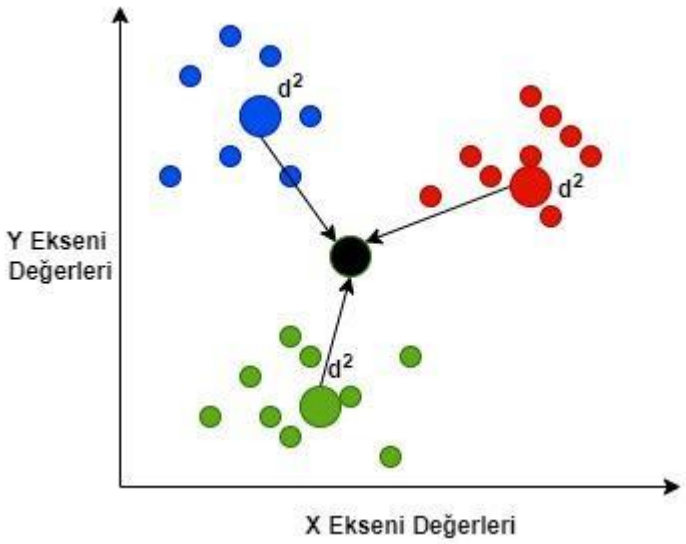
4. kNN Yöntemi

Geçmiş verilerden bir bir eğitim yaparak karakteristik değer elde eden makine öğrenmesi yöntemleri daha sonrasında bu değerleri sınıflandırma, kümelendirme ve tahmin işlemlerinde kullanmaktadır. Dilimize çevirisi K'ıncı En Yakın Komşu teoremi olarak geçen kNN yöntemi, kümelendirme işlemlerinde sıkça kullanılan en basit yöntemlerden biridir.

Elimizde bilinen kategorileri olan bir veri seti olduğunu düşünebiliriz. Bu verileri farklı yöntemler kullanarak kümeleyebilir (PCA, kMeans vb) ve iki boyutu

koordinat sisteminde gösterebiliriz. kNN algoritması bahsedildiği gibi bir veritabanı ve kümeleme durumuna göre eğitilebilir. Bu işlemin sonucunda koordinat düzlemine yeni bir veri eklendiği zaman, verinin parametrelerine göre koordinat düzleminde alacağı yer belirlenebilir. Konumlanması tamamlanan verinin hangi kümeye ait olduğunun bulunması için verinin yakınında yer alan hücrelere olan uzaklığının ölçülmesi gerekmektedir. En yakın olduğu hücre veya en fazla yakınlığının bulunduğu kümeye göre atama işlemi yapılabilir. Bu hesaplama esnasında "euclidean distance", öklid mesafe ölçümü kullanılabileceği gibi aynı zamanda çoklu boyutlarda farklı mesafe ölçüm algoritmaları kullanılabilir. Yöntemde ki "k" sayısı kaç adet komşu gruba olan yakınlığının ölçümünü sembolize eder. Eğer k sayısını çok düşük tutulursa tahmin edilebilir ve basit bir kümelendirme görebiliriz, eğer k sayısı çok fazla tutulur ise kümeleme durumuna uygun olmayan bir bütünlüğün gözükmediği sonuçları elde etmek mümkündür. Bahsedilen k değerinin ideal veya en iyi değerinin tespit edilmesi pek net bir durum değildir. Yöntemin deneneceği sistemin ideal kümeleme senaryousuna göre bir değer tahmin edilebilir veya istenebilir. Farklı durumlarda ideal k değerini hesaplamak için birden fazla tekrar yapılarak değer tespit edilmeye çalışılabilir.

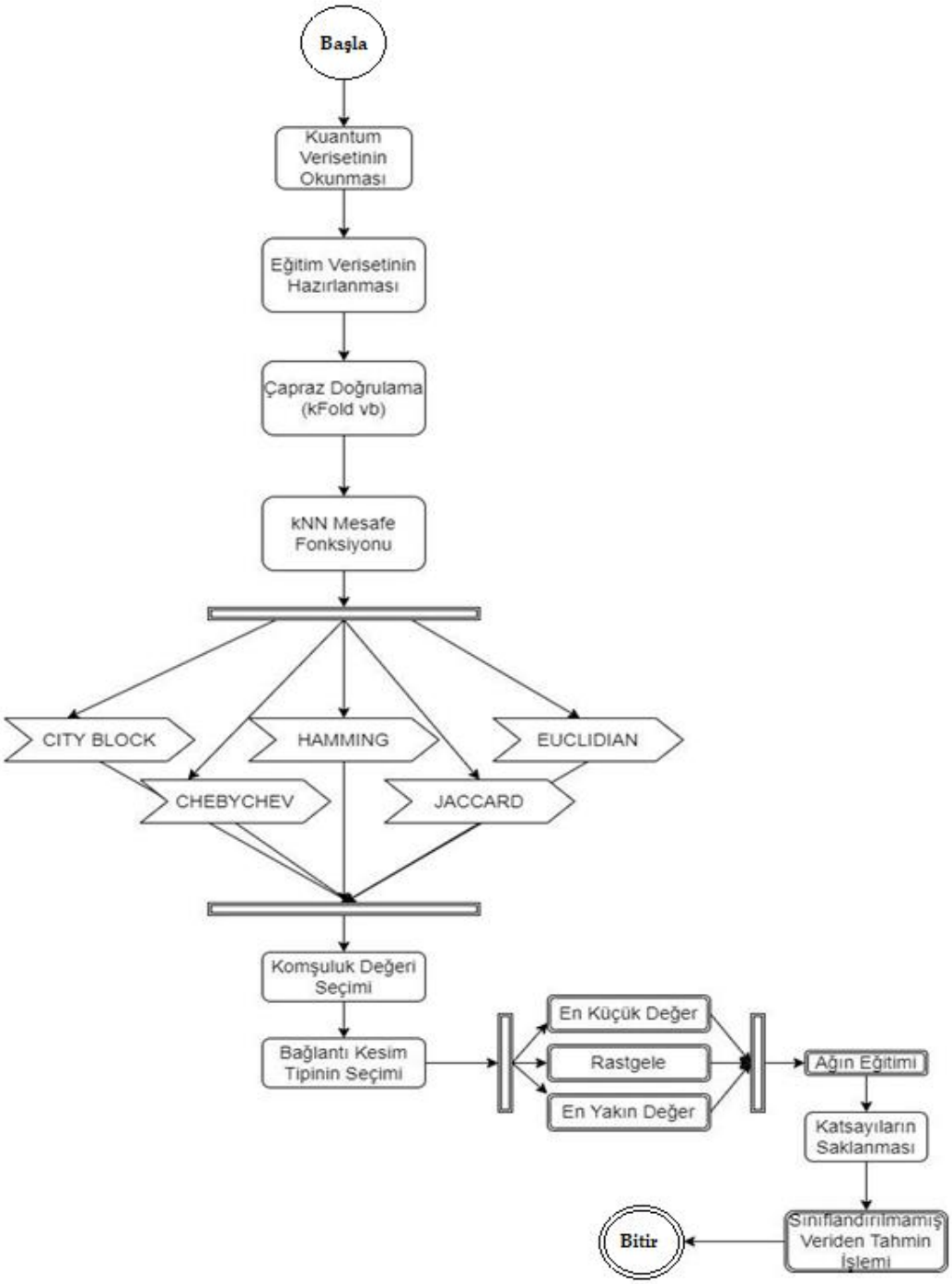
Elde edilen sonuçların görselleştirilmesi kısmında iki boyutlu koordinat düzleminde görüntüleme işlemleri yapılabilir. Görselleştirme için hat sınıflandırması, sıcaklık haritası gibi görselleştirme metotları da kullanılabilir.



Şekil 5 Görselleştirme örneği

kNN yönteminde kullanılan bir diğer kümeleme mantığı ise hiyerarşik kümelemedir. Bu yöntemde örnek verme işlemini koordinat düzleminden farklı olarak ısı-sıcaklık haritalarına göre verebiliriz. Bu yöntemde kare matris şeklinde sıralanan küme değerlerinin her bir satırında bir kümeye ait veri değerleri yer alacaktır. Kümelenmesi gereken veri bloğu atandığı satır ve sütun değerlerinde yer alan sütun bazlı değerlere göre ait olduğu küme belirlenebilir. Eğer ait olduğu küme değerleri tek bir kümeye ait değil ise oylama yöntemi ile en ideal küme belirlenir. Eğer oylama sayısal sonuçları aynı gelir ise rastgele olmak üzere eşit kümelerden biri seçilir veya sınıflandırma başarısız olmuştur denilerek işlem kapatılabilir.

Aşağıda doktora çalışmasında kullanılan kNN yönteminin genel şeması yer almaktadır. Doktora çalışmamızda Matlab platformunda kNN yöntemi kullanılmış, eğitim işlemi esnasında eğitim veri seti %50 eğitim %50 test oranından %25 eğitim %75 test oranına kadar farklı kombinasyonlarda denenmiştir. Eğitim için ayrılan veri setleri kFold gibi veri setinin belirli bir sayıya göre alt kümelere ayrılmasını ve eğitim için her bir tekrarda farklı bir eğitim alt kümesinin kullanılması esasına dayanmaktadır. Şekil 6'da kNN genel sistem diyagramı paylaşılmıştır. Aşağıda yer alan tüm komşuluk mesafesi hesaplama yöntemleri kullanılarak kNN sonuçları elde edilmiştir.



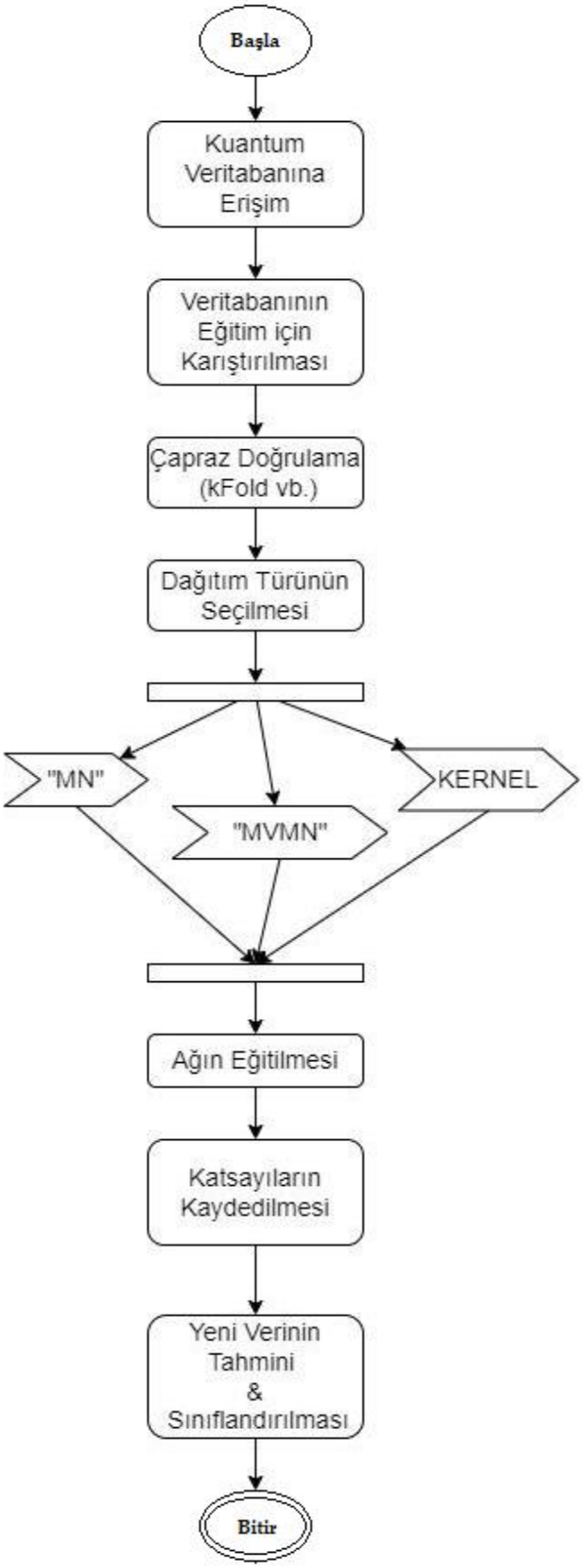
Şekil 6 kNN genel sistem diyagramı

Bu doğrultuda yukarıda yer alan CITY BLOK, HAMMING, EUCLIDIAN, CHEBYCHEV ve JACCARD mesafe hesaplama yöntemleri farklı büyüklükteki veritabanları ile eğitim işlemlerinde farklı eğitim oranları ile denenmiştir. Mesafe hesaplama yöntemlerine ek olarak komşuluk kısıtlama değeri de 2'den 4'e kadar farklı değerlerde denenerek sonuçları gözlemlenmiştir. Sonuçları ilgili yöntemler ve kullanılan veri bloklarının uzunluğuna göre test ve sonuçlar kısmında yer almaktadır.

5. Naïve Bayes Yöntemi

Naive Bayes yöntemin olasılıksal değerler üzerinden tahmin işlemleri yapmaktadır. Bu yöntemde, eğitim için kullanılan kontrollü veri setinde her bir kümeye ait elemanlar ile bu elemanların varsa alt bileşenlerinin olasılıksal olarak kendilerine ait kümelerde yer alma sıklıkları ve olasılıkları hesaplanır. Bu işlemlere öncelikle "ground truth" adı verilen kontrollü eğitim kümesinin histogramı bulunarak başlanılır. Histogram küme içerisinde yer alan nesnelerin sıklık değerini bize gösterir.

Tüm histogram hesaplamaları tamamlandıktan sonra küme içerisinde yer alan tüm elemanların toplam eleman değerine göre olasılıksal değerleri hesaplanır. Eğer sınıflandırma için gönderilecek yeni değer tekil olarak hesaplanacak ise kümeler içerisinde yer aldığı maksimum olasılık değerlerine göre karar verilir, eğer çoklu değerler içeren bir dizi eleman ise, her bir elemanın yer aldığı kümedeki olasılıksal çarpımlarının sonuçları kontrol edilir. Elde edilen en yüksek olasılık sonucuna göre ilgili kümeye atama işlemi yapılabilir. Bazı durumlarda veri kümelerinde ortak değerler yer alabilir veya benzer değerler farklı küme içerisinde tekrarlanıyor olabilir. Küme bazlı histogramlarda her verinin bütün kümelerde tekrar etmemesi hali yaşanabilir. Bu durumda olasılık hesaplaması yapılırken tüm tekrar ettiği küme elemanlarının histogramı elde edilerek olasılık bu değer üzerinden hesaplanmalıdır. Histogram analizinde bu değerin olmadığı alanlar sıfır "0" değeri alacaktır ve eğer bağlantılı olduğu diğer küme elemanları ile ortak olasılık hesaplaması yapılacağı zamanda olasılık çarpım sonucunu sıfır olarak oluşturacak bir durum ortaya çıkacaktır. Böyle durumlarda doğru hesaplama yapabilmek için her bir eleman histogramında bir değer arttırılabilir. Tüm değerlerde bir arttırma işlemi yapıldığında olasılık değerinde bir sapma olmayacaktır ancak çarğım durumunda tüm olasılık sonucunu etkileyecek durum ortadan kalkarak, daha doğru atama işlemi gerçekleştirilebilir. Şekil 7'de doktora çalışması kapsamında hazırlanmış Naive Bayes yöntemi genel şeması yer almaktadır.



Şekil 7 Naive Bayes genel sistem diyagramı

Diğer yöntemlerde olduğu gibi, veritabanından elde edilen değerler, "**kFold**" ve "**Random Partitioning**" değerlerine göre farklı boyutlardaki eğitim veri setleri farklı oranlarda ağın eğitim işlemlerinde kullanılmıştır. Yukarıda genel şemada görebileceğiniz gibi Naive Bayes yönteminde olasılıksal dağılımların hesaplanması işlemi temelinde sınıflandırma yapılır bu yüzden farklı olasılıksal tahmin yöntemleri Naive Bayes yönteminde performans kıyaslaması amacı ile kullanılabilir. Bu amaç doğrultusunda "MN"- MultiNomial dağıtım, "MVMN"- MultiVariate Multinomial dağıtımı, "KERNEL" isminde farklı olasılık dağıtımını hesaplayan denklemler ve sonuca etkileri test edilmiştir. Bu yöntemlerden Denklem 2'de paylaşılan MN-Multinominal dağıtım Bag-of-Tokens modelini kullanarak, "j" değerinin k sınıfı içinde olasılıksal tekrarını hesaplar.

$$P(token\ j\ |class\ k) = \frac{1 + c_{j/k}}{P + c_k}$$

(Denklem 2)

Eğer tahmin için kullanılan değişken çok terimli bir dağılıma sahip ise Naive Bayes işleminde Multivariate Multinomial dağıtım yöntemini kullanır. Bu işlemde ihtimaller arasındaki benzersizlik seviyelerinin bir histogramı elde edilir. K ismi verilen bir sınıf içerisinde j tahmincisinin L düzeyine sahip olma olasılığını aşağıda paylaşılan Denklem 3 üzerinden hesaplayabiliriz.

$$P(predictor\ j \mid L\ class\ k) = \frac{1 + m_{j/k}(L)}{m_j + m_k}$$

(Denklem 3)

Kernel yönteminin tercih edilmesi durumunda sistemde tanımlı olan tahmin yöntemlerini kullanabiliriz. Gaussian, Epanechnikov, Triangular vb yöntemleri veya kulanıcılar tarafından tasarlanabilecek bir olasılıksal tabanlı tahmin fonksiyonu kullanılabilir. Denklem 4'de Epanechnikov tahmin denklemi, Denklem 5'de Gauss tahmin denklemi ve Denklem 6'da Triangular tahmin denklemi paylaşılmıştır.

$$f(x) = 0.75(1 - x^2)I\{|x| \leq 1\}$$

(Denklem 4)

$$f(x) = \frac{1}{\sqrt{2\pi}} \exp(-0.5x^2)$$

(Denklem 5)

$$f(x) = (1 - |x|)I\{|x| \leq 1\}$$

(Denklem 6)

Naive Bayes yönteminin en temel dezavantajı ise elde edilen veri serileri içerisinde semantik -mantıksal- bir anlam bütünlüğü oluşturamamasıdır. Sıralı ve anlam bütünlüğü içeren veriler, örneğin bir e-mail yazısı içerisinde kelimelerin yeri ve sırasının filolojik bir anlam içermesi gibi, karmaşık bir şekilde sıralanarak verildiği zamanda sınıflandırma işlemini gerçekleştirebilir. Bir e-mail içeriğine bakılarak, e-mail'in spam veya normal bir mesaj olduğunun anlaşılması işleminde kelimelerin tekrarlanması ve olasılıklarına bakıldığından semantik bir sıralama olmaması durumunda da sınıflandırma işlemi yapılabilir. Ancak okuyucu için bu mesaj sınıfladırması kabul edilebilir değildir.

6. Karar Ağacı Yöntemi

Karar ağacı sistemleri genel olarak veri kümesinden veya değerlere sorulan sorulara alınan cevaplara göre sınıflandırma işlemi yapar. Sınıflandırma işlemi kategorik olabileceği gibi numerik değerlere bağlı ve evet/hayır verileri de içerebilir. Tüm vu adımlar ile yapılması istenilen şey, doğruluğu yüksek oranda bir sonuca ulaşabilmektir.

Karar ağaçlarında sınıflandırma ve tahmin işlemleri sağ ve sol olarak (bazı durumlarda ortada bir dal daha ilerlemesine rastlanılabilir) iki farklı **"dal- branch"** üzerinden ilerlemektedir. Her dal'da yukarıda bahsedilen farklı türlerdeki sorgu işlemlerinin yapıldığı **"düğüm- node"** 'lar yer almaktadır. Sorgunun en tepesinde yer alan düğüm **kök düğüm** olarak adladırılır. Tüm diğer düğümler bu kök'ten türeyen düğümlerdir. Bu düğümler sonrasında daha doğru bir tahmin ve sınıflandırma işlemi yapabilmek için ya bir sonraki seviyede yer alan düğüm sorgusuna girilir ya da var olan seviyede yer alan düğümün sonucu sınıflandırma sonucu olarak kabul edilir. Giriş ve bir sonrasındaki seviyede yer alan düğümler **"interval nodes"** olarak adlandırılır. Sistemde ne kadar fazla düğüm kullanılırsa o kadar karmaşık bir sistemin karmaşıklığı o kadar artar.

İki farklı dal'dan ilerleyen düğüm sorgularında dikkat edilmesi gereken husus, aynı seviye düğüm sorgularında farklı soruların sorulması gerektiğidir. Sayısal, kategorik veya evet-hayır türünden soruların aynı seviyede sorulmasında bir sakınca yoktur ancak bu aynı tip soru türlerinin aynı soruyu içermemesi geremektedir. Ancak aynı türde ve içerikte sorular farklı seviyelerde ve dallarda yer alan düğümlerde tekrarlı olarak sorulabilirler. Son seviye düğümlerden sonra elde edilen sınıflandırma sonuçları ise **"yaprak-leaf"** olarak adlandırılır. Yaprak düğümleri bir önceki düğüm tarafından bir ok ile işaretlenir ancak yaprak düğümlerinden sonra bir başka düğüm veya leaf yer almaz, herhangi bir ok ile yaprak düğümünden sonra işaretleme yapılmaz. Karar ağacının farklı seviye düğümlerinde ve benzer seviyelerde aynı yaprak düğümler yer alabilir.

Önemli bir diğer konu karar ağacının kök düğümünün hangi sorgu ile başlayacağına karar verilmesidir. Elde edilen veri setinden her bir veri sütununun sonuç sütunu ile olan tekil ilişkisine bakılmalıdır. Bunun için en az kirliliğe sahip sütunun bulunması gerekmektedir. Bu işlem her bir sütunda gini katsayısının hesaplanılması ile elde edilir. Veri setinde yer alan sonuç sütunu ile her bir sütunun ve sütunlarda yer alan değerlerin sonuç ile olan ilişkisinin sorgulanması durumudur. Örneği elimizde bir kalp rahatsızlığı ile ilgili veri setinin olduğunu kabul edelim. Veri setinin sütunlarında göğüs ağrısı, yüz renginde solukluk ve damar tıkanıklığı verilerinin olduğunu düşünelim. Her bir veri sütununun kalp krizinin sebebi olma durumunu birbirinden bağımsız olarak sonuç sütunu ile ilişkilendirmek gerekmektedir. Sütun değerlerine göre kalp krizi geçirenlerin her birinde göğüz ağrısı olup olmadığını sorgulayıp sonuçları bir kenara not edebilir ve daha sonrasında kalp krizi geçirenlerde göğüs ağrısı yaşama ve yaşamama durumunun tüm vakalara bölümü ile gini katsayıları hesaplanır. Bu işlem tüm sütunlarda teker teker yapılır ve en düşük gini katsayısına sahip olan sütun en düşük kirlilik oranına sahip olacağından kök düğüm olarak atanır. Düğümler en az kirlilik oranına göre sırası ile kök düğümden en alt düğüme kadar sıralanır. Kirlilik oranı arttıkça sonuca etki eden veri sütununun içerisinde her iki değerden de karışık miktarda bulunduğunu göstermektedir. Ne kadar az bir gini katsayısı elde edilir ise o kadar sonuca direkt etki eden bir düğüm elde edildiği düşünülebilir.

Veri sütunları ile sonuç sütunu arasında veri türü açısından bir benzerliği olmaması durumunda veya sonuç sütunu ile ilişkili veri sütununun sabit değerler

içerdiği ancak tahmin edilmesi gereken verinin bu sabit değerlere denk gelmemesi durumunda bazı sorunlar yaşanabilir. Böylesi durumlarda sütun içerisinde yer alan verilerin kapsayıcı ortalama değerler arasında konumlandırılıp daha sonrasında gini katsayısı hesaplamasının yapılması gerekmektedir.

Aşağıda doktora çalışmasında kullanıdığımız karar ağacı yönteminin genel bir mekanizması bulunmaktadır. Bu işlemde diğer sınıflandırma yöntemlerinde olduğu gibi işlemlere verinin elde edilmesi ve eğitim için hazırlanmasından başlanılmıştır. Veriler farklı boyutlarda elde edilmiş, farklı oranlarda ve kFold, partitioning gibi yöntemler kullanılarak çapraz doğrulamaya tabi tutulmuştur. Bu işlemler ile birlikte hem verinin farklı oranlarda eğitiminin sonuca etkisi kıyaslanmış olup hemde verinin ezberlenmesi sorununa engel olunmaya çalışılmıştır. Karar ağacı mekanizmalarında önemli olan unsurlar yukarıda anlatıldığı gibi ideal bölünme sayısının bulunması ve kullanılan veri setine uygun bir bölünme kriterinin tespit edilmesidir. Bu amaçla matlab platformunda bölünme kriteri olarak yukarıda anlatıldığı gibi sıkça kullanılan kriterlerden biri olan Gini katsayısı kullanılmıştır. Ek olarak "Twoing" kriteri ve "Deviance" değer hesaplaması yapılabilir. Kırınım hesaplama kriterlerinin performansa etkisi karşılaştırılmak istenilmiştir. Sınıflandırma işleminden elde edilmek istenilen sonuç temel olarak karşı tarafında polarizasyon filtresi olduğundan bu işlem için Şekil 8'deki şemada da görülebileceği üzere bir kırınım sonucunda gerekli sonucun elde edilmesi planlanmıştır. Denklem 7'de Deviance, Denklem 8'de GNI ve Denklem 9'da Twoing formülleri paylaşılmıştır.

$$-\sum_{i} p(i)\log 2\, p(i)$$

(Denklem 7)

$$1-\sum_{i} p^2(i))$$

(Denklem 8)

$$P(L)P(R)\left(\sum_{i}|L(i)-R(i)|\right)^2$$

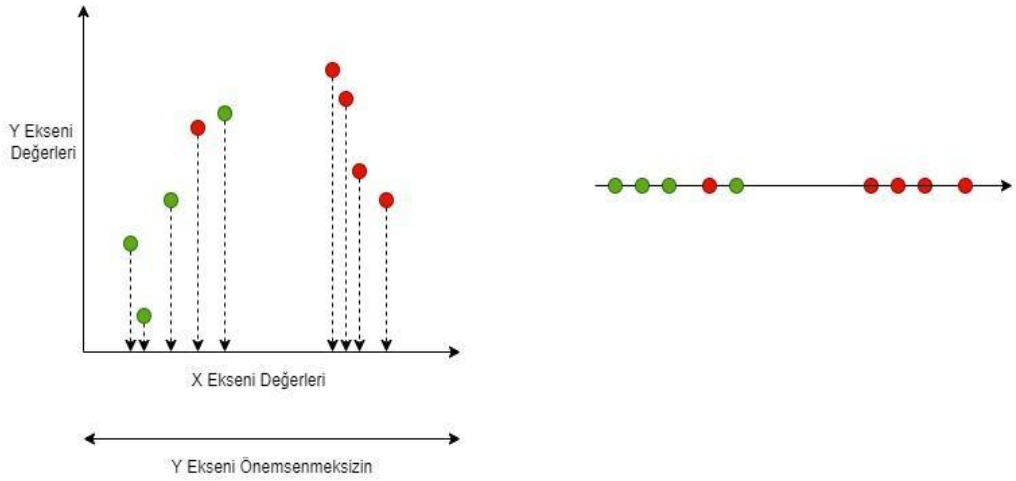
(Denklem 9)

Şekil 8 Karar ağacı genel şeması

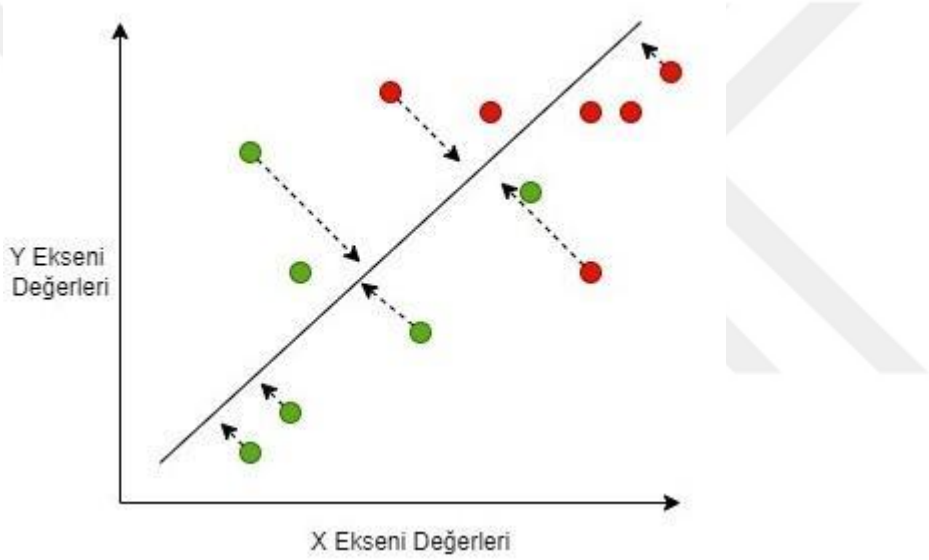
7. Diskriminant Analizi Yöntemi

Discriminant Analysis yöntemi temel olarak kategorisi bilinen sınıflar arasındaki ayrıştırabilme durumunu maksimize etmeye çalışır. Büyük veri bloğunu kategoriler halinde gösterebilme ve bu veri bloklarını ideal bir düzlemsel ortamda ayrıştırma bilmeyi amaçlar. Ayrıştırma işleminin görselleştirilmesi için iki boyutlu koordinat düzlemi kullanışlı bir yöntem olabilir. Veri bloğunun kategorilerine ayrıştırılması ve ayrıştırılmış kategorilerin maksimize edilmesi işleminde koordinat düzleminde üç farklı özelliğe göre ayrıştırma işlemi yapılabilir. Görsel olarak iki boyutlu ekranlar kullanıyor olmamızdan dolayı üçten fazla boyut ve düzlemde gösterim ve ayrıştırma yapma işlemi mümkün olmamaktadır. Ayrıştırma işlemi ve kategoriler arasındaki ayrışımın maksimize edilmesi tamamlandıktan sonra sonucu belli olmayan bir veri bloğunun veya tekil verinin koordinat düzleminde en yakın olduğu kümeye atanması kolaylıkla sağlanabilir. Tersinir bir şekilde, elde edilen 3 boyutlu sınıflandırma işlemi 2 boyuta ve 2 boyutulu sınıflandırma işlemi bir boyutlu lineer grafiğe entegre edilebilir.

Bu tarz bir işlem yapılmasının temel sebebi yukarıda da bahsedildiği gibi mevcut yöntemin ayrıştırma işini maksimize edebilmesidir. Bu özelliğinden bakılacak olursa Discriminant Analysis yöntemi bir boyut indirgeme yöntemi olarak karşımıza çıkmaktadır ve PCA-Principal Component Analysis yöntemi ile benzemektedir. Discriminant Analysis yönteminin bahsedilen kullanımında dikkat edilmesi gereken işleminde hangi eksen tabanında boyut indirgeme işleminin yapılacağıdır. Şekil 9, Şekil 10 ve Şekil 11'de ilgili örnekler paylaşılmıştır.

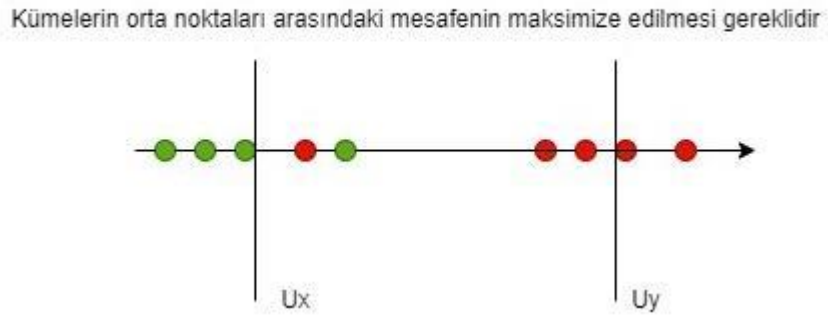


Şekil 9 X ekseninde boyut indirgeme örneği



Şekil 10 Diagonal eksende boyut indirgeme örneği

Tekil eksenler bazında boyut indirgeme işlemi yapmak her durumda başarılı sonuçlar doğurmayacağından eksenler arası bir ayrıştırma işlemi gerekmektedir. Bu doğrultuda elde edilecek değerler ile iki boyutlu düzlemden tek boyutlu bir düzleme geçilebilir. Bu işlem sonucunda elimizdeki verileri tek bir düzlemde konumlandırabiliriz. İlk olarak grupları mean değerlerinin bulunması gerekmektedir. Gruplar bazında elde edilen ve test edilen mean değerlerinin birbirlerine göre değer olarak uzaklıkları arttırılmalıdır. Bir diğer işlemde ise bu grupların varyasyon değerleri hesaplanılarak, ilgili değerlerin arasındaki farkın azaltılması gerekmektedir.



Şekil 11 Kümeler arası mesafe görsel örneği

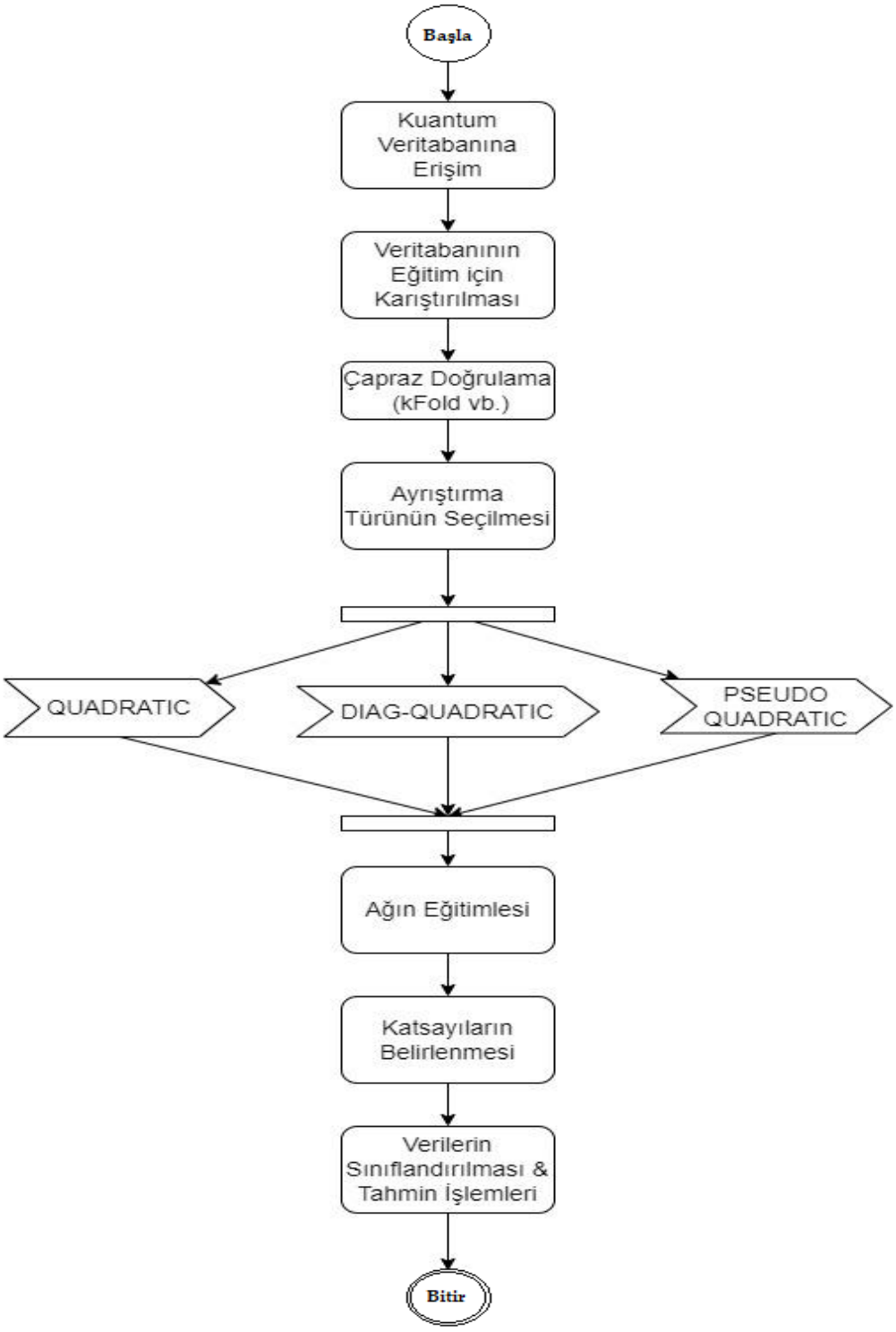
$$\frac{(meanX)^2 - (meanY)^2}{Sx^2 + Sy^2} = \frac{a}{b}$$

(Denklem 10)

Yukarıdaki denklemde yer alan "a" değerinin ideal olarak büyük değerde olması beklenir. Diğer parametre olan "b" değerinin ideal olarak küçük değerlerde olması beklenir. Bu işlemi üç boyutlu bir düzlemde yani üç farklı veri kategorisinde yaptığımızı düşünelim. Böyle bir durumda boyut indirgenerek sınıflandırma yapmak için yukarıda denklem için güncelleme yapmamız gerekir. Yukarıda yapılan işlemlerden farklı olarak koordinat sisteminde yer alan üç farklı kategori için veri orta noktaları bulunur ve bu koordinat düzleminin merkezinde yer alan bir orta nokta seçilir. Yukarıda bahsedilen işlemler benzer bir şekilde bu orta noktaya göre tüm kategoriler için yapılarak sonuç elde edilir.

Doktora çalışmasında Discriminant Analiz yöntemi aşağıdaki genel şemada yer alan adımlar doğrutulsunda ilerlemiştir. Ayrıştırma yöntemi olarak "Quadratic", "Diag-Quadratic" ve "Pseudo Quadratic" yöntemleri denenerek, yöntemlere göre performans kıyaslaması işlemleri yapılmıştır. Bahsedilen yöntemlerin haricinde "Linear", "Diag-Linear" ve "Pseudo Linear" gibi sınıflandırma yöntemleride bulunmaktadır ancak benzer sınıflandırma işlemlerinde elde edilen sonuçlara göre ilk bahsedilen yöntemlerin kullanılması uygun görülmüştür. Kullanılan yötemlerin değişimi sınıflandırma ve boyut indirgeme işlemlerinde kullanılan kovaryans matrislerinin yapısındaki değişimleri sembolize eder. En basit açıklama ile "Quadratic" fonksiyonunun kullanımı kullanılan kovaryans matrislerinin sınıflar arasında değişim göstereceğini, "Diag-Quadratic" fonksiyon kullanımının bu matrislerin köşegen olacağını, "Pseudo-Quadratic" ise kovaryan matrislerin tersine çevirilerek kullanılması durumudur. Tüm bu işlemlere göre elde edilen sonuçlara

göre en ideal yöntem belirlenecek ve ağın eğitimi işlemi tamamlanacaktır. Daha sonrasında sonucu belirli olmayan veriler eğitimde belirlenen katsayılara göre tahmin işlemi yapılarak sınıflandırılacaktır. Şekil 12'de ilgili görsel paylaşılmıştır.



Şekil 12 Diskriminant analizi genel şeması

8. Diğer Yöntemler

Regression Tree yöntemi karar ağacı yönteminin bir türüdür. Bu yöntemin karar ağacı yöntemlerinden farklı olarak her "leaf"-yaprak değerinde bir sayısal değer bulunmaktadır. Bu yöntem, discriminant analiz yönteminde düzlemsel ve doğrusal ayraçlar eklenerek ayrıştırmanın mümkün olmadığı durumlarda efektif olarak kullanılabilir. Ayrık olarak dağınıklık gösteren verilerin gruplandığı alanlarda bir ortalama değer bulunarak, regression tree node larının sınırlandırma sınır değerleri belirlenebilir. Bu sayede regression tree method bu belirli bölgelere göre eğitilip, node seviyesin bazında yüksek başarılı sonuçlar elde edilebilir. Bu ağ eğitimi esnasında ana kök node unun değerinin doğru belirlenmesi gerekmekte ve kırınımların yani kaç seviyede bir regression tree olacağının belirlenmesi önemlidir. Öncelikli olarak tüm değerlere göre ideal eşik değeri seçilmelidir. Tüm değerler üzerinden teker teker geçilerek; seçilen değer dışındaki tüm değerlerin ortalaması alınmalı ve tüm değerlerin bu ortalama değere göre olan uzaklıkları hesaplanmalıdır. İdeal değer olan ortalama değere olan uzaklıklarına "residual" artıklık denilir. En az toplam artıklık değeri en tepede yer alacak olan kök düğüm-node olarak adlandırılır. Bu hesaplama tüm değerlere yapıldığından elde edilen tüm artıklık seviyelerine göre ortalama değerler sıralanır ve bu sıralamaya göre regression tree'de yer alacak node'lar belirlenir. Dikkat edilmesi gereken çok fazla seviyede kırınım olmaması ve fazla node kullanılmamasıdır. Artan node sayısı sistemin performansını düşürür, karmaşıklığı arttırır ve temel yapay zekâ eğitim problemlerinden olan eğitim verisinden ağın tüm sistemi ezberlemesi "memorizing- overfitting" problemini ortaya çıkarır.

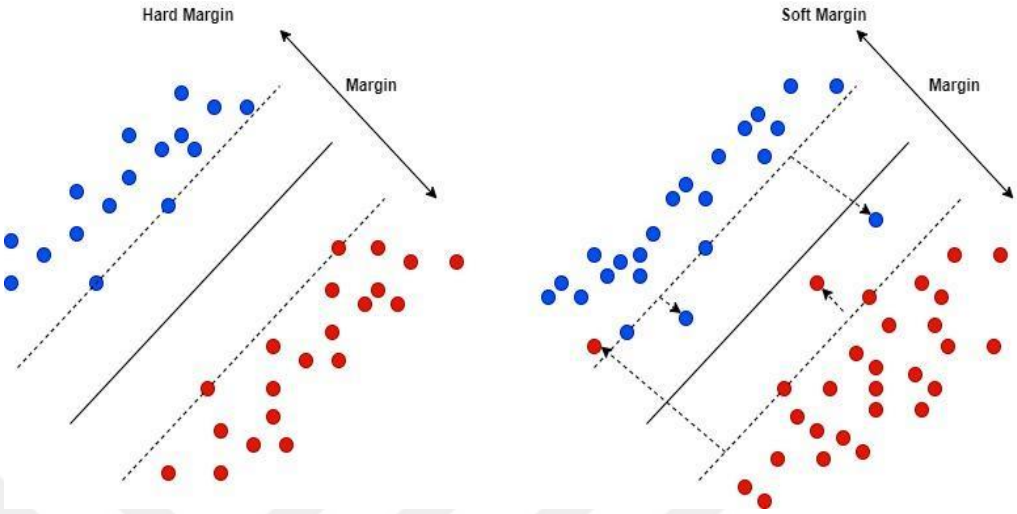
Random Forest yöntemi diğer karar ağacı ve türevi metotlardan farklı olarak eğitim veri setinden ilgili veri satırlarını rastgele seçerek ön yükleme veri setine aktarır. Daha sonrasında karar ağacını inşaa etmek için bu veri setinden her bir node için rastgele birden fazla veri sütünu seçer ancak bunlardan birtanesini kullanılır ve diğerlerini tekrar seçmek üzere bırakır. Kullanım yöntemine göre sadece bir adet veri sütunu seçilebilir. Elde edilen veri sütunu kök node olarak en tepede yer alır ve sağ, sol olmak üzere farklı kombinasyonlarda node'lara dallanır. Elde edilen yeni node'lar bir önceki kök node'da yapıldığı gibi rastgele seçilerek atanır. Bu rastgele atama yöntemi ile birden fazla farklı kombinasyonlarda karar ağacı oluşturulabilir. Elde edilen karar ağaçlarından en iyisini performansları ölçülerek belirleyebiliriz.

Random Forest yönteminde ilk başta ön yükleme veri setinde rastgele eğitim verilerinin seçildiğinden bahsetmiştik. Oluşturulan bu yeni veritabanı temel olarak eğitim veritabanından beslendiği için ve içeriğinde yer alan değerler tekrarlı bir şekilde eğitim veritabanından seçildiğinden, tekrarlı veriler içerebilir. Dolayısı ile eğitim verileri arasında hiç kullanılmamış verilere rastlanılabilir. Bu veriler "Out of Bag" değerler olarak adlandırılmalıdır. Bu değerler üretilen karar ağaçlarında test edilerek, doğru ve yanlış sınıflandırma sayıları ölçülür, bu ölçüme Out of Bag Error değeri denilir ve karar ağacının kalitesini ölçmek için kullanılır.

SVM- Support Vector Machine yöntemi, perceptron makine öğrenmesi yönteminin bir üst ve gelişmiş verisyonu gibi düşünülebilir. Perceptron yönteminde iki sınıflı bir sınıflandırma yöntemi ike SVM'de bu sınıf sayısı çok daha fazla olabilir. Perceptron yöntemi temel olarak koordinat düzeleminde birbirinden ayrıştırılması gereken iki farklı kümenin ayrışmasını sağlayacak bir doğru denklemini belirler bu iki veri kümesinin birbirinden bir doğru ve/veya düzlem ile ayrır. Bu doğru denklemi aslında bir eşik değeri oluşturmakta ve sınıflandırılması istenilen diğer bir verinin bu eşik değerine göre konumlandırılması sağlanmaktadır. Ancak SVM'de bu eşik değerinde margin adı verilen bir genişlik katsayısı mevcuttur. Sınıflandırma yapılması istenilen yeni değerin eik değerine çok yakın olması durumunu düşünelim. Değer eşik değerine göre farklı bir sınıfa atanabilir ancak eşik değerinin karşı kümesinde yer alan değerlere mevcut sınıfından değer olarak daha yakındır. SVM'de margin adı verilen bu aralık ayarlanarak aslında değerin olması gereken mevcut sınıfa eşik değerinden dolayı atanamaması engellenebilir. Eşik değerinin katsayı olarak atanması işleminde esas alınan nokta sınıfların eşik değerine ek olarak sınıfların orta noktalarının belirlenerek eşik değerinin konumunun güncellenmesidir. Böylelikle değerler yakın oldukları sınıflara daha doğru atanabilirler. SVM yöntemi eğitilirken margin değerini belirleyen katsayı ile alakalıdır. Eğer katsayı arttırılırsa margin alanı daralır ve sınıflandırma eşik değeri daha hassas olabilir ancak bu durumda SVM algoritması yukarıda diğer yöntemlerde bahsedilen ezberleme sorunu "overfitting" ile yüksek oranda karşılaşır. Eğer katsayı değeri azaltılır ise margin alanı genişler, sınıflandırma daha genel bir sınıflandırma olur ve overfitting sorunu çözülür. Elde edilmek istenilen sonuç doğrultusunda margin değeri bu kıstaslara göre ayarlanmalıdır. Denklem 11'de margin formülü paylaşılmıştır. Şekil 13'de SVM margin örneği verilmiştir.

$$y = \begin{cases} 0 \; if \; w^T.x + b < 0, \\ 1 \; if \; w^T.x + b \geq 0 \end{cases}$$

(Denklem 11)



Şekil 13 SVM margin örnekleri

9. Yapay Sinir Ağları

Yapay sinir ağları 1940'lı ve 1950'li yıllarda beynin sinir ağ yapısını modellenerek oluşturulmuş bir makine öğrenmesi yöntemidir. Diğer makine öğrenmesi ve sınıflandırma yöntemleri önceki bölümlerde anlatılmıştır. Bu yöntemlerde genel olarak kullabılan bir doğrusal veya düzlemsel ayıraç ile veri setinde sınıflandırmalar ve bölümlendirmeler yapılmakta veya oluşturulan bir yapısal sistem ile, karar ağaçlarıı gibi, sınıflandırılması istenilen veri en alakalı olan birime aktarılmaktadır. Yapay sinir ağları, insan beyninde yer alan ve biyoelektronik sinyallerin işlenmesinden sorumlu nöronlar ile sinyallerin aktarımından sorumlu sinapsların örnek alınarak modellenmesi ile oluşmuş karar ve tahmin sistemleridir.

Diğer sınıflandırma ve tahmin sistemlerinden farklı olarak yapay sinir ağlarında sınıflandırma için kullanılacak fonksiyonlar çoklu nöron katmanlarında ve her katmandaki çoklu nöronlarda farklı seçilebilir. Böylelikle alışılmışın dışında ayraçlar ve matematiksel çok boyutlu karmaşık düzlemler üreterek kullanabilir.

Yapısal olarak veri girişinin yapıldığı input/giriş katmanı, verilerin yukarıda bahsedilen aktivasyon fonksiyonlarından geçirildiği nöronları sembolize eden node'ların ve bu node'ların hesaplama sonuçlarını etkileyici dış etmen/bias ve node ağırlığı/weight olarak adlandırılan katsayılardan oluşan ara/hidden katmanı ve sonuçların oluşturulduğu çıktı/output katmanı yer almaktadır. Yapay sinir ağlarında

kaç katman bulunması, katmanlarda kaç adet nöron kullanılmasının ideali hakkında belirli yaklaşımlar olduğu gibi çoğunlukla bu değerler ve hatta nöronlar içerisinde yer alan aktivasyon fonksiyonlarının çeşidi deneysel çalışmalar ile tespit edilmektedir. Aktivasyon fonksiyonları bazı kaynaklarda transfer fonksiyonları olarak adlandırılabilir. Ara/gizli katman olarak adlandırılan hidden layer'larda yer alan nöronlar birbirilerine ağırlık değerleri ve aktivasyon fonksiyonlarından elde edilen sonuçları aktarmaktadır. Temelde her bir node bir ağırlık ve aktivasyon fonksiyonundan oluşmalı, dış etmenleri sembolize eden bir "bias" değeri gerekli olması durumunda eklenebilmelidir. YSA, Yapay Sinir Ağları bahsedilen bu temel sistem sonucunda gerekli isterlere göre sistemin tasarımcısı tarafından tek bir sonuç üretebileceği gibi birden fazla sonuçta üretebilir. Çoklu üretilen sonuçlar istenildiği taktirde olasılıksal durumlarını gösteren bir başka fonksiyondan geçirilerek tahmin ve tespit işleminde kullanılabilir, aynı zamanda çoklu parametrelerin her biri bağımsız bir değere refere edecek şekilde sonuç elde edilmiş olabilir. Sistem ideal parametrik değerlerinin tespit edilmesin kullanılan yöntemler bu tarz çoklu parametre üreten sistemlerdir.

Temel bölütleri belli olan YSA'da elde edilen ve gerekli olması durumunda ön işlemlerden geçirilmiş olan veri setleri ile eğitim işlemi gerçekleştirilip daha sonrasında ideal başarı değerlerini yakalayan YSA sistemi sınıflandırma işlemlerin kullanılabilir. Eğitim işleminde kullanılan birden fazla yöntem mevcuttur. Tez konusu çalışmamızda ağımız kontrollü veri değerleri ile denetimli öğretime tabii tutulmuş, bu işlem esnasında ağ değerlerinin güncellenmesi için her işlem adımında geri besleme sistemi ile ağın ağırlık değerleri güncellenmiştir.

Denetimli eğitim sistemleri, yapay zekâ eğitimi için verilen sonuçları belli veri setlerinin eğitim işlemi sonrasında yaptıkları tahmin ve sınıflandırmalar ile karşılıklı bir eğitim sistemi oluşturmaktadır. Yapay zekanın veri ile sınıflandırma yapılması istenilen sonuç arasındaki bağlantıyı matematiksel formüller ve katsayılar ile kurabilmesini amaçlar. Her bir eğitim işlemi sonrasında sistemde meydana gelen yanlış sınıflandırma ve hataların eğitim işlemi esnasında düzeltilerek tekrar eğitime devam edilmesi prosedürüne dayanır. Bu düzeltme işlemi geri yayılım olarak adlandırılan "back-propagation" sistemidir. Eğitim aşamasında verilen setlerden elde edilen sonuçlar ile olması gereken sonuçlar arasındaki hata payı ve oranı geriye dönük olarak ağda yer alan node-düğümlerin ağırlık katsayılarında ve varsa eğer bias

değerlerinde güncellenerek bir sonraki adımda daha az veya hatasız sonuçlar alınması beklenir. Başlangıç aşamasında tüm nöron ağrılık değerleri ve bias değerleri rastgele olarak atandığından veya sıfır olarak sistem başlangıcında verildiğinden back-rpopagation işleminden sonra değerler ideal değerler olacak ve başlangıç aşamasında yapılan işlemlerin doğruluk oranı oldukça düşük olacaktır. Bu yüzden yapay zekâ ağlarının eğitimi ve başarı oranları çoklu tekrarlardan sonra netleştirilir. Başlangıç aşamasındaki değerler ile elde edilen sonuçlar sonrasındaki fark, "Residual" artık değer olarak hesaplanır. Bu hesaplama işlemi temel ve basit bir işlemdir ve Denklem 12'de paylaşılmıştır. Elde edilen değer ile kontrollü eğitim setinde yer alan beklenen değer arasındaki farkın hesaplanması ile bulunur.

$$Residual = Observed - Expected$$

(Denklem 12)

Elde edilen bu artık değer miktarınca geri besleme yöntemi ile tüm nöronların ağırlık değerleri güncellenir. Her güncelleme ve yeni tespit işlemi sonrasında yukarıda yer alan hesaplama işlemi tekrarlanır. Tek bir nöron için yapılabilecek yukarıdaki denklem çoklu nöronlar hesaba katıldığında tüm nöronların hatalarının karelerinin ortalaması her bir tekrarda alınarak genel fenomende nasıl bir iyileşme olduğu gözlemlenebilir.

$$SSR = (Observed_x - Expected_x)^2 + (Observed_y - Expected_y)^2 + (Observed_z - Expected_z)^2$$

(Denklem 13)

Denklem 13 sonucunda elde edilen değerin her bir tekrar sonrasında tekrar hesaplanmak zorunda olması anlaşılırlık açısından zor bir yöntem olsa bile iyileştirmenin yapılması gereken aşamaları "Gradient Descent" yöntemi ile SSR sonuçlarının gösterildiği eğri üzerinden saptamak ve gerçekleştirmek mümkündür. Bu yöntem SSR boyunca her bir adımda elde edilen sonuçların bir grafiğinde yer alan kıvrım noktalarında türev alınımı ile elde edilir. Türev alımı ve hesaplama işlemlerinde türevin denklemsel özellikleri kullanılır. Türev işleminde SSR çıktılarının ağırlık veya bias değerlerine göre ayrık bir şekilde alınabilmesini sağlar. Aşağıda Denklem 14'de Chain Rule formülü paylaşılmıştır.

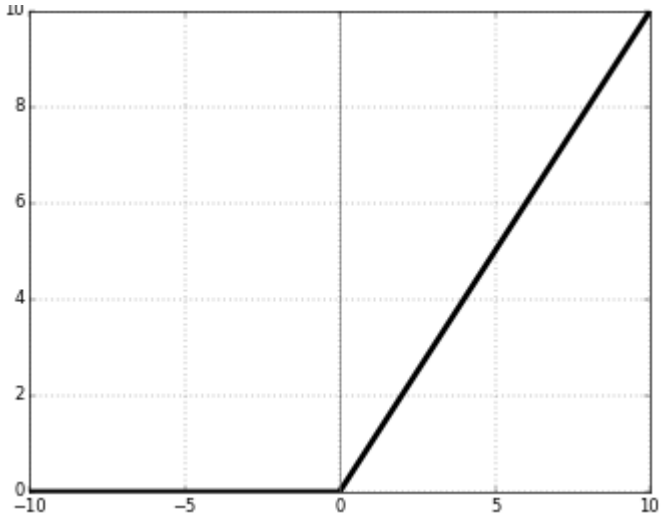
$$\frac{d_{SSR}}{d_n} = \frac{d_{SSR}}{d_{Predicted}} * \frac{d_{Predicted}}{d_{bias(n)}}$$

(Denklem 14)

Node'lar içerisinde kullanılan aktivasyon veya transfer fonksiyonlarına örnek olarak ReLU-Rectified Linear Unit, Sigmoid, TanH, Argmax ve Softmax gibi fonksiyonlar sıkça kullanılmaktadır ancak sınıflandırma yapılması gereken işlem ve eğitimde kullanılacak veri setinin uygunluğuna göre bu fonksiyonlar değişebilir. Node'lar kullanılan bu fonksiyonlar tek bir ara katmanda olabileceği gibi birden fazla ara katmanlarda bu aktivasyon fonksiyonları kullanabilir. Benzer bir şekilde her katmanda aynı aktivasyon fonksiyonları kullanabileceğimiz gibi, aynı katmanda yer alan nöronlarda farklı aktivasyon fonksiyonlarını da kullanabiliriz. Aktivasyon fonksiyonlarından en temel olanı ReLU kullanımı ve içeriğini oluşturan fonksiyon sebebi ile girdi olarak gelen değerler içerisinde max değerini bulur. Diğer yöntemlerden farklı olarak fonksiyonun koordinat düzlemindeki görüntüsü bir step fonksiyonu andırır ve doğrusal artış grafiğine benzer, önceki bölümlerden bahsedilen kıvrımlı eğrilere benzememektedir. ReLU yöntemi yukarıda bahsedilen backpropagation yöntemlerindeki gibi Gradient Descent yönteminde Chain Rule uygulanarak kıvrımlı bölgelerde türev hesaplaması yapılamamakta ancak fenomenin değiştiği keskin dönüm noktalarında bu işlem yapılabilmektedir. Ancak ağ içerisinde birden fazla katman ve katmanlarda çoklu nöronlar yer alacağından bu durum çok önemli bir sorun olarak karşımıza çıkmamaktadır. Aşağıda Denklem 15'de ReLU formülü yer almaktadır. Şekil 14'de ReLU görseli paylaşılmıştır.

$$Func(x) = \max(0, x) = y\ düzlemi\ değeri$$

(Denklem 15)

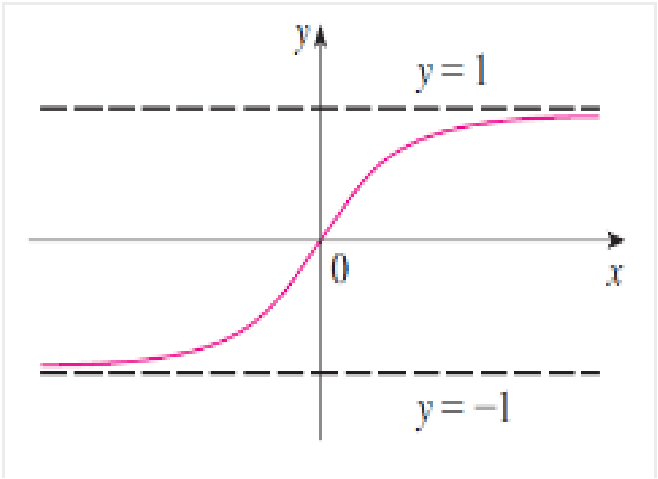


Şekil 14 ReLU görseli

TanH fonksiyonu hiperbolik tanjant fonksiyonu olarak adlandırılmaktadır. Girdi olarak verilen değerin hiperbolik tanjant değerini hesaplar, formulü aşağıdaki Denklem 16 gibidir. Fonksiyon görselinde de anlaşılacağı gibi Sigmoid'den farklı Y değerinin 0 ila 1 arasında değil +1 ve -1 değeleri arasında sınırlandırılmasıdır.

$$TanH(arg) = \frac{\sinh(arg)}{\cosh(arg)} = y\ düzlemi\ değeri$$

(Denklem 16)



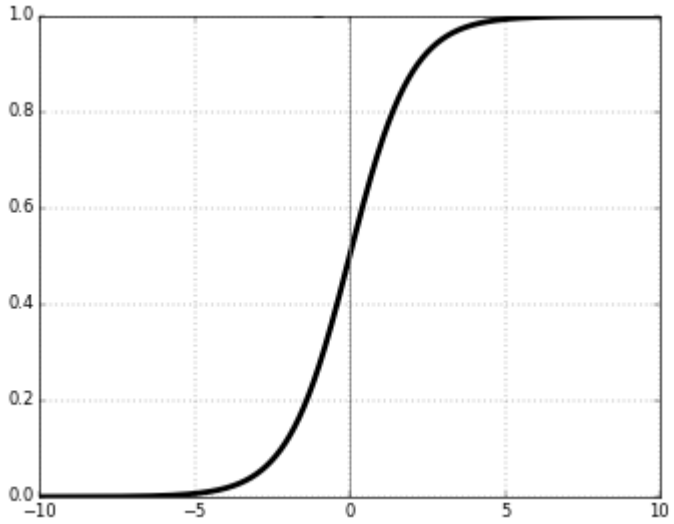
Şekil 15 TanH fonksiyonu görseli

Sigmoid aktivasyon fonksiyonu, doğrusal olmayan bir denklemdir. Doğrusal olmadığı için yani bir step fonksiyon gibi fenomen içermediğinden gradyan hesaplamalarına ve türev hesaplamalarına daha uygundur. Aşağıdaki Şekil 16'da anlaşılacağı gibi girdilere karşılık elde edilecek sonuçları 0 ila 1 arasında tutar ve böylelikle minimum ve maksimum noktalarımızdan ve bağıntılı olan nöron ağırlık

değerlerimizin çok yüksek değerlere gitmeyeceğinden emin olmuş oluruz. Ancak fonksiyonun görselinden de görebileceğiniz gibi 0 değerine bir yakınsama göze çarpmaktadır. Geri besleme ve ağ eğitimi esnasında 0 değerleri alınması halinde performans kayıpları gözlenebilir. Sigmoid fonksiyonu Denklem 16'da paylaşılmıştır.

$$S(x) = \frac{1}{1 + e^{-x}}$$

(Denklem 16)



Şekil 16 Sigmoid fonksiyonu görseli

Argmax fonksiyonu ağın output/çıktı katmanında yer alan fonksiyonlardan biridir. Hidden/ara katmandan gelen girdi değerlerinin en büyüğünü bir "1" değerine, diğer değerleri ise sıfır "0" 'a eşitler. Sıfıra eşitlediği alanlarda gradyan değerleri üzerinden geri besleme ile ağ eğitimi ve ağırlık değerlerinin güncellemesi sıfır ile çarğımından tüm değerlerin sıfır geleceğinden yapılamaz. Aşağıdaki Denklem 17'de ilgili formül paylaşılmıştır.

$$\frac{dLossFunc}{dParametreler} = \frac{dLossFunc}{dArgMax} * \frac{dArgMax}{dFinalOutput}$$

(Denklem 17)

Kırmızı ile renklendirilmiş alan gradyan hesaplamalarında türev alımı ile elde edilen alandır. Bu alan argmax değerinden dönecek olan 0 değeri ile tüm işlem sonucunun 0 olmasına sebebiyet verir.

Softmax fonksiyonu ağın çıktı/output katmanında yer alan fonksiyonlardan biridir. Argmax fonksiyonundan farkı, çıktı olarak girdilerin hepsinden sadece 1 veya 0 üretmez. Çoklu girdi değerleri için çoklu olasılık tahminleri üretir. Temel olarak yapmakta olduğu işlem tüm girdileri ve çıktıları birbirilerine oranlamak ve 0-1 arası değerleri ilgili girdilerin karşılığına atamaktır. Girdi değer ne kadar büyük olursa olsun farketmeksizin bu işlemi gerçekleştirir. Softmax sonucunda üretilen 0-1 arassı çoklu değerlerin toplamının 1'e eşit olması gereklidir ve elde edilen sonuçlar "predicted possibilities", tahmini olasılıklar olarak adlandırılır. Sadece 1 ve 0 değeri üretmediğinden çıktı kısmında elde edilen sonuçlar geri besleme işlemlerinde kullanılabilir. Denklem 18'de Softmax fonksiyonu paylaşılmıştır.

$$Softmax = \frac{e^{OutputValue}}{\sum_{j=1}^{k} e^{OutputValue}} = \frac{e^{x}}{e^{x} + e^{y} + e^{z}}$$

(Denklem 18)

Yukarıda bahsedilen aktivasyon fonksiyonları ve çıktı katmanında kullanılabilecek fonksiyonlar ile ağın kurulumu tamamlanır. Yapay zekâ ağı denetimli, denetimsiz (derin öğrenme algoritmalarında ve çok büyük veri setlerinde kullanılır) ve hibrid eğitim modellerine göre eğitimi sağlanır. Eğitim işlemi her bir tahmin işleminden sonra elde edilen çıktılar ile ağın geri beslemesi ile gerçekleştirilebilir. Geri besleme işleminde kullanılabilecek yöntemlerden bir tanesi bölümün ilk kısımlarında bahsettiğimiz SSR- Sum of Squarred Residuals değerinin hesaplanmasıdır. Diğer bir yöntem node'ların "**Cross Entrophy**" değerinin hesaplanması ve tekrardan türev bazlı gradyan hesaplaması ile geri besleme ağının değerlerinin güncellenmesidir. Denklem 19'da Cross Entrophy formülü paylaşılmıştır.

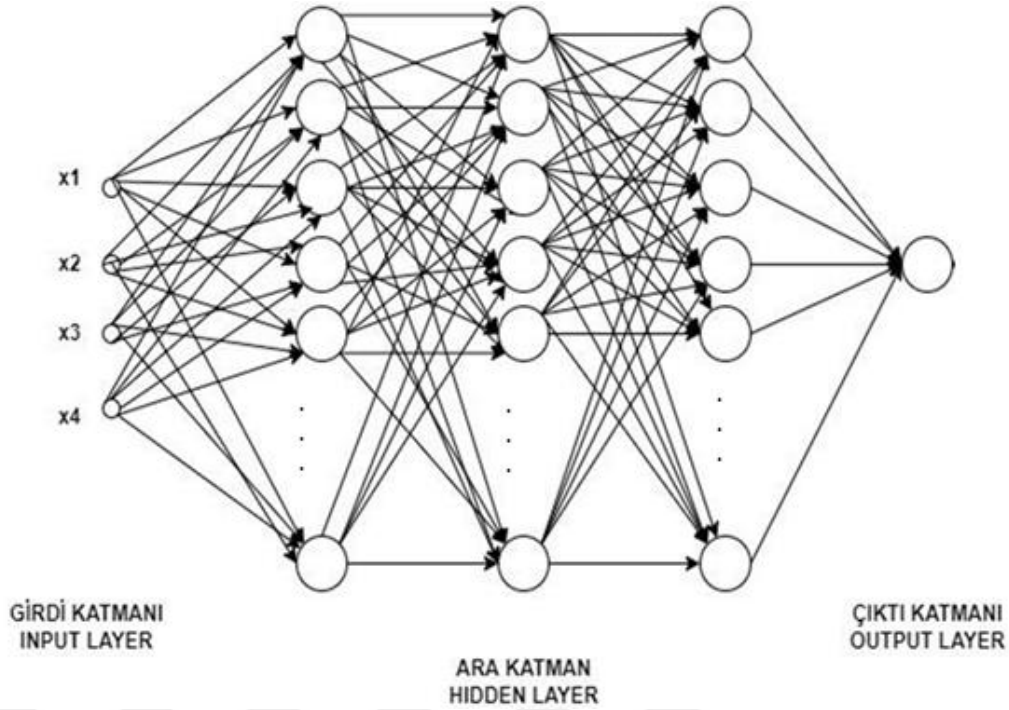
$$CrossEntrophy = -\log(Predicted\ Probability)$$

(Denklem 19)

Cross Entropy işlemi SSR'dan farklı olarak logaritmik tabanda işlem yaptığından ve türev hesaplamalarına daha uygun olduğundan kullanılacak yöntemlerin ve veri setlerinin içeriğine göre karşmaşık işlemlerde daha tercih edilebilir olmaktadır.

Doktora tez çalışmamızda artık bit veri setinden bir desen tahmin edebilmek için yapay sinir ağı tasarlanmıştır. Tasarım esnasında bu alanda literatürde

gözlemlenen kısıtlı çalışmalarda yapılan ön hazırlıklar ve bilgilendirmeler göz önüne alınarak çalışmalarda yer alan sinir ağlarına benzer bir ağ tasarımına gidilmiştir. İşlem için bir giriş ve sonuç katmanının yanı sıra birden fazla ara katman kullanılmıştır. Kullanılan ara katmanlarda 200 nöron kullanışmıştır. Eğitim veri setleri diğer makine öğrenmesi metotlarından farklı olarak gönderilmek istenilen veri, polarizasyon filtresi değeri ve oluşan QBit kullanılarak eğitim yapılmıştır. Eğitim sonucunda alıcı tarafında seçilen rastgele polarizasyon filtre değerleri ve QBit değerleri kullanılarak üretici kısımdaki seçilen bit'ler tahmin edilmeye çalışılmıştır. Bu işlemlere uygun olarak tüm katmanlarda yer alan aktivasyon fonksiyonları test edilmiştir. Katmanlarda sırası ile "Sigmoid", "Relu", "elu", "tanh" ve "Softmax" aktivasyon fonksiyonları denenmiştir. Elde edilen sonuçlar ve ağ katmanlarındaki uygunlukları sonuçlar üzerinden kontrol edmiştir. Girdi katmanı ve ara katmanlarda tanh aktivasyon fonksiyonu kullanılmıştır. Ara katmanların son seviyesinde Sigmoid aktivasyon fonksiyonu kullanılıp elde edilen değerler çıktı katmanında Softmax aktivasyon fonksiyonu kullanılıp 0 ile 1 arası sonuç değerleri elde edilmiştir. Elde edilen sonuçlar ortalama değerin üstünde seyir gösterdiklerinde 1 altında değer gösterdiklerinde ise 0 olarak final sonucu atanıp foton üreticisi olan tarafın bit'leri tahmin edilmeye çalışılmıştır. Eğitim işleminde tekrar sayısı "epoch" olarak 10, 100 ve 1000 tekrarlı değerler uygun görülmüştür. Geri besleme ile eğitimin güncellenmesi işlemi esnasında tahmin edilen değerler ve elde edilen sonuçlar arasındaki fark öğrenme oranı katsayısı ile çarpılarak elde edilen sonucun tüm ağırlık değerlerinden çıkarılması ile yapılmıştır. Aşağıda Şekil 17'de işlemler için tasarlanmış farklı yapay sinir ağı modellerini aşağıdaki gibidir.



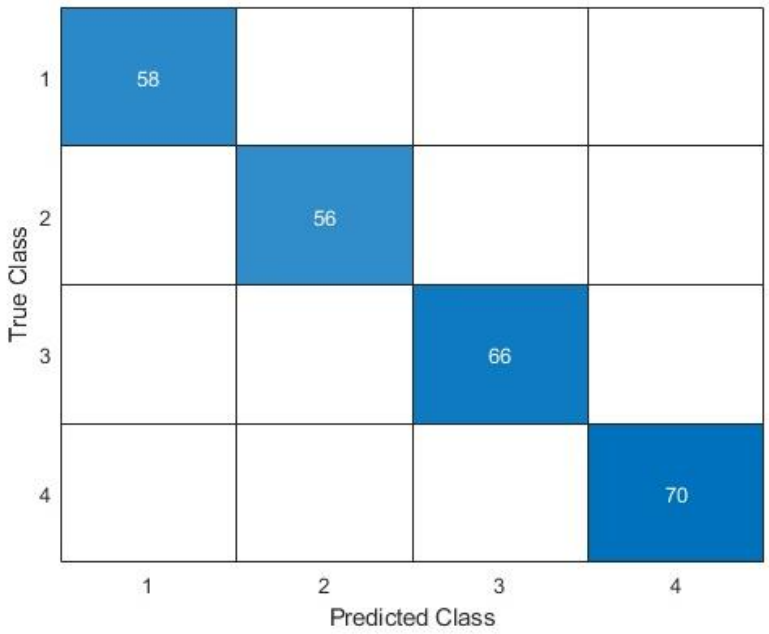
Şekil 17 YSA tasarımı

H. Test ve Sonuçlar

1. kNN Sonuçları

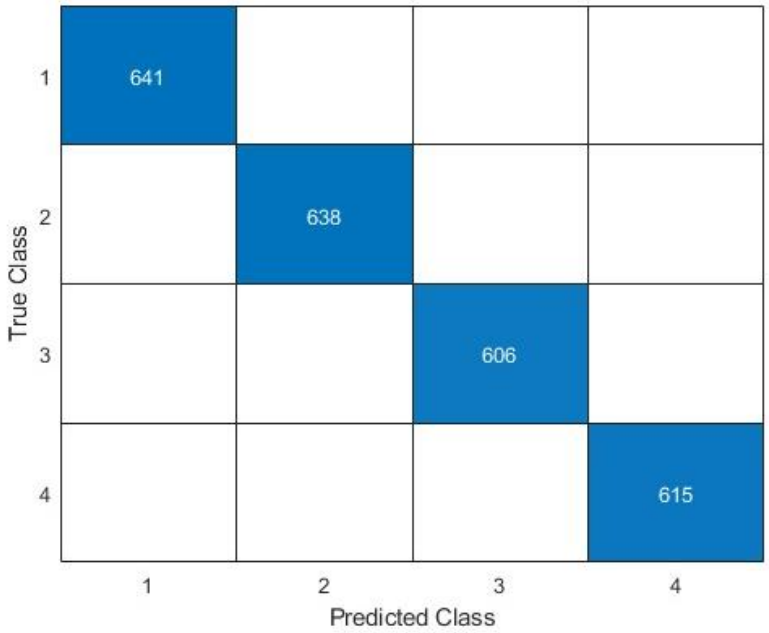
Şekil 18-21 arası paylaşılan görsellerde kNN algoritmasının Chebychev mesafe ölçüm fonksiyonu ile alınmış sonuçları bulunmaktadır. Her bir sonuç farklı oranlarda eğitim ve test verisi içermekte ve aynı zamanda farklı veri seti kullanılarak yapılmaktadır.

Şekil 18'de 1000 uzunluğunda bir veri setinde %25'i test verisi olmak üzere %75'lik bir oranda eğitim verisi kullanılarak elde edilen sonuçlar yer almaktadır.



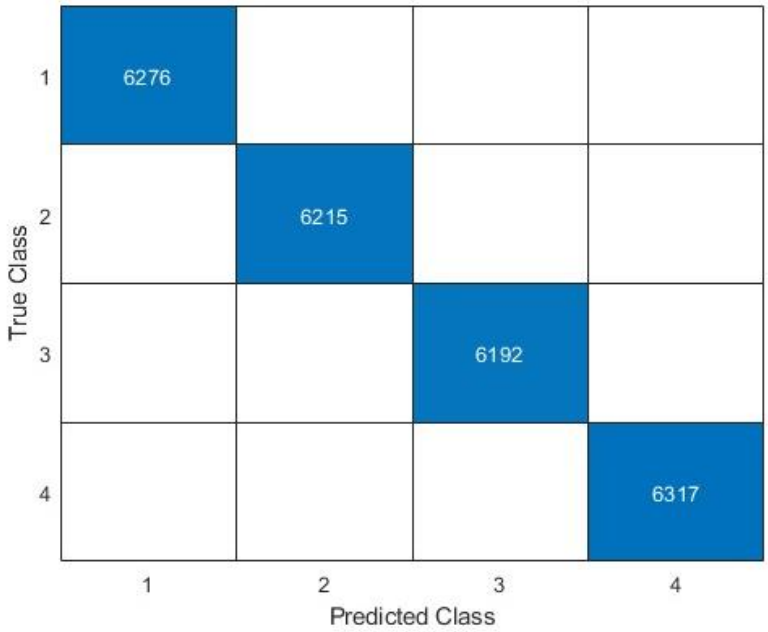
Şekil 18 1K Chebychev sonuçları

Şekil 33'de Chebychev mesafe ölçüm fonksiyonu kullanılarak, 10000 uzunluğunda bir veri setinde %25'i test verisi olmak üzere %75'lik bir oranda eğitim verisi kullanılarak elde edilen sonuçlar yer almaktadır.



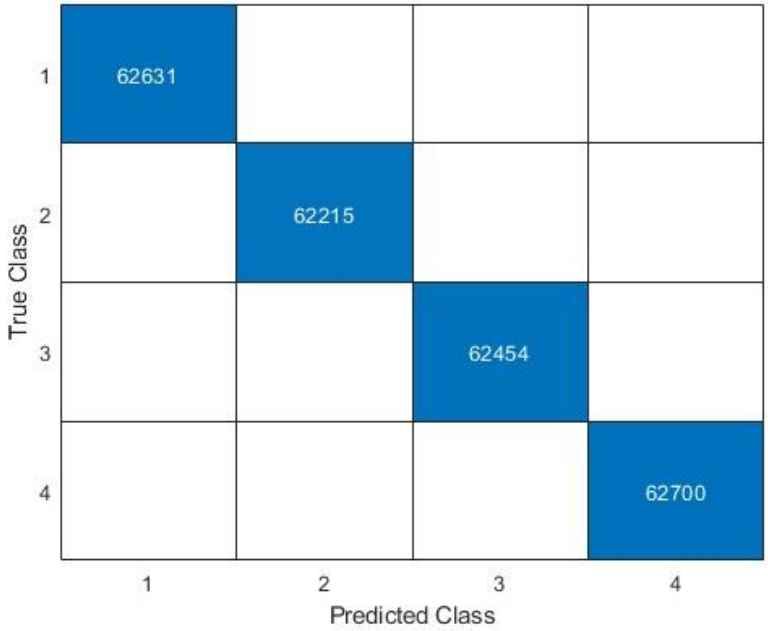
Şekil 19 10K Chebychev sonuçları

Şekil 20'de Chebychev mesafe ölçüm fonksiyonu kullanılarak, 100000 uzunluğunda bir veri setinde %25'i test verisi olmak üzere %75'lik bir oranda eğitim verisi kullanılarak elde edilen sonuçlar yer almaktadır.



Şekil 20 100K Chebychev sonuçları

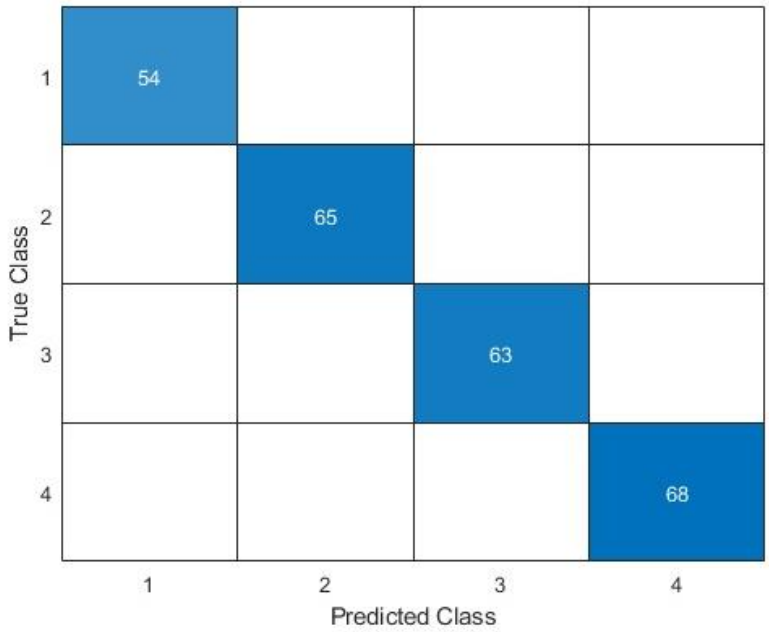
Şekil 21'de Chebychev mesafe ölçüm fonksiyonu kullanılarak, 1000000 uzunluğunda bir veri setinde %25'i test verisi olmak üzere %75'lik bir oranda eğitim verisi kullanılarak elde edilen sonuçlar yer almaktadır.



Şekil 21 1M Chebychev sonuçları

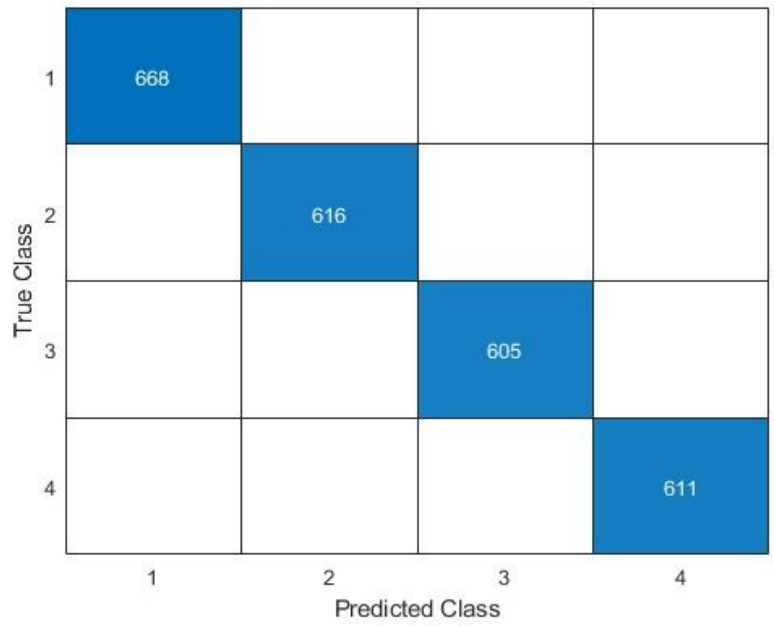
Şekil 22-25 arası paylaşılan görsellerde kNN algoritmasının CityBlock mesafe ölçüm fonksiyonu ile alınmış sonuçları bulunmaktadır. Her bir sonuç farklı oranlarda eğitim ve test verisi içermekte ve aynı zamanda farklı veri seti kullanılarak yapılmaktadır.

Şekil 22'da hesap edilecek değerin küme bloğuna uzaklığını ölçmede kullanılan CityBlock algoritması ile yapılan test sonucu yer almaktadır. Bu sonuç 1000 uzunluğunda veri barındırmaktadır. Veri bloğunun %75'lik bir kısmı eğitim için %25'lik bir kısmı test işlemi için kullanılmaktadır.



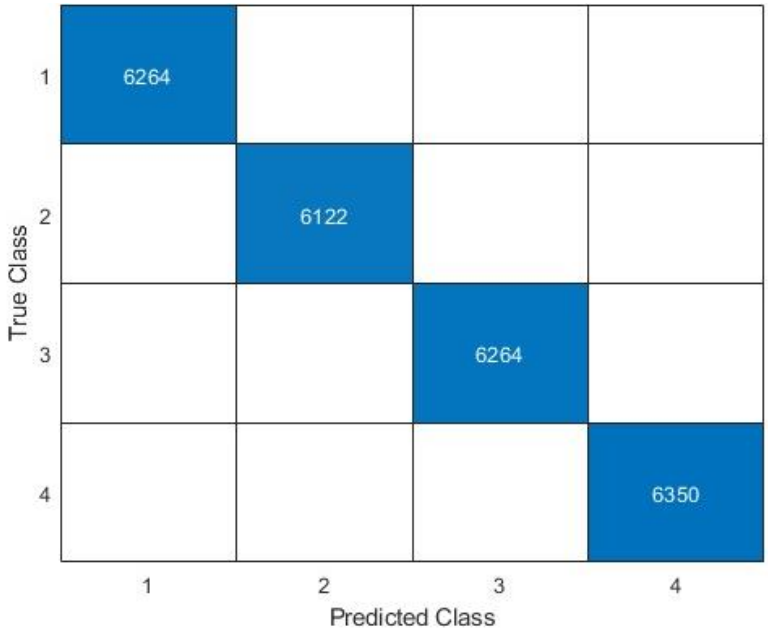
Şekil 22 1K CityBlock sonuçları

Şekil 23'de mesafe ölçüm işlemi için CityBlock fonksiyonu 10000 uzunluğunda bir veri bloğu için kullanılmıştır. Ağın eğitimi ve test işlemleri için %75'e %25'lik bir oranda veri tercih edilmiştir.



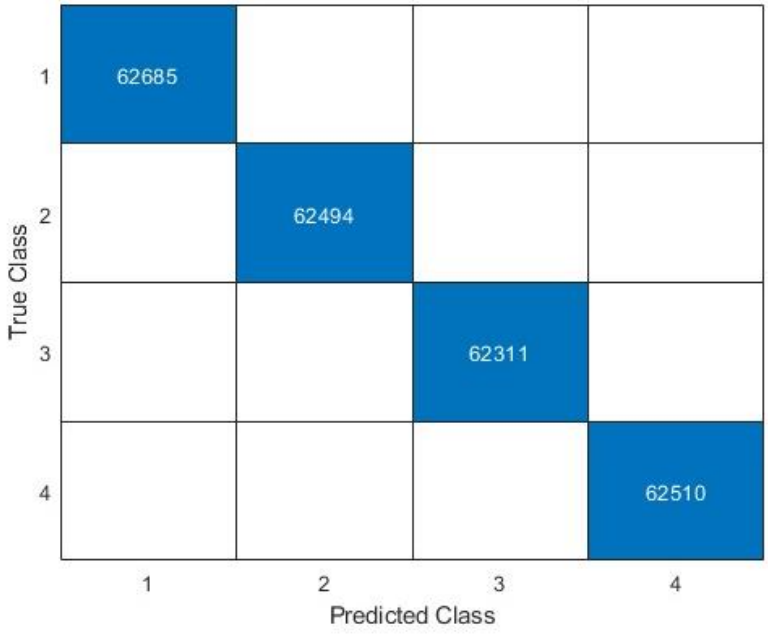
Şekil 23 10K CityBlock sonuçları

Şekil 24'de 100000 uzunluğunda bir veri bloğu CityBlock mesafe ölçüm fonksiyonu kullanılarak test edilmiştir. Eğitim ve test işlemleri için %75'e %25'lik bir oran tercih edilmiştir.



Şekil 24 100K CiyBlock sonuçları

Resim 25'de mesafe ölçüm fonksiyonu olarak CityBlock fonksiyonu kullanılmış olup 1 milyon uzunluğunda bir veri bloğu eğitim ve test işlemlerinde kullanılmıştır.

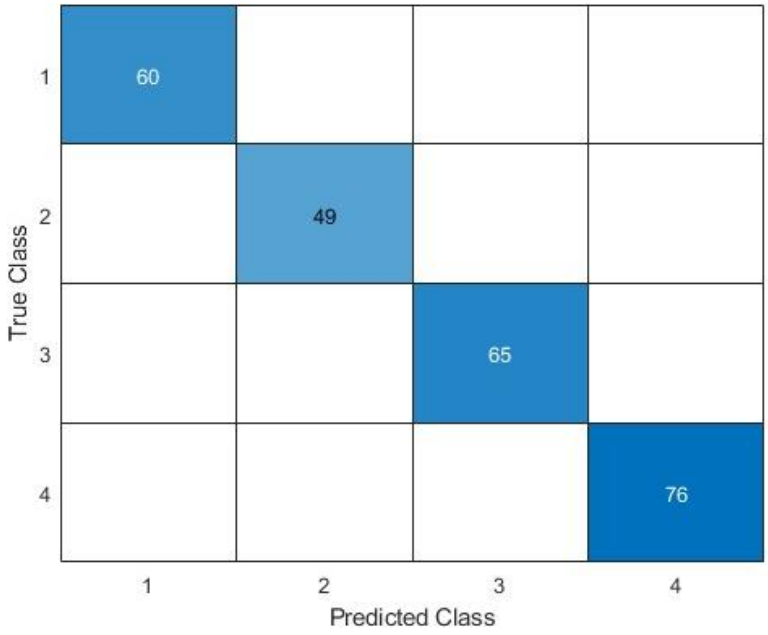


Şekil 25 1M CityBlock sonuçları

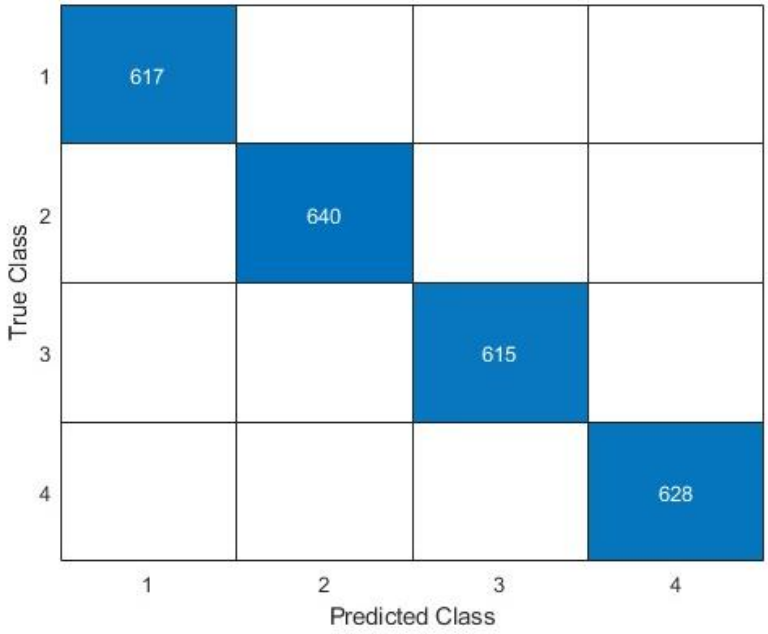
Resim 26-29 arası paylaşılan görsellerde Euclidean mesafe ölçüm fonksiyonu farklı uzunluklardaki veri bloklarında kullanılarak kNN algoritmasının

performansına olan etkisi ölçülmek istenilmiştir. Eğitim ve test işlemleri için %75 eğitim %25 test verisi oranı belirlenmiştir.

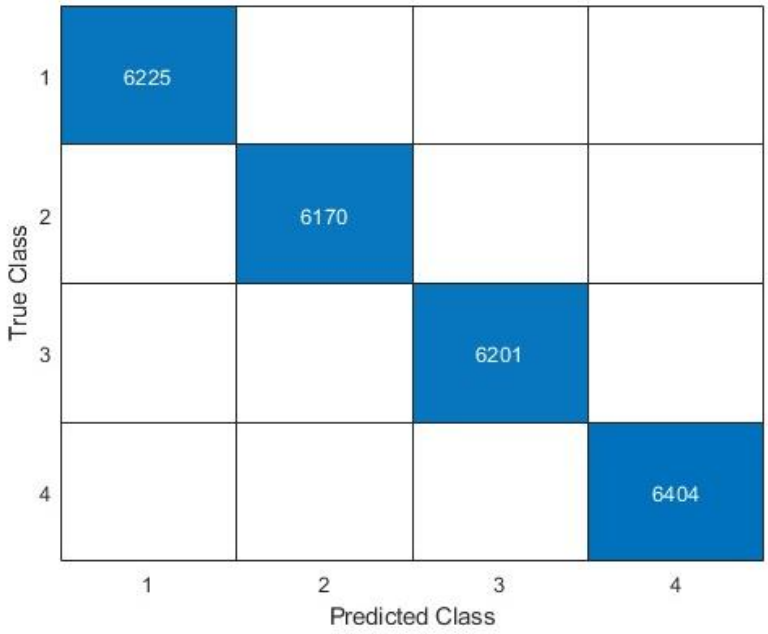
Resim 26'da yer alan sonuçlarda 1000 uzunluğunda bir veri setinde çalışmalar yapılmış, elde edilen sonuçlar confusion matrix şemasında gösterilmiştir. Resim 27'de benzer işlemler 10.000 veri uzunluğunda bir veri setinde denenmiş ve sonuçları gösterilmiştir. Resim 28 ve 29'te 100.000 ve 1.000.000 uzunluğunda veri setleri kullanılarak eğitim ve test işlemleri yukarıda bahsedilen oranlara yapılmış ve sonuçları gösterilmiştir.



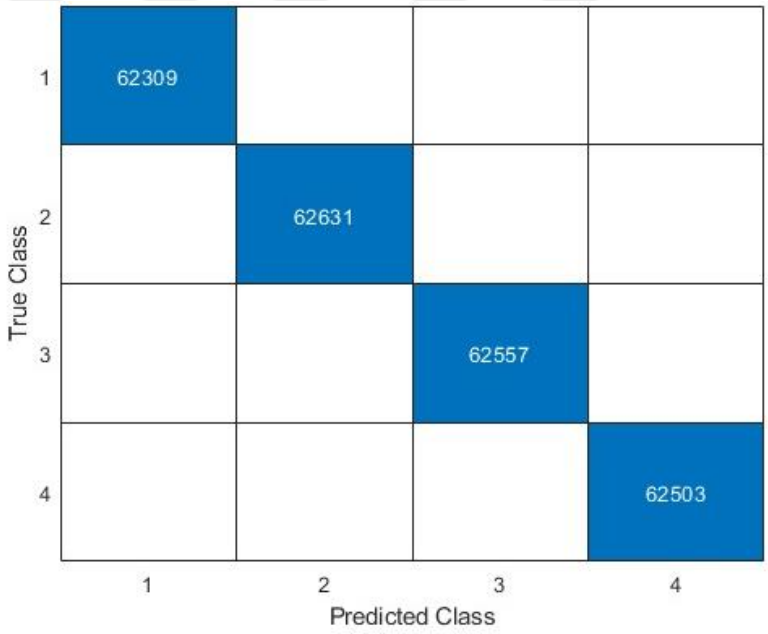
Şekil 26 1K Euclidean sonuçları



Şekil 27 10K Euclideean sonuçları



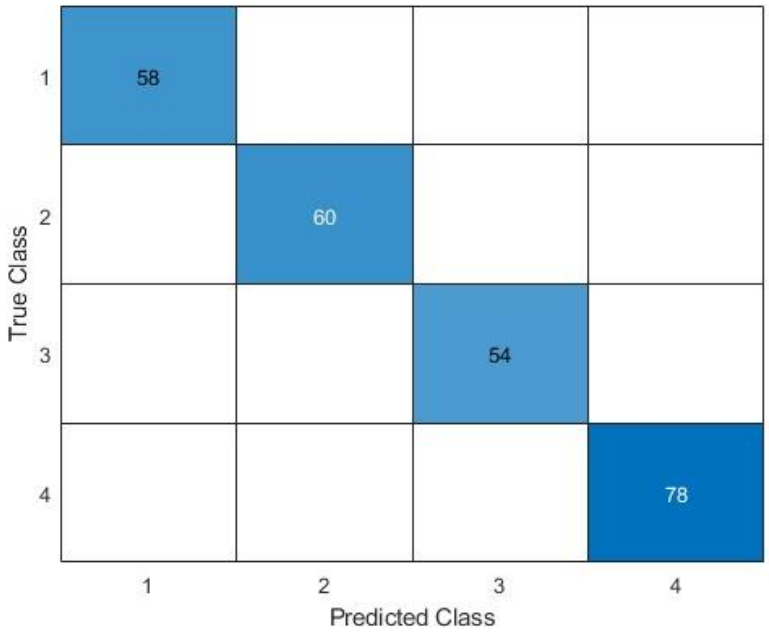
Şekil 28 100K Euclidean sonuçları



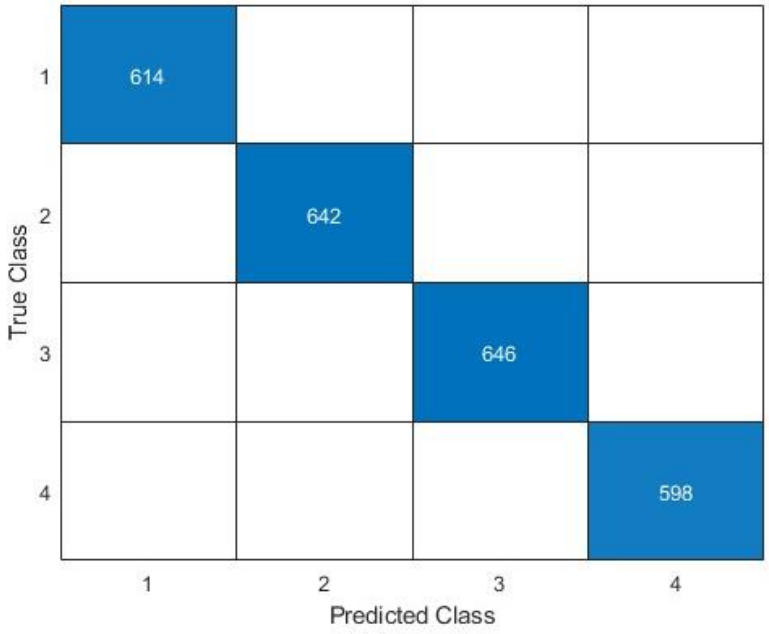
Şekil 29 1M Euclidean sonuçları

Şekil 30-33'de paylaşılan kNN algoritmasının mesafe hesaplama alt fonksiyonlarından Hamming mesafe ölçüm sistemi kullanılarak elde edilen sonuçlar yer almaktadır. Yapılmak istenilen işlem kNN algoritmasının eğitim işlemleri esnasında mesafe ölçümü için hamming fonksiyonunun kullanılması ve kullanılan fonksiyonun kNN algoritmasının sonuçlarına olan etkisi gözlemlenmek istenmiştir. Farklı uzunlukta veri blokları kullanılarak algoritmanın tahmin başarısında meydana gelebilecek değişimlerin test edilmesi amaçlanmıştır. Tüm veri uzunluklarında kNN eğitimi için veri bloğunun %75'i ayrılmış kalan kısım ise test için kullanılmıştır.

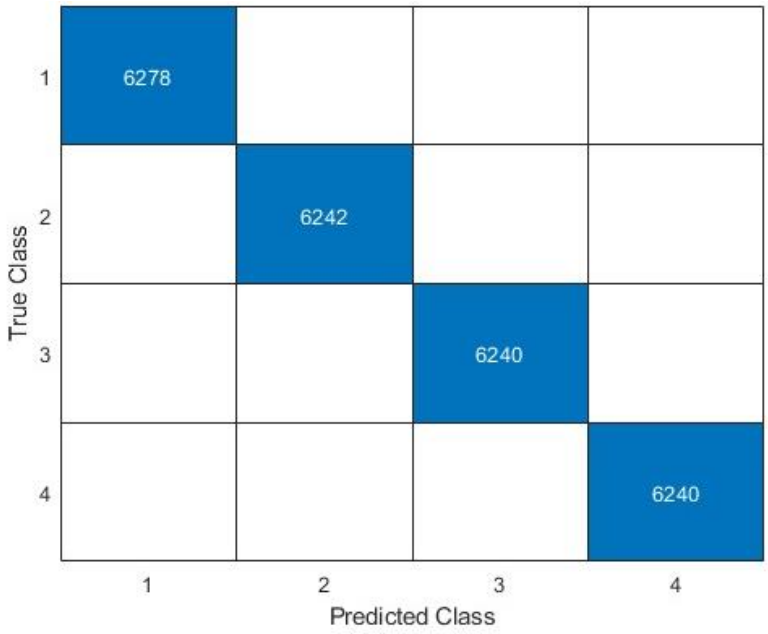
Sırası ile Şekil 30'dan başlayarak Şekil 31, 32 ve 33'de 1.000, 10.000, 100.000 ve 1.000.000 uzunluğunda veri blokları kullanılmıştır. Elde edilen sonuçlar aşağıdaki gibidir.



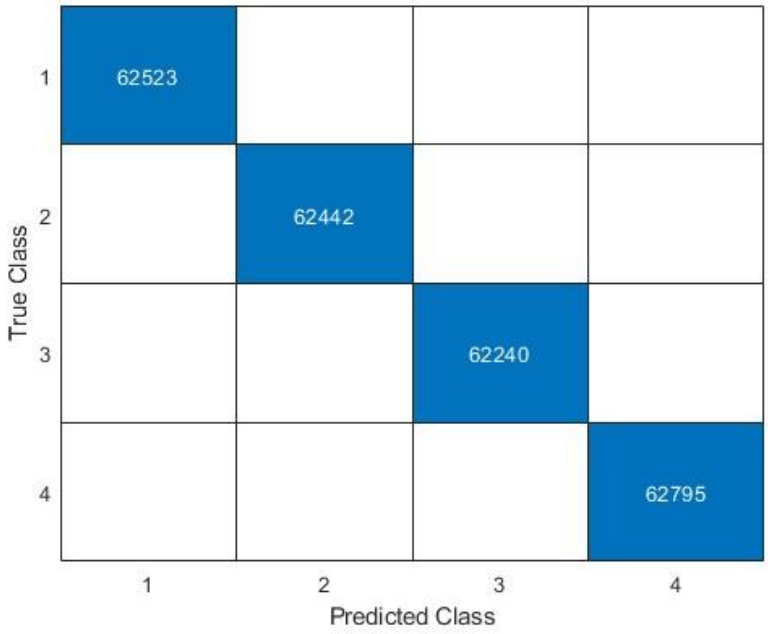
Şekil 30 1K Hamming sonuçları



Şekil 31 10K Hamming sonuçları



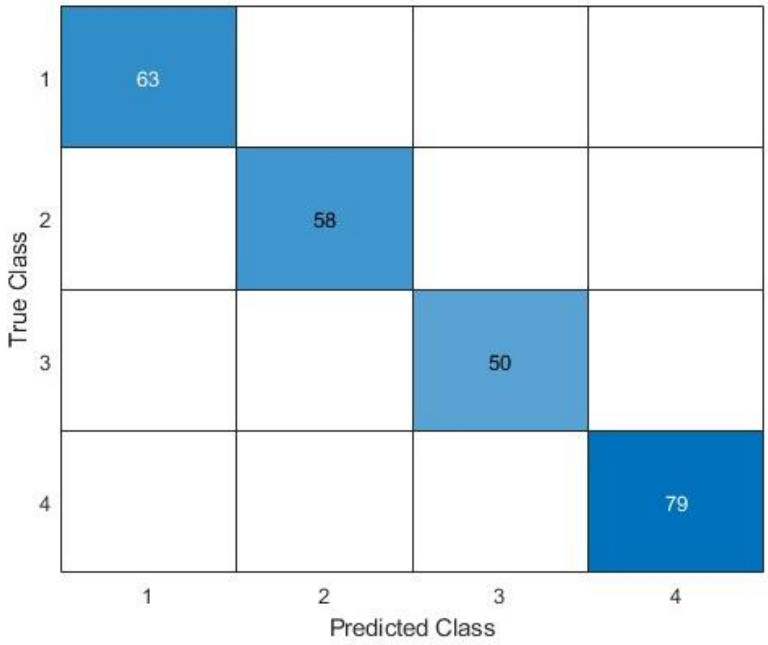
Şekil 32 100K Hamming sonuçları



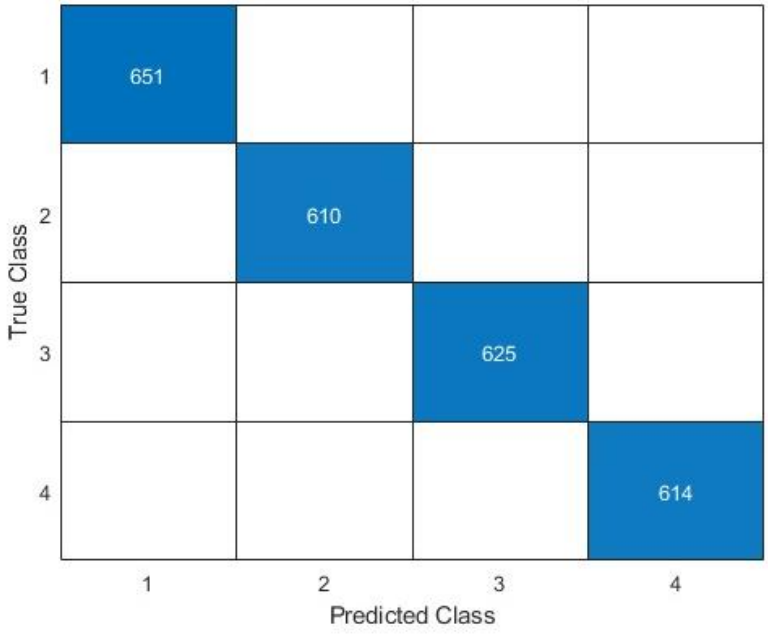
Şekil 33 1M Hamming sonuçları

Şekil 34-37'de paylaşılan görsellerde kNN algoritmasının kullanıdığı mesafe fonksiyonlarından biri olan Jaccard mesafe ölçüm fonksiyonu sonuçları yer almaktadır. Temel amacımız diğer mesafe ölçüm fonksiyonlarında olduğu gibi kNN metotunda mesafe ölçüm fonksiyonlarının kendisinin ve farklı uzunluklarda veri blokları kullanılarak eğitilmesi ile meydana gelebilecek farklılıkları gözlemlemektir. Bu amaç doğrultusunda Şekil 34-37'de sırası ile 1000, 10.000, 100.000 ve 1.000.000 uzunluğunda veri blokları kullanılmıştır. Tüm veri bloklarının %75'i eğitim %25'i

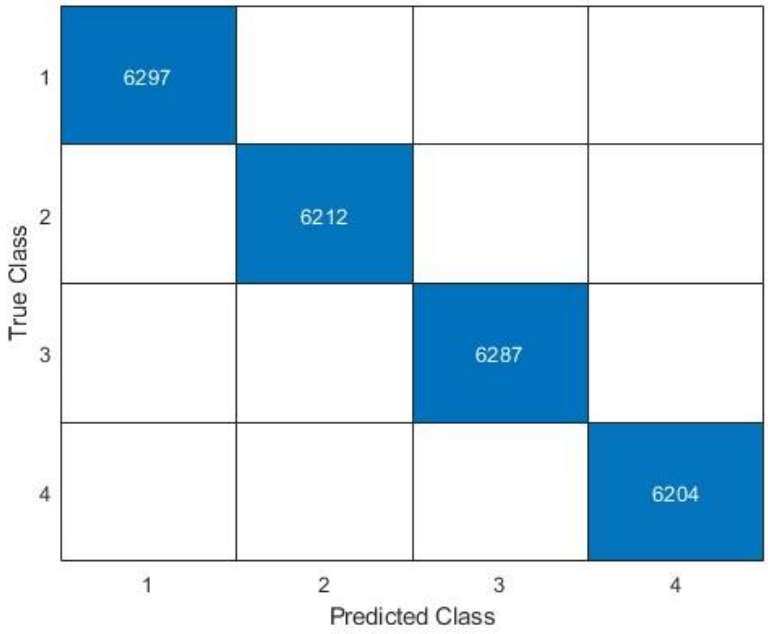
test işlemleri için ayrılmıştır. Sonuçları confusion matrix türünde aşağıdaki gibi gösterilmektedir.



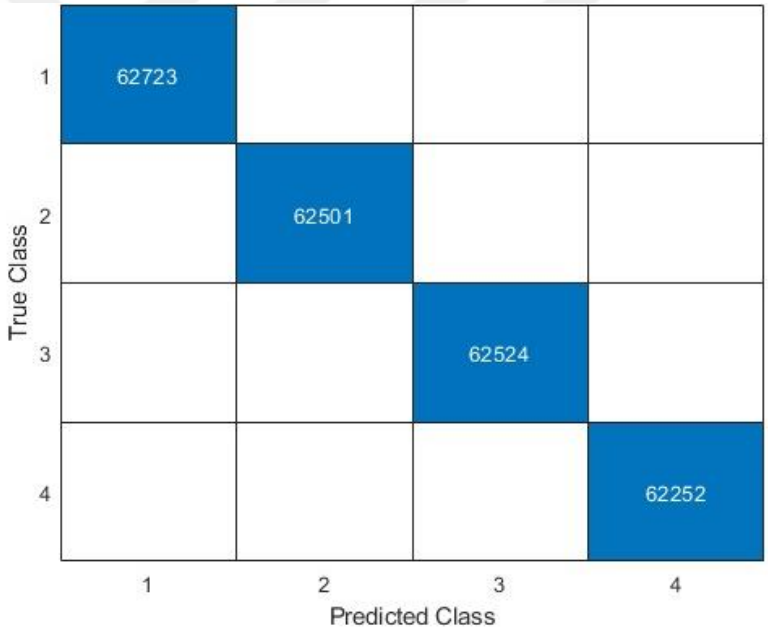
Şekil 34 1K Jaccard sonuçları



Şekil 35 10K Jaccard sonuçları

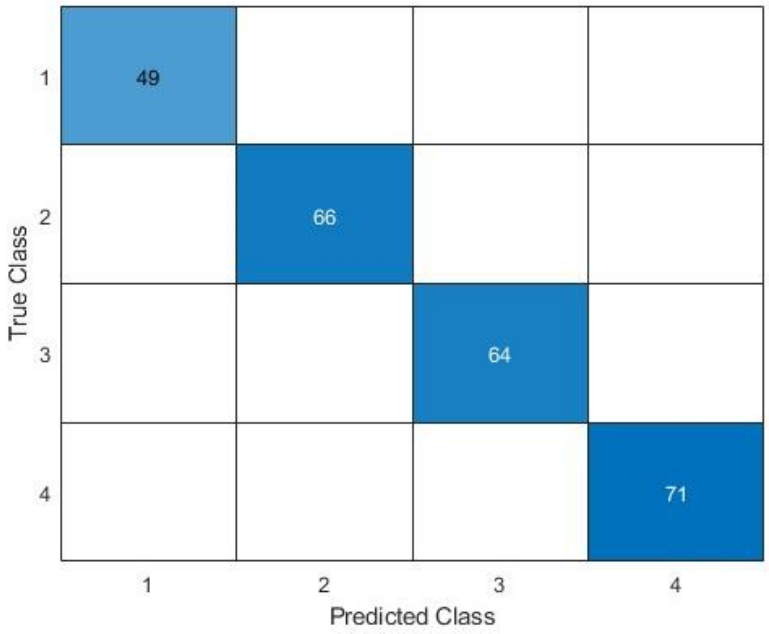


Şekil 36 100K Jaccard sonuçları

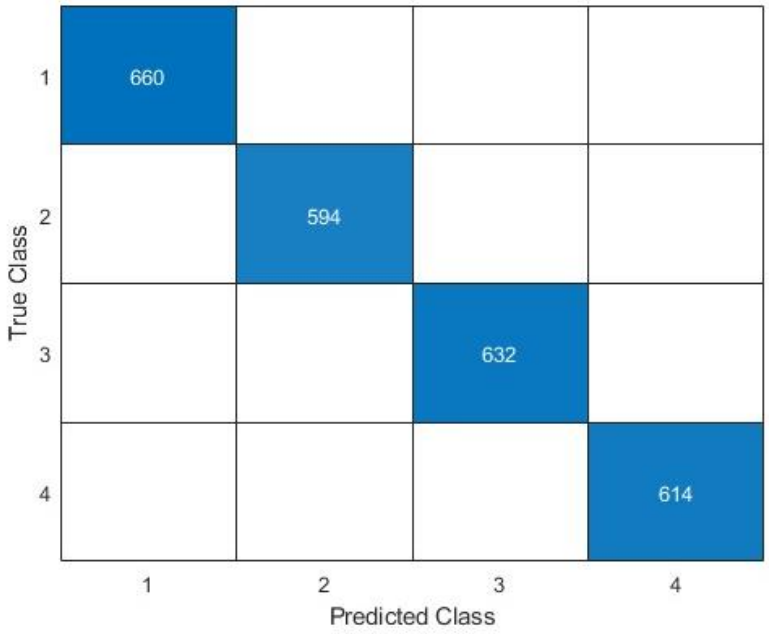


Şekil 37 1M Jaccard sonuçları

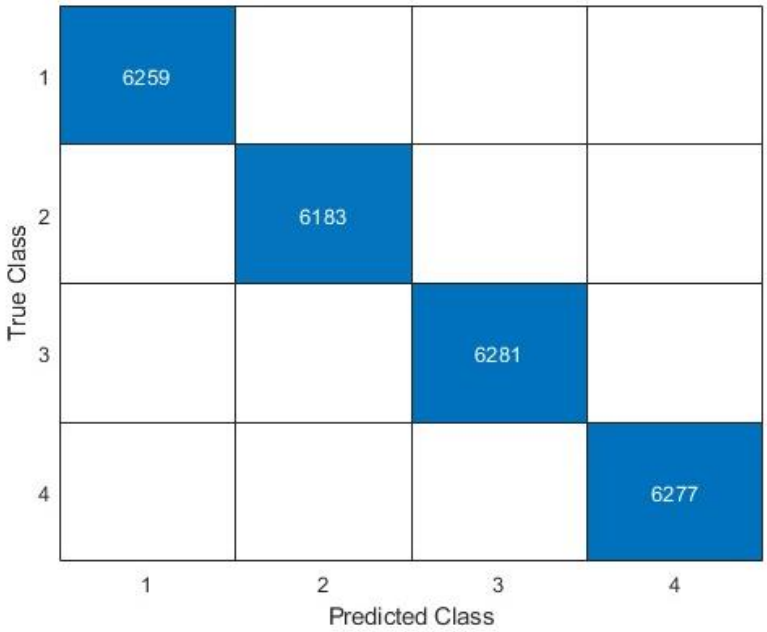
Şekil 38-41 arası görsellerde kNN algoritmasının eğitim işlemlerinde sEuclidean mesafe ölçüm fonksiyonu kullanılarak elde edilen tahmin sonuçları yer almaktadır. Tüm eğitim ve test işlemleri için farklı uzunluklarda veri blokları kullanılmıştır. Eğitim işlemleri için her bir veri bloğunun %75'i, test işlemleri için %25'i kullanılmıştır. Şekil 38-41 arası görsellerde sırası ile 1.000, 10.000, 100.000 ve 1.000.000 uzunluğunda veri blokları kullanılarak elde edilen tahmin sonuçları confusion matrix şeklinde aşağıda gösterilmiştir.



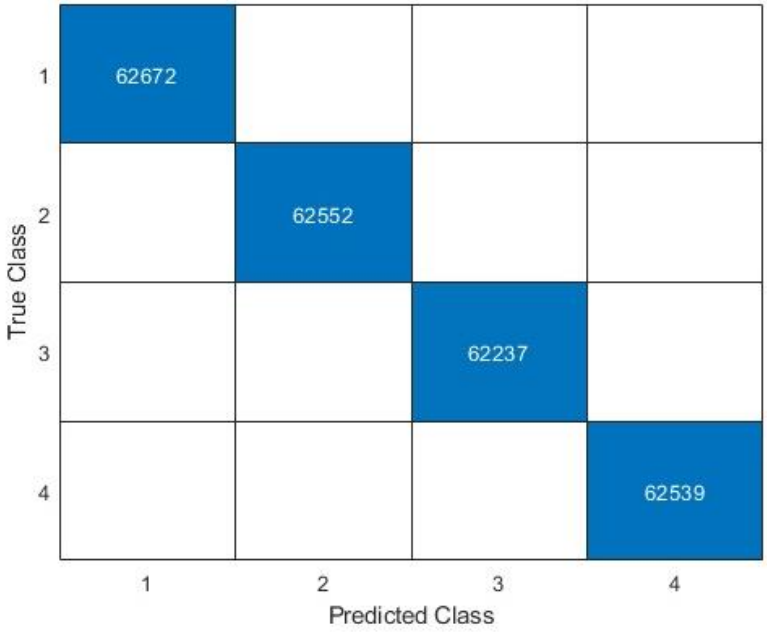
Şekil 38 1K sEuclidean sonuçları



Şekil 39 10K sEuclidean sonuçları



Şekil 40 100K sEuclidean sonuçları



Şekil 41 1M sEuclidean sonuçları

2. Naïve Bayes Sonuçları

Aşağıdaki tablolarda Naive Bayes yönteminin farklı fonksiyonlarının farklı uzunlukta veri blokları ile birlikte kullanılması ile elde edilebilecek sonuçları yer almaktadır. Buna ek olarak farklı uzunluklardaki veriler farklı oranlarda Naive Bayes yönteminin eğitim ve test işlemlerinde kullanılarak, oransal bu değişimlerin genel sonuca yapacağı etkiler gözlemlenmek istenmiştir. Elde edilen sonuçlar doğru tahminlerin tüm test verisine oranı ile gösterilmiştir. Çizelge 3'den Çizelge 6'ya

kadar sırası ile Naive Bayes algoritmasının distribution fonksiyonları olan Kernel, MN, MN non-Negative ve MVMN algoritmasının sonuçları yer almaktadır.

Çizelge 3 Naive Bayes kernel distribution sonucu

BIT Uzunluğu	TEST Uzunluğu	Doğru	Yanlış	Oran
1024 Bit- %75	256	164	92	%64
1024 Bit- %90	102	46	56	%45
10.000 Bit- %75	2500	1252	1248	%50
10.000 Bit- %90	1000	518	482	%52
100.000 Bit- %75	25.000	12.518	12.482	%50
100.000 Bit- %90	10.000	5067	4933	%50
1.000.000 Bit- %75	250.000	187.196	62.804	%75
1.000.000 Bit- %90	100.000	50.014	49986	%50

Çizelge 4 Naive Bayes MN distribution sonucu

BIT Uzunluğu	TEST Uzunluğu	Doğru	Yanlış	Oran
1024 Bit- %75	256	129	127	%50
1024 Bit- %90	102	54	28	%53
10.000 Bit- %75	2500	1236	1264	%49
10.000 Bit- %90	1000	526	474	%52,5
100.000 Bit- %75	25.000	12521	12479	%50
100.000 Bit- %90	10.000	5048	4952	%50
1.000.000 Bit- %75	250.000	125178	124822	%50
1.000.000 Bit- %90	100.000	50018	49982	%50

Çizelge 5 Naive Bayes MN-Non negative sonucu

BIT Uzunluğu	TEST Uzunluğu	Doğru	Yanlış	Oran
1024 Bit- %75	256	99	157	%37,8
1024 Bit- %90	102	34	68	%33,3
10.000 Bit- %75	2500	1294	1206	%51,7

Çizelge 5 … Devam

10.000 Bit- %90	1000	518	482	%51,8
100.000 Bit- %75	25.000	12562	12438	%50,25
100.000 Bit- %90	10.000	4997	5003	%49,9
1.000.000 Bit- %75	250.000	124850	125150	%49,9
1.000.000 Bit- %90	100.000	49950	50050	%49,9

Çizelge 6 Naive Bayes MVMN distribution sonucu

BIT Uzunluğu	**TEST Uzunluğu**	**Doğru**	**Yanlış**	**Oran**
1024 Bit- %75	256	26	230	%10
1024 Bit- %90	102	15	87	%15
10.000 Bit- %75	2500	618	1882	%25
10.000 Bit- %90	1000	233	767	%23
100.000 Bit- %75	25000	3184	21816	%13
100.000 Bit- %90	10000	1333	8667	%13
1.000.000 Bit- %75	250000	62856	187144	%25
1.000.000 Bit- %90	100000	24904	75096	%25

3. Karar Ağacı Sonuçları

Tez çalışmasında karar ağacı metodunda node seviyesi ve kırınım hesaplama fonksiyonları olarak “deviance”, “twoing” ve “gini” alt hesaplama fonksiyonları kullanılmaktadır. Mevcut veri setlerimize hesaplama uygunluğu açısından Gini daha uygun görülmüş ve Gini katsayısının farklı değerlerinin karar ağacı yöntemine olan etkisi gözlemlenmek istenmiştir. Gini 1 değerinden 4 değerine kadar sırası ile test sonuçları aşağıdaki tablolarda Çizelge 7’den Çizelge 10’a kadar görülebilir. Elde edilen sonuç tablolarında farklı Gini değerleri ile birlikte karar ağacı yönteminin farklı veri uzunluğunda ve farklı eğitim-test oranlarında sonuçları gösterilmiştir.

Çizelge 7 Karar ağacı Gini katsayısı = 1 ile hesaplama sonuçları

BIT Uzunluğu	TEST Uzunluğu	Doğru	Yanlış	Oran
1024 Bits- %75	256	131	125	%51,1
1024 Bits- %90	102	60	42	%58,8
10.000 Bit- %75	2500	1255	1245	%50,2
10.000 Bit- %90	1000	491	509	%49,1
100.000 Bit- %75	25.000	12592	12408	%50,3
100.000 Bit- %90	10.000	5001	4999	%50
1.000.000 Bit- %75	250.000	125191	124809	%50
1.000.000 Bit- %90	100.000	50027	49973	%50

Çizelge 8 Karar ağacı Gini katsayısı = 2 ile hesaplama sonuçları

BIT Uzunluğu	TEST Uzunluğu	Doğru	Yanlış	Oran
1024 Bits- %75	256	126	130	%49,2
1024 Bits- %90	102	50	52	%49
10.000 Bit- %75	2500	1243	1257	%49,7
10.000 Bit- %90	1000	505	495	%50,5
100.000 Bit- %75	25.000	12457	12543	%49,8
100.000 Bit- %90	10.000	4989	5011	%49,8
1.000.000 Bit- %75	250.000	124850	125150	%49,9
1.000.000 Bit- %90	100.000	50070	49930	%50

Çizelge 9 Karar ağacı Gini katsayısı = 3 ile hesaplama sonuçları

BIT Uzunluğu	TEST Uzunluğu	Doğru	Yanlış	Oran
1024 Bits- %75	256	131	125	%51,1
1024 Bits- %90	102	50	52	%49
10.000 Bit- %75	2500	1226	1274	%49
10.000 Bit- %90	1000	487	513	%48,7
100.000 Bit- %75	25.000	12492	12508	%49,9
100.000 Bit- %90	10.000	4963	5037	%49,6
1.000.000 Bit- %75	250.000	125050	124950	%50
1.000.000 Bit- %90	100.000	50050	49950	%50

Çizelge 10 Karar ağacı Gini katsayısı = 4 ile hesaplama sonuçları

BIT Uzunluğu	TEST Uzunluğu	Doğru	Yanlış	Oran
1024 Bits- %75	256	154	102	%60
1024 Bits- %90	102	63	39	%61,7
10.000 Bit- %75	2500	1578	922	%63,1
10.000 Bit- %90	1000	646	354	%64,6
100.000 Bit- %75	25.000	15722	9278	%62,8
100.000 Bit- %90	10.000	6352	3648	%63,5
1.000.000 Bit- %75	250.000	155825	94175	%62,3
1.000.000 Bit- %90	100.000	62510	37490	%62,5

4. Diskriminant Analizi Sonuçları

Tez çalışmasının bu bölümünde temelde bir boyut küçültme yöntemi olan Discriminant Analiz yönteminin oluşturduğumuz veri setinin farklı boyutlarında elde edilen sonuçları yer almaktadır. Discriminant Analiz hesaplama işlemlerinde birden fazla alt fonksiyon barındırmaktadır ancak var olan veri setimizin içeriği sadece Diag-Quadratic yöntemi ile uyum sağlayabilmiştir. Yapılan çalışmada Diag-Quadratic fonksiyonu farklı uzunluklarda ve farklı eğitim-test oranlarında kullanılarak tahmin sonuçlarına yapacağı etkiler gözlemlenmek istenmiştir. Elde edilen sonuçlar Çizelge 11'de paylaşılmıştır.

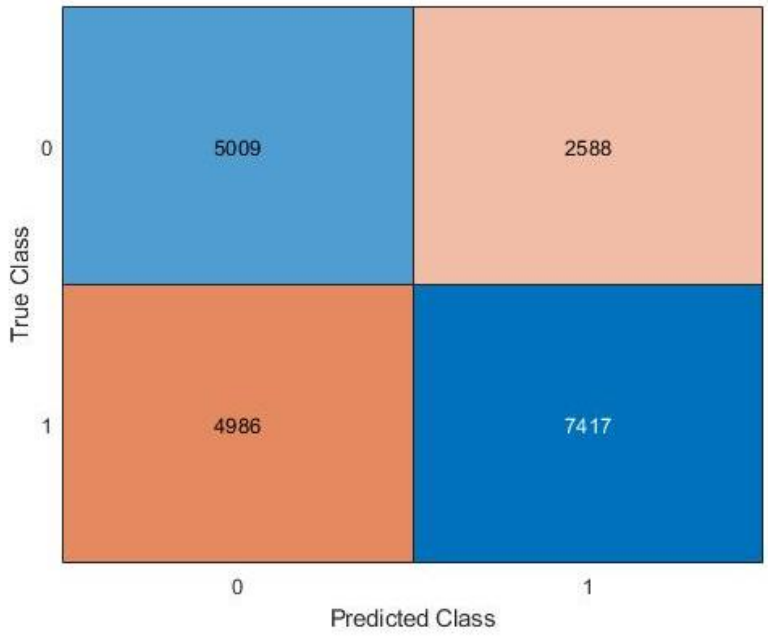
Çizelge 11 Discriminant Analysis Diag-Quadratic sonuçları

BIT Uzunluğu	TEST Uzunluğu	Doğru	Yanlış	Oran
1024 Bits- %75	256	57	199	%22,2
1024 Bits- %90	102	24	78	%23,5
10.000 Bit- %75	2500	624	1876	%25
10.000 Bit- %90	1000	242	758	%24
100.000 Bit- %75	25.000	6299	18.701	%25,2
100.000 Bit- %90	10.000	2449	7551	%24,5
1.000.000 Bit- %75	250.000	62.652	187.348	%25
1.000.000 Bit- %90	100.000	25.082	74.918	%25

5. Yapay Sinir Ağı Sonuçları

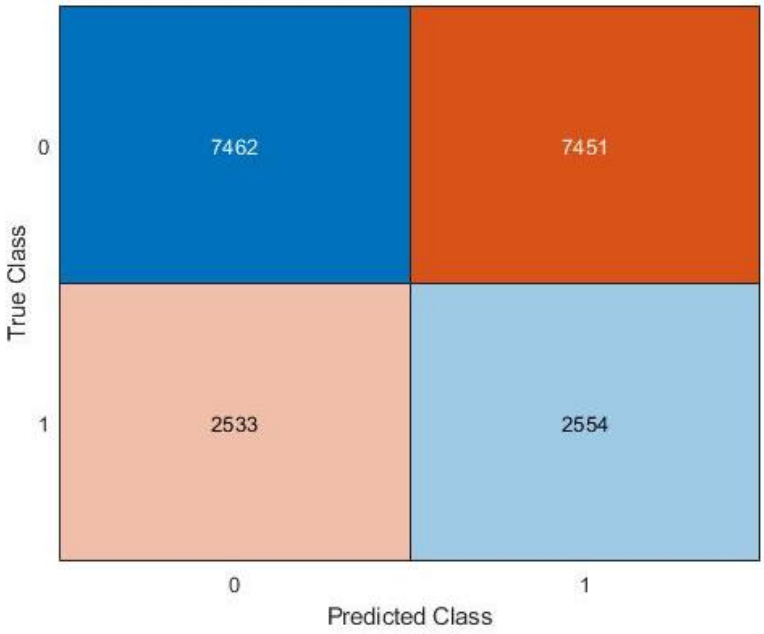
Tez çalışmasında yukarıda tasarımından bahsedilen yapay sinir ağının temelde farklı iki veri uzunluğunda yapılan test sonuçları yer almaktadır. Öğrenme oranı 0.01 seviyesinde tutulan yapay sinir ağı sisteminin farklı tekrar sayılarında elde edilen sonuçları yer almaktadır. Şekil 42-44 arası 20.000 uzunluğunda bir veri setinin farklı tekrarlarda eğitiminden sonra yapılan tahmin sonuçları yer almaktadır.

Şekil 42'de 20.000 veri kullanılarak 10 epoch'ta yapılan test sonucu %62,13 'lük bir başarı ortalaması ile tahmin işlemi gerçekleştirilmiştir



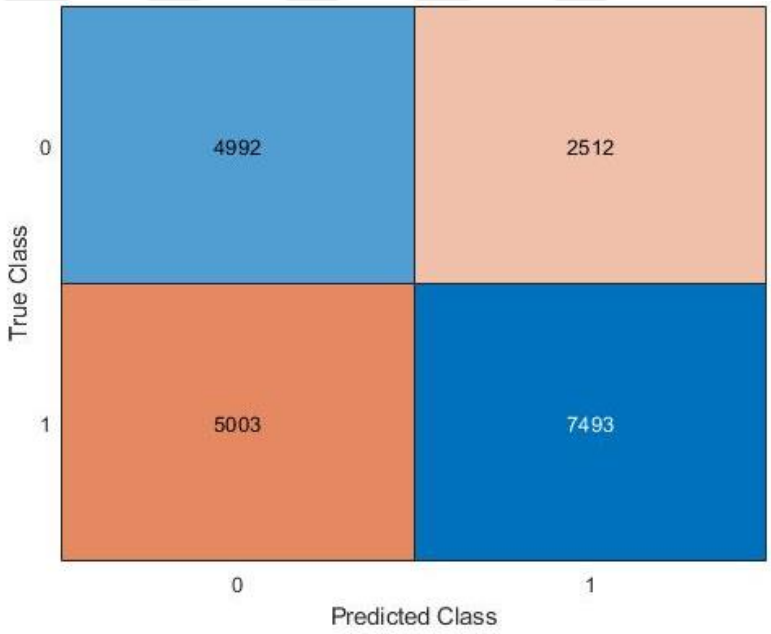
Şekil 42 YSA 20K veri 10 epoch sonucu

Şekil 43'de 20.000 veri kullanılarak 100 epoch'ta yapılan test sonucu %50,08 'lik bir başarı ortalaması ile tahmin işlemi gerçekleştirilmiştir.



Şekil 43 YSA 20K veri 100 epoch sonucu

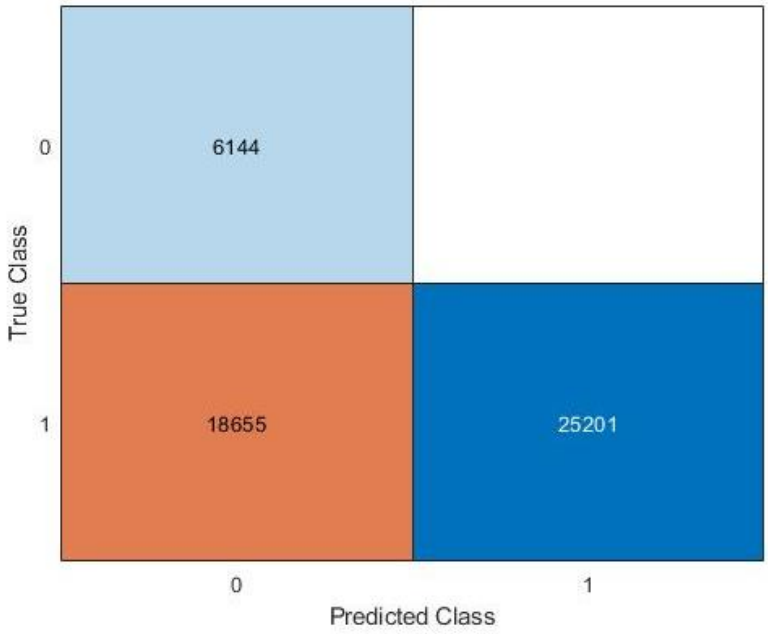
Şekil 44'de 20.000 veri kullanılarak 1000 epoch'ta yapılan test sonucu %62,42 'lik bir başarı ortalaması ile tahmin işlemi gerçekleştirilmiştir.



Şekil 44 20K veri 1000 epoch sonucu

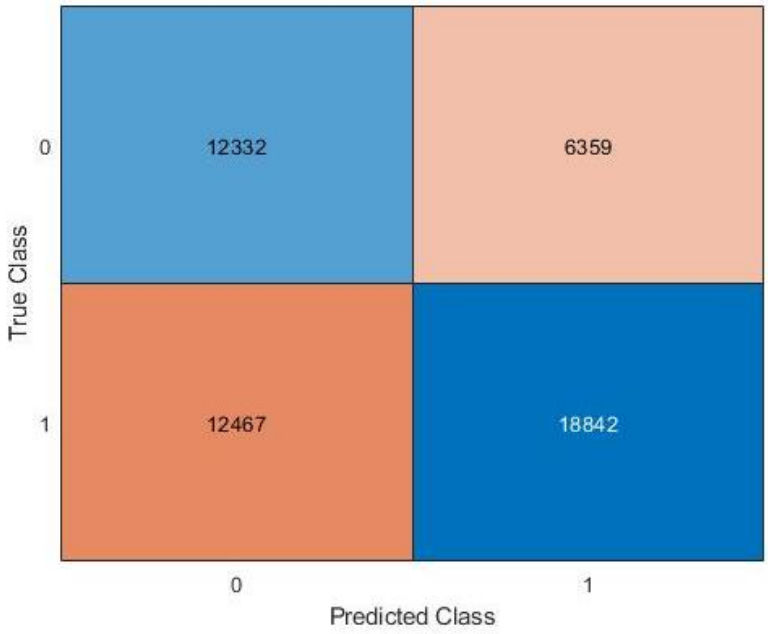
Şekil 45'den Şekil 47'ye kadar yer alan resimlerde yukarıdaki gibi yapay sinir ağının farklı eğitim tekrarları sonrasında elde edilen sonuçları yer almaktadır. Bu görsellerde yer alan sonuçlar 50.000 veri kullanımından elde edilen sonuçları içermeketedir. Resim 45'de veri seti 10 tekrar ile eğitilmiş ve elde edilen sonuç

confusion matrix biçiminde paylaşılmıştır. Başarı oranı olarak %62,69 elde edilmiştir.



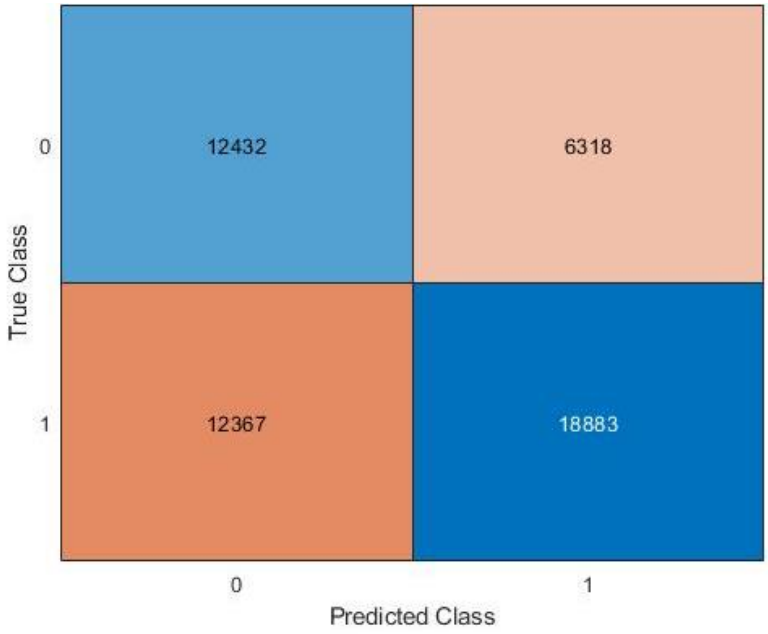
Şekil 45 YSA 50K veri 10 epoch sonucu

Şekil 46'de 50.000 uzunluğunda bir veri seti sinir ağının eğitimi işleminde kullanılmıştır. Eğitim işleminde 0.01 öğrenme oranında 100 tekrar ile tamamlanmıştır. Tahmin sonucunda %62,35 başarı oranı elde edilmiştir.



Şekil 46 YSA 50K veri 100 epoch sonucu

Şekil 47'de 50.000 uzunluğundaki veri seti 0.01 öğrenme oranı ile 1000 tekrarda eğitimini tamamlamıştır. Tahmin işlemi sonucunda %62,63 oranında başarı elde edilmiştir.



Şekil 47 YSA 50K veri 1000 epoch sonucu

I. Yapay Zekâ Tahmin Yöntemlerinin Kullanımı ve Elde Edilen Çıkarımlar

kNN yönteminde grup olarak kullanılan veri setleri tek düze değerler içermektedir. Polarizasyon filtre değerleri için 1-2-3-4, gönderici ve alıcı değerleri için 0 ve 1, uzlaşı olup olması durumuna göre 1 ve -1 gibi sabit değerlerden eğitim veri seti oluşmaktadır. kNN gibi veri setlerini kümeleyen ve sınıflandırılması için verilen veri setlerini bloklar halinde gruplanan değerlerin oluşturduğu belirli bir desen vardır. Son olarak tahmin amaçlı verilen veri seti, koordinat düzlemi üzerinde düşündüğünde gruplanmış olan 4 farklı polarizasyon filtre grubundan birine denk düşmektedir. Eğitim esnasında veri setinin sürekli olarak değişmesi, farklı boyutlarda veri setlerinin eğitim ayrılması, kullanılan verilerin 0-1 arasında normalize edilmesi, kNN'in %100 doğru tahminler yapmasını yani ağın overfitting durumunu yaşamasını engelleyememektedir. Kullanılan verilerin niteliği sebebi ile kNN algoritması tahmin işlemlerinde uygunluk göstermemiştir.

Karar ağaçları eğitim veri setinde eğitildiklerinde ve eğitim veri setine göre yapısal mekanizması kurulduğunda çok başarılır sonuçlar verebilmektedir, ancak eğitim harici veri bütünlüğü ve farklı form içeren değerlerde başarılı sonuçlar alınamaya bilmektedir. Kullanılan eğitim ağında kırınım sayısının arttırılmasına bağlı olarak başarının arttığı gözlemlenmektedir. Denemeler esnasında kırınım sayısının 7 olması durumunda ağın overfitting durumu ile karşılaştığı gözlemlenmiştir. Ancak

sınıflandırma yapılması gereken maksimum grup sayısı polarizasyon sınıfları sayısı kadar olması gerektiğinden 4 adetten fazla kırınım yapılmaması gerekmektedir. 4'ten fazla kırınım yapılan işlemler test edilmiştir ancak bu mantıktan dolayı sonuçlara yer verilmesi gerekli görülmemiştir. Karar ağacı katsayı hesaplama değerlerinde Gini katsayısı hesaplayan "GNI" yöntemine muadil "DEVIANCE" ve "TWOING" yöntemleri ile yapılan hesaplamalarda tüm veri boyutlarında ağın ezberleme yaptığı, "over-fitting" durumu ile tüm kırınım değerlerinde rastlanıldığı gözlemlenmiştir.

Naive Bayes yönteminde "MN" fonksiyonunda negatif değer içeren veri seti uyarısı alınabilir. Bunun engellemesi için -1 değerleri 0 olarak değiştirilmiştir. Değiştirilmiş hali ile elde edilen değerler ilk kısımda yer alan sonuçlardır. Benzer bir şekilde bir farklı denemede -1 değeri 99 olarak değiştirilip tekrar test edilmiştir. Elde edilen sonuçlar arasında farklar bulunmaktadır, ancak başarı fenomeninde radikal bir değişim gözlenmemiştir.

Discriminant analiz yönteminde test sonuçlarında görülebileceği gibi diag-quadratic yöntemi dışındaki yöntemler ile kullanılan veri setinin niteliği ile uyuşmamaktadır. Quadratic yönteminde kovaryans matrislerin tekil değerler içermesinden dolayı hesaplama işlemleri yapılamamaktadır. Kullanılan tüm eğitim veri seti oranlarında %10 eğitim %90 test'den %50 eğitim %50 test oranına kadar tüm denemelerde %100 hatalı tahmin sonuçları alınmaktadır.

Yapay Sinir Ağları yönteminde test sonuçlarından da anlaşılabileceği gibi veri seti yoğunluğu ile birlikte tekrar sayılarının arttırılması ile başarılı sonuçlar elde edilmiştir. Yapılan çalışmalarda mevcut ağın geri besleme öğrenim oranı, ağda kullanılan aktivasyon fonksiyonlarının sonuca etkisi sürekli testler sonucunda elde edilmiştir. İdeal eğitim ve tekrar sayısı bulunduğunda tahmin başarısı oranının %60 seviyelerinde olabileceği test sonuçlarından gözükmektedir. Farklı eğitim tekrarları ve farklı veri seti büyüklüklerinde yapılan testlerin ortalamasında diğer yöntemlerden farklı olarak %50 üzeri başarılı tahmin yürüttüğü gözlemlenmiştir.

Literatürde rastlanılan mevcut KAD sistemlerinin başarılı anahtar dağıtım oranlarının %20-%30 aralığında olduğu göz önüne alındığında, yukarıda bahsedilen makine öğrenmesi ve yapay sinir ağı tasarımının başarılı tahmin işlemlerinde başarılı sonuçlar elde edebildiği ve bu yöntemler kullanılarak geliştirilecek sistemlerde artık bit'lerin azaltılabileceği gösterilmiştir. Mevcut incelenen makine öğrenmesi

yöntemleri ve yapay sinir ağı tasarımımız ile tahmin işlemleri yapılmıştır. Yapılan işlemler sonucunda en başarılı tahmini %75 seviyesinde Naive Bayes yönteminin sağladığı görülmüştür. NAive Bayes yöntemi bu işlemi 1 milyon uzunluğunda bir veri setinde yakalamıştır. Eğitim için kullanılan veri seti azaldığında elde edilen başarının da azaldığı gözlemlenmiştir. Ancak tüm Naive Bayes yöntemleri tüm alt fonksiyonları ve tüm veri setlerinde denenip ortalama başarıları hesaplandığı durumunda Naive Bayes yönteminin başarı ortalamasının %42'ler olduğu gözlemlenmiştir. Buna karşılık tasarlana Yapay Sinir Ağı tasarımının 20 bin'lik veri setlerinde eğitim ve test işlemlerini tamamlaması sonrasında %62 gibi yüksek oranda bir tahmin performansı sergilemiştir. Farklı kombinasyonlarda elde edilen Yapay Sinir Ağı değelerinin başarılı tahmin ortalaması %60.34 olup diğer tüm yöntemlerden daha üst düzeyde bir performans göstermiştir. Maksimum başarı oranı ile ortalama başarı oranı arasında diğer yöntemlere göre daha az fark olması geliştirilen sinir ağının tahmin yapma işleminde tutarlılığını göstermektedir. Yapay sinir ağının her bir ara katmanında 200 nöron olması ve her nörorunun içerdiği aktivasyon fonksiyonları ve bu fonksiyonların her birinin hesaplama işlemi yaparak sonuca etki etmesi lineer olmayan bir hesaplama üstünlüğü sağlamaktadır. Böylelikle kıyaslama yapıldığı diğer makine öğrenmesi metotlarına göre daha üstün bir başarı oranına sahip olmuştur.

Çizelge 12 Makine öğrenmesi metotları karşılaştırılması

METOT	**Max Başarı Oranı**	**Ortalama Başarı Oranı**
kNN	%0	%0
Decision Tree	%64	%40
Naive Bayes	%75	%42
Discriminant Analysis	%25	%24
Neural Network	%62	%60,34

III. ÖNERİLEN ANAHTAR DAĞITIMI YÖNTEMİ

A. Blokzincir Genel Tanımı

Blokzincir teknolojisi kavram olarak 2014 yılında kullanılmaya başlamıştır. Blokzincir teknolojisinin ortaya çıkmasında gelişimsel olarak birçok bilimsel gelişmenin katkısı olmuştur. Ancak Bitcoin ismiyle 2009 yılında Satoshi Nakamoto mahlaslı kişi yahut organizasyon tarafından tanıtılan kripto paranın değerinde görülen yüksek artışlar ve insanların kolay gelir elde etme kaygısıyla çokça yatırım yapması sonucunda küresel anlamda kabul görmesi neticesinde bu ürünün geliştirilmesinde kullanılan teknolojinin ne olduğu üzerine merak uyanmaya başlamıştır. Gelinen noktada Blokzincir Teknolojisi kavramından daha önce üretilmesine rağmen Bitcoin kripto parası için blokzincir demek değildir, blokzincir teknolojisinin bir ürünüdür denilmeye başlanmıştır. Teoride bu fikir doğrudur. Çünkü blokzincir teknolojisi zaman damgası algoritması, özüt algoritması, Merkle ağacı algoritması, kriptoloji bilimi, bilgisayar bilimleri ve yazılım mühendisliği bilimi gibi birçok bilimsel çalışma konusunun olgunlaşması ve birlikte kullanımı neticesinde ortaya çıkmış bir çalışma konusudur (Hussein vd., 2022).

Gelinen noktada blokzincir teknolojisi ortaya çıktığı süreçteki kullanım kaygılarının dışında ilerlemeler kaydetmiş ve gelişim göstermiştir. İlk olarak Bitcoin kripto parasında elde edilmek istenen merkezi otoritenin aradan çıkartılıp ademi merkeziyetçi, şeffaf ve anonim finansal alternatif önerisi zamanla teknolojinin merkezi otorite olarak nitelendirilebilecek banka, noter, tedarik zinciri hizmetleri gibi alanlarda kullanılması ile birlikte sistem kontrolü merkezileşmiş ve üretilirken elde edilmek istenen amacı aşmıştır. Bu sebeple blokzincir teknolojisi için söylenen dağıtık bir veri tabanı sistemidir açıklaması doğru olmakla birlikte yeterli değildir. Yapılması gereken tanım: Blokzincir teknolojisi veri kayıtlarının tek yönlü ve değiştirilemez olduğu, oldukça güvenli, dağıtık bir defter teknolojisidir (Aklilu ve Ding, 2022).

Blokzincir sistemleri adından da anlaşılacağı üzere bloklardan oluşan sistemlerdir. İlk üretilen blok için yaratılış bloku denir. Yaratılış bloku ayrıca blokzincir sisteminin karakteristik özelliklerinin belirlendiği bloktur. Karakteristik özelliklerden kasıt blok yapısında bulunacak bölümlerin belirlenmesi ve ihtiyaca göre bu bölümlere ayrılan boyutların netleştirilmesidir. Yaratılış bloku sonrasında üretilen tüm bloklarda özüt değeri bulunmaktadır. Özüt değeri elde edilemesi için SHA256 isimli algoritma çokça tercih edilmektedir. Özüt algoritmaları tek yönlü çalışan, geri alınamayan ve 256 bitlik uzunlukta girilen veriye göre değişen sonuçlar veren algoritmalardır. Bu özüt değerleri blokzincir sistemleri için hayati önem taşımaktadır. Çünkü blokzincir sistemlerinde fiziki hiçbir değer tutulmaz. Bir başka deyişle finansal uygulama üzerinden örnek vermek gerekirse, insanların kripto cüzdanlarında bulunan coinlerin aidiyet bilgisi sistemde tutulmaktadır. Yani bu aidiyet bilgisi birileri tarafından sizin bilginiz dahilinde olmayacak şekilde değiştirilebilirse tüm yatırımlar kaybedilebilir. Özüt algoritmaları bu aidiyet bilgilerinin değiştirilememesini sağlamaktadır. Çünkü bir blok oluşturulduğunda o blok özütlenir ve kendisinden bir önceki blokun özüt değerini de tutarak zincire dahil olur. Sonrasında sistemde yapılmak istenen herhangi bir değişiklik durumunda bu özüt değerleri değişir. Özüt değeri bir sonraki blokla eşleşmeyeceği için tutarsızlık oluşacak ve o blok eski haline getirilene kadar sistemden çıkartılacaktır. Bu sayede sistem üzerinde herhangi bir kurcalama yapılamamakta ve yapısal olarak veri kaydı gerçekleşen blokların değiştirilmesi mümkün olmayan bir hale gelmektedir (Polas vd., 2022).

Özüt değerleriyle birbirlerine bağlanan bloklar zincir haline geldiği gibi aynı zamanda da bir defter benzetmesine de uymaktadır. Çünkü her bir işlem gerçekleştiğinde bloklara yazılı ve blok için belirlenen boyut dolduğu anda da yeni bir bloka geçilir. Bu sebeple aynı bir defterin sayfaları gibi blokzincir blokları doldukça yeni bir sayfaya yani bloka geçilmektedir. Blokzincir sistemlerine erişim izni olan düğümler aktif olmadıkları süreçte gerçekleşen işlem kayıtlarının tutulduğu veri tabanları olan blok kayıtlarının öncelikle güncel halini sistemden elde eder ve sonrasında erişim imkânı bulduğu sistem üzerinde arzu ettiği transfer işlemlerini yapabilirler. Anlaşılacağı üzere blokzincir sistemleri dağıtık olması yani her bir düğümde sistemin veri

kayıtlarının bulunması sayesinde gerçekleşecek saldırılara karşı oldukça dayanıklı ve erişim imkânı ve sistem güvenliği açısından iyi bir yapıdadır (Pennino vd., 2022).

Blokzincir teknolojisinin gelişimi üç aşamada incelenmektedir. İlk aşama olarak Bitcoin kripto parası ve blokzincirin finansal alanlarda uygulanması ve alt yapısal olarak ihtiyaçların belirlenmesi ve geliştirilmesi olarak kabul edilir ve bu döneme Blokzincir 1.0 denilmektedir. Burada Bitcoin kripto parasının kendi blokzincir sistemini geliştirdiği ve kullanıma açtığı bilgisinin de paylaşılması gerekir. Benzer bir şekilde Ethereum kripto parası da kendi blokzincir geliştirme platfomunu geliştirmiş ve kullanıma açmıştır. Ethereum ayrıca kendi sistemlerinde akıllı sözleşme olarak ifade edilen, spesifik bir durumla karşılaşıldığında sürekli aynı işi yapan kod parçacıklarının Ethereum platformunda kullanılabilmesini sağlamıştır. Bu sayede statik olarak kabul edilebilecek blokzincir sistemlerine bir dinamizm gelmiş ve blokzincir teknolojisinin daha etkileşimli bir hal alması sağlanmıştır. Ethereum platformunun akıllı sözleşmeleri kullanılabilir hale getirmesiyle geçilen blokzincir dönemine Blokzincir 2.0 denilmektedir. Blokzincir teknolojisinin finansal olmayan alanlarda uygulanmasına ise Blokzincir 3.0 denilmektedir. Blokzincir sistemleri yukarıda paylaşılan Bitcoin ve Ethereum platformları dışında farklı platformlar (Solana gibi) ya da programlama dilleri kullanılarak (Java, Java Script, C#, C, C++ gibi) ihtiyaç duyulan sistemin gereksinimlerine göre geliştirilebilirler. Blokzincir teknolojisinin içinde bulunduğu günümüz döneminde ise artık takas edilemez jeton ve sanal evren çalışmalarının hızlanmıştır. Bu dönemin ilerleyen süreçte Blokzincir 4.0 olarak adlandırılmasına şahit olunabilir (Gatabazi vd., 2022).

Blokzincir teknolojisi daha önce de ifade edildiği üzere farklı bilimsel gelişmeleri kullanarak geliştirilebilmektedir. Bu bilimsel gelişmelerden bir diğeri zaman damgası algoritmasıdır. Zaman damgası algoritmaları bir blokzincirinde oluşturulan işlemin blokzincir sistemi tarafından doğrulandığı anın bilgisini tutan zaman serileridir. Türkiye'de zaman damgası hizmetini sadece TÜBİTAK Kamu Sertifikasyon Merkezi sağlamaktadır (Takaoğlu vd., 2019). Burada dikkatten kaçmaması gereken bir diğer husus zaman damgalarının her programlama dilinde kodlanabilecek yapıda olan karmaşıklığı

düşük ve kodlanması kolay yapıda olmalarıdır. Ancak zaman damgalarının belirlenene standartlara uygun olarak sertifikalı bir şekilde kullanılabilmesi için TÜBİTAK Kamu SM'den hizmet alınması gerekmektedir.

Blokzincir teknolojisinde bir diğer önemli konu konsensüs algoritmalarıdır. Konsensüs algoritmaları blokzincir sistemlerinde gerçekleştirilen işlem kayıtlarının bloklara kim tarafından yazılacağını ve ödül olarak belirlenen bedelin nasıl dağıtılacağını ele almaktadır. Blokzincir sistemlerinin dağıtık olması ve ademi merkeziyetçi olması sebebiyle sistemin sürdürülebilmesi için gerekli olan donanım ihtiyacı madenci denilen ve donanım yani işlem gücü sağlayan düğümler tarafından karşılanır. Bu madenciler sahip oldukları işlem gücünü aynı finansal yatırım yapan yatırımcılar gibi en çok kar edeceği blokzincir sistemi için kullanmak ister. Bu sebeple özellikle kripto para sistemlerinde işlem gücü sunan madenciler için kullanılan konsensüs algoritması büyük önem taşımaktadır (Muduli vd., 2022).

Bitcoin kripto parasında kullanılan konsensüs algoritması işin ispatı algoritmasıdır. İşin ispatı algoritmasında çözülmesi gereken bir bulmaca bulunmakta ve bu bulmacayı ön önce çözen madenciye bloku sisteme ekleme hakkı verilmektedir. Bu sayede bulmacayı bilen ve yazma hakkını kazanan düğüm verilen ödülün sahibi olur. İşin ispatı algoritmasında zorluk adı altında bulmacanın çözülme seviyesini ayarlayan bir özellik bulunmaktadır. Bu zorluk seviyesinin en optimal şekilde belirlenmesi gerekmektedir. Çok zor bulmacaların çözülmesinde daha çok işlem gücü harcanacağı için enerji tüketimlerinde ciddi artışlara sebebiyet verilebilmektedir. Bu sebeple işin ispatı algoritmasını kullanan blokzincirlerde bulmaca zorluğu üzerine yapay zekâ destekli çalışmalar başta olmak üzere yenilikçi fikirler üretilmeye çalışılmaktadır (Sanda vd., 2022).

Birçok farklı blokzincir sisteminde hissenin ispatı algoritması kullanılmaktadır. Hissenin ispatı algoritması blok yazılması aşamasında bir bulmaca çözme şartı koşmaz ve madencilerin cüzdanlarında bulunan coin miktarının yani hisse miktarının fazlalığına göre yazma hakkını dağıtır. İlk önerildiğinde sadece hissesi çok olan ödül aldığı diğer madencilerin sorun yaşadığı bu konsensüs algoritması daha sonra adaletli bir sisteme geçmiş ve sürekli aynı düğümlerin ödül almayacağı daha makul bir ödül dağıtım sistemine

geçmişledir. Hissenin ispatı algoritması işin ispatı algoritmasına göre çok daha çevre dostu bir algoritmadır. Günümüzde birçok konsensüs algoritması bulunmaktadır. Geliştirilecek blokzincir sisteminin gereksinimlerine göre uygun algoritmanın seçilmesi gerekmektedir (Varavallo vd., 2022).

Merkle ağaçları blokzincir sistemleri için olmazsa olmaz konulardan biridir. Merkle ağaçları blokzincir bloklarında bulunan baş bölgesinde işaretlediği değeri bünyesinde tutarak çok uzun bir süre o blokun varlık bilgisini saklar. Bu sayede blokzincir sisteminde gerçekleşen işlemlerin doğrulanabilmesi sağlanmaktadır (Damisa ve Nwulu, 2022).

Blokzincir sistemleri erişilebilirliklerine göre sınıflandırılabilirler. Bitcoin ve Ethereum örneğinde olduğu gibi herkesçe işlem kayıtlarının incelenebildiği, sisteme dahil olup coin transferi gerçekleştirebilmek ve madenci olarak sisteme dahil olmanın mümkün olduğu blokzincir sistemlerine açık blokzincir denilmektedir. Bu sistemler anlaşılacağı üzere işlem verileri herkesçe incelenebildiği için şeffaf, düğümlerin bilgisi hiçkimse tarafından bilinmediği için anonim ve blokzincir teknolojisinin yapısal özellikleri sayesinde oldukça güvenli ve sağlam sistemlerdir. Bir diğer blokzincir şekli ise özel blokzincirlerdir. Düğümlere verilen erişim izni ve erişim izni olanların da veri okuma ya da yazma hakkının olup olmadığına göre farklılaşabilen blokzincir sistemlerine özel blokzincir sistemi denilmektedir. Bir başka blokzincir sistemi de konsorsiyum blokzincir sistemleridir. Bu sistemler daha çok özel şirketlerin spesifik ihtiyaçları için uygun olan blokzincir sistemleridir (Meidute-Kavaliauskiene vd., 2022).

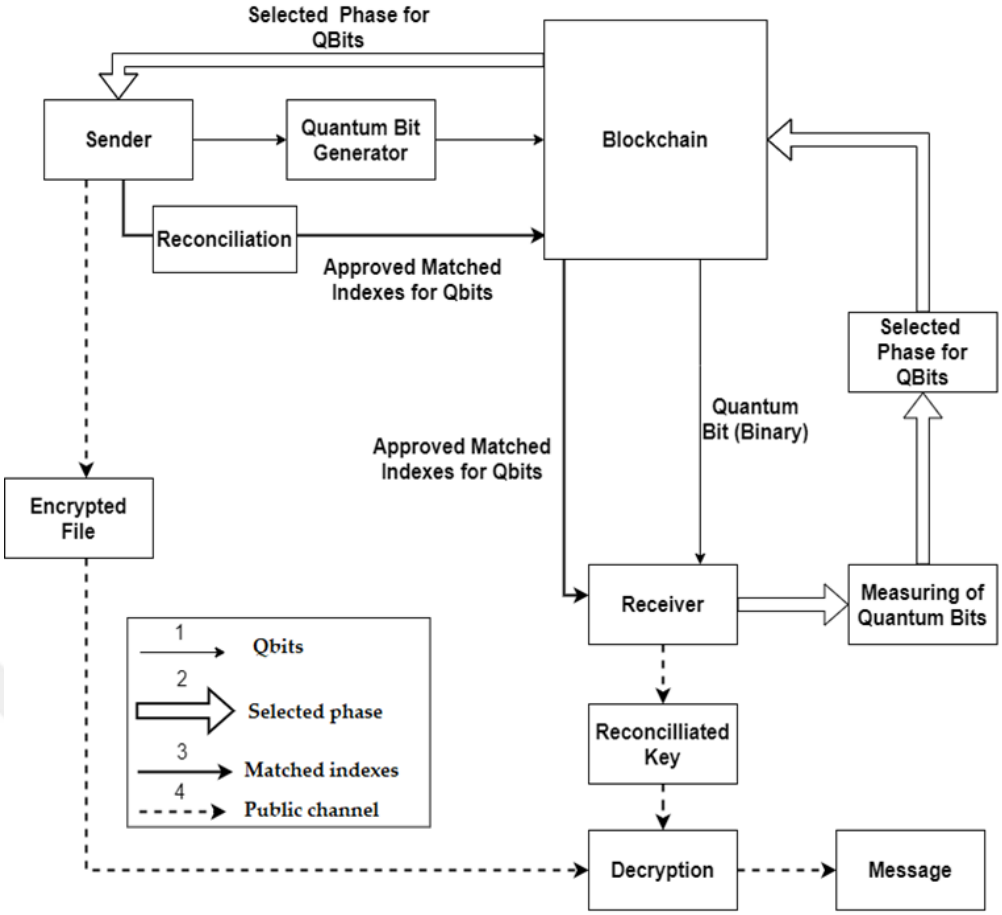
Blokzincir teknolojisi yeni kabul edilebilecek bir çalışma konusu olması sebebiyle her geçen gün yeni alanlarda kullanımı test edilmektedir. Tez çalışmamızda olduğu üzere kuantum anahtar dağıtımında bu teknolojinin imkanlarının katkı sağlayıp sağlayamayacağı test edilmiştir. Anlaşılacağı üzere blokzincir teknolojisinin bu denli farklı alanlarda uygulanabilmesi için karmaşıklığının düşük ve uygulanabilirliğinin yüksek olması gerekmektedir. Blokzincir sistemleri için karmaşık olmayan sistemlerdir denilmesi pek mümkün değildir. Ancak uygulama açısından aynı durum söz konusu değildir. Hali hazırdaki sistemlerin güvenliğinin arttırılması yahut blokzincir teknolojisiyle değiştirilebilecek modüller üzerinde çalışılması mümkündür. Yani

blokzincir sistemleri hali hazırdaki sistemlere bir katman olarak eklenebilen yapıdadırlar. Ayrıca tümüyle blokzincir sisteminden oluşan sistemler de geliştirilebilir.

Blokzincir sistemlerinin uygulandığı spesifik durumlar için veri boyutunun çok yüksek ya da boyutundan bağımsız olarak çok fazla veri kaydı gerektiren işlemlerin olduğu durumlarda blokzincir-içinde ve blokzincir-dışında sistemleri kullanılmaktadır. Örneğin bir hastanede her gün çok yüksek sayılarda ve büyük boyutlarda üretilen çeşitli formlardaki dosya türlerinin blokzincir sisteminde kaydedilmesi, sürdürülebilecek bir durum değildir. Böyle durumlarda blokzincir-dışında bir mimari kullanarak blokzincirde tutulacak verilerin belirlenmesi sonrasında diğer verilerin sistem dışında bulunan sunucularda tutulması yolu tercih edilebilir.

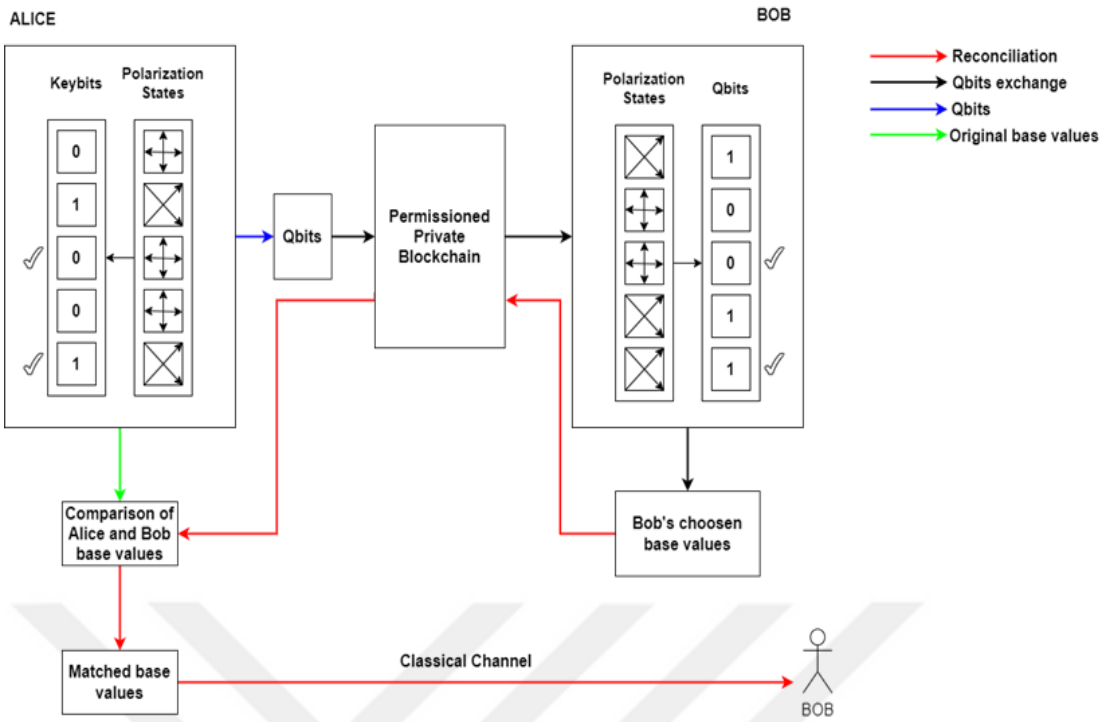
B. Önerilen Blokzincir Tabanlı Sonuç

Önerilen bu sistemde özel bir blokzincir ağı kullanılarak, herkese açık olmayan ledger- defterleri kullanılarak veri aktarımının fiber hatlarda yer alan foton güvenliğine benzer bir güvenlik ile korunabileceği düşünülmektedir. Kuantum anahtar üretecinden üretillen fotonlar, üreteç devresinde polarizasyon filtrelerinden geçirilip okunarak, daha sonrasında elde edilen değerleri ile blokzincir sisteminde yer alan defterlere yazılacaktır. Defterlerde yer alan anahtar değerleri taraflar arasıdna güvenli bir şekilde aktarılacaktır. Aktarılan değerler daha sonrasında üst bölümlerde aktarıldığı ve şemada gösterildiği üzere uzlaşı protokolüne başlayacak ve karşılıklı anahtar kararlaştırma işlemini blokzincir üzerinden tamamlayacaklardır. Şekil 48'de BB84 algoritması için geliştirilmiş blokzincir sisteminin mimarisi paylaşılmıştır.

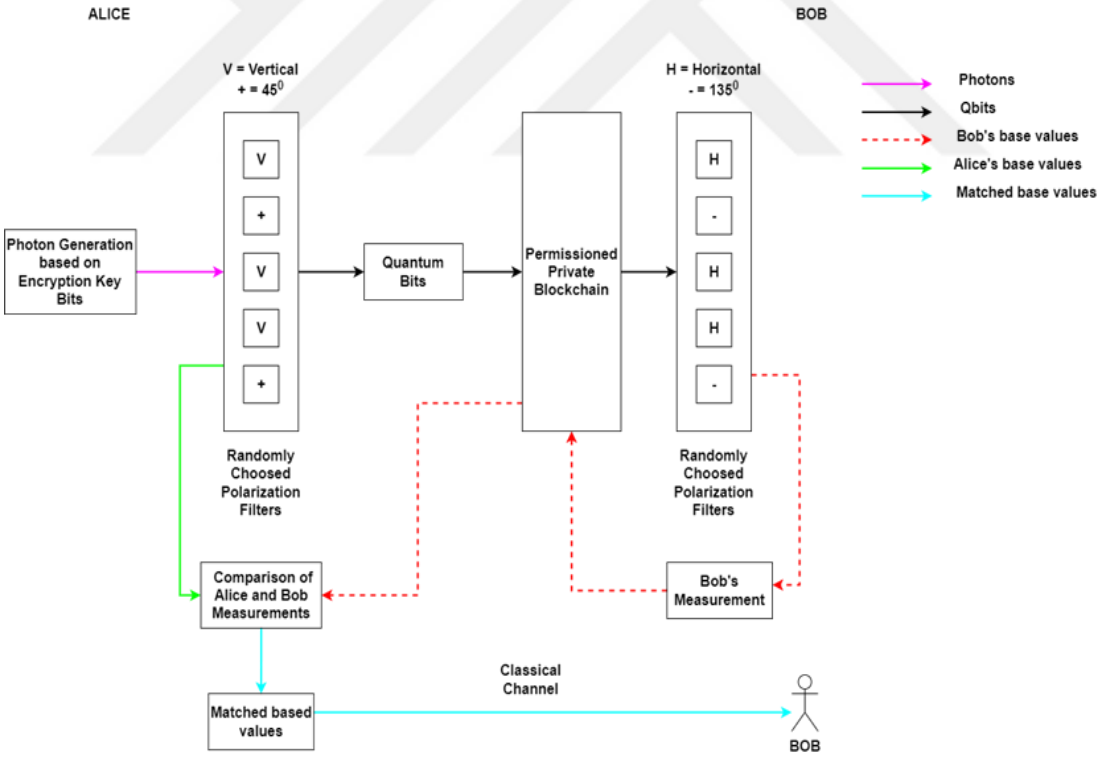


Şekil 48 BB84 protokolü için blokzincir sistemi önerisi

Aşağıda paylaşılan Şekil 49 ve Şekil 50'de benzer bir şekilde BB84 algoritması için kurulan mevcut yöntemin E91 ve B92 protokollerine revize edilmiş yöntemlerini gösteren mimariler yer almaktadır.



Şekil 49 E91 protokolü için blokzincir sistemi önerisi



Şekil 50 B92 protokolü için blokzincir sistemi önerisi

C. Çıkarımlar

Tezin ilk bölümlerinde anlatıldığı üzere, yukarıki bölümlerde kuantum anahtar üretimi ve dağıtımı sistemlerinin çalışması simule edilmiştir. Simulasyon ötesi gerçek sistemlerin temelinde güvenilirliği yüksek optik bileşenler ve bu bileşenlere entegre hassas elektro-optik düzenekler ve ilgili destekleyici yazılımlar bulunmaktadır. Tüm bu sistemler yüksek seviyede dış etmenler ve kalibre edilmesi gereken modüller içermektedir. Bu hassas düzeneklerin günümüzde donanımsal bazda iyileştirilmesi devam etmektedir ve bu sistemlerin teknolojik altyapıları ve yatırımsal yüksek seviyeli masrafları bulunmaktadır. Geliştirilen sistemler yüksek veri kayıpları ve artık kuantum bit üretimi gerçekleştirmektedirler. Günümüzde geleceğin teknolojisi olarak görülen bu yeni teknolojiye entegre olması gerekmektedir. Ancak mevcut teknolojik altyapı ile tüm ülkelerin entegre olabilmesi mümkün gözükmemektedir. Günümüzde bu teknolojinin ve sağladığı avantajlarından faydalanılabilmesi için günümüzde entegrasyonu daha hızlı bir şekilde ilerlemekte olan başka bir teknoloji ile hibrid çözümler üretilmesi gerekmektedir. Üretilecek bu çözüm ile kuantum teknolojilerinin fiziksel ve donanımsal gelişmeleri ve üretilmeleri beklenmeden, bağımsız olarak blockchain teknolojisinden faydalanılabilir. Blockchain teknolojilerinden faydalanılarak üretilen tamamen rastgele olan anahtarların benzer bir güvenlik seviyesine sahip bu teknoloji ile dağıtımı sağlanabilir. Karşılıklı olarak doktora tezimizin konusu olan makine öğrenmesi metotları ile artık bit'lerin azaltımı da sağlanarak önerilen hibrid sistemi daha efektif olması sağlanabilir. Güncel olarak her iki teknolojinin kullanımı ve gündelik hayatımıza entegresi kullanılabileceği teknik alanların arttırılması ile daha da hızlanabilir.

IV. ANALİZ VE TARTIŞMA

Doktora tez çalışmamızda temeli; rastgele ve kaotik olarak görünen bir yapının aslında ne kadar karmaşık ve kaotik olsa dahi içerisinde bir desen içerebileceği varsayımından ilerlemektedir. Bu inanışımızı kuvvetlendiren unsur kuantum anahtar dağıtım sistemlerinin aslında rastgele oluşturulan ve kullanımının temel taşı olan fotonların işlenip Qbit'lere dönüştürülmesinde sınırlı sayıda polarizasyon filtresinin kullanılıyor olmasıdır. Bu çalışmayı yapmamızın temel motivasyonlarından biri bilgi alanının stratejik ve geleceğin teknolojisi olmasıdır. Mevcut kuantum anahtar dağıtımı sistemleri kuantum teknolojilerinin günlük hayatımıza ilk girdiği, en temel seviye ve en erken adapte olması gereken sistemleridir. Bu sistemleri ile ilgili kuantum anahtar üreteçlerinin geliştirilmesi ve ticarileştirilmesi tamamlanmış olup, gelişmiş ülkeler seviyesinde yer alan birkaç ülke tarafından kablolu ve kablosuz kuantum veri aktarımları üzerine çalışmalar devam etmektedir. Mevcut sistemsel altyapılar ve sistemin oluşturduğu artık bit'lerin fazlalığı, kuantum sistemlerinin sunduğu avantajların kullanılabilirliğini olumsuz manada etkilemektedir. Üretilen anahtarların %18 ila %25'lik bir kısmının aslında kullanılabilir olduğu, artık bit'lerin sistemsel sebepler, dış etmenler ve algoritmik temelde yatan güvenlik unsuru tasarımlardan dolayı mevcut olma durumlarına devam etmektedir.

Bu soruna çözüm olarak önerdiğimiz makine öğrenmesi tabanlı tahmin sistemlerinde birden fazla yöntem ve metot, üretici tarafın bilgilerini alıcı tarafın elde ettiği ve edeceği değerler üzerinden tahmin etmeye çalışmak üzerinedir. Çalışmanın test ve sonuçlar kısımları incelendiğinde anahtar paylaşımı için kullanılacak veri aktarım bit'lerinin güncel veri aktarımı için ideal bir seviye olan 1024 bit uzunluğundan başlatılarak 1 milyon bit uzunluğuna kadar test edildiği gözlemlenebilir. Mevcut tahmin sistemlerinde %50 ve %60 oranlarında başarılı tahmin sonuçları elde edilmiştir. Sırasıyla kNN, Decision Tree, Naive Bayes ve Discriminant Analiz yöntemleri MATLAB

platformunda tanımlanarak mevcut veriler üzerinden test edilmiştir. Eğitim işlemi esnasında test sonuçları kısmında da yer aldığı gibi %90-%10 seviyesinden %50-%50 oranlarında eğitim ve test veri paylaşımı yapılmıştır. kNN algoritmasında eğitimden sonra test aşamasında tahmin yapabilmesi için verilen bilgiler kNN'in farklı özelliklerinde test edilerek, kNN içerisinde farklı kombinsayonların birbirilerine göre olan üstünlükleri karşılaştırılmıştır. Bu doğrultuda kNN mesafe ölçüm fonksiyonları değiştirilmiştir. Ayrıntılı sonuçlar ve bilgiler için kNN test ve sonuçlarının yer aldığı bölümler incelenebilir. İşlem sonucunda kNN yönteminin temel olarak kullandığımız veritabanı ile uyumlu olmadığı gözlemlenmiştir. Elimizdeki verilerde sürekli olarak 0-1 bit değeleri, 1'den 4'e kadar farklı değerler ile polarizasyon filtrelerinin sembolize edilmesi ve uzlaşı protokolü sonucu olumlu ve olumsuz olma durumları 1,0 ve 1,-1 şeklinde gösterilmiştir. Eğitim işleminde oranların değiştirilmesi, kullanılan mesafe ölçüm fonksiyonlarının değiştirilmesi kNN'in eğitim veri setini ezberlemesini engelleyememiştir.

Diğer bir makine öğrenmesi metodu olan Decision Tree'de benzer bir şekilde kNN'de olduğu gibi veri setine farklı eğitim ve test oranları uygulanmıştır. Ağ bu farklı oranlarda eğitimini tamamlamış ve test işlemlerine tabi tutulmuştur. Elde edilen sonuçlarda farkı kırınım algoritmaları tercih edilmiştir. Bu kırınım algoritmaları "Gini", "Twoing" ve "Deviance"'dır. Gini yöntemi dışında kullanılan yöntemlerde Decision Tree yöntemi eğitim verilerini ezberleşmiş ve eğitim sonucu başarısız olmuştur. Gini yönteminde yapılan eğitim işlemlerinde farklılık olması açısından farklı Gini seviyeleri algoritmaya verilmiş ve bu değerlere kadar kırınım yapması sağlanmıştır. Kırınım sayısı arttırıldıkça sistemin eğitim verileri üzerinen ezberleme sorununa daha çok yaklaştığı, sistemsel karmaşıklığın ve iş yükünün arttığı gözlemlenmiştir. Elde edilen sonuçlar içerisinde Gini değeri 1 ve 2 olan sonuçların birbirilerine yakın sonuçlar içerdiği gözlemlenmiştir. Başarı oranı olarak ortalama %50 başarılı tahmin yaptığı gözlemlenmiştir.

Tezde kullanılan diğer bir makine öğrenmesi yöntemi ise Naive Bayes'dir. Bu yöntemde yukarıdaki bölümlerde de anlatıldığı gibi eldeki verilerin tekrarlanma sıklıkları ve gerçekleşme olasılıklarını temel olarak kullanmaktadır. Yöntemlerin hepsinde olduğu gibi Naive Bayes farklı oranlarda veri blokları ile

eğitilip test edilmiştir. Farklı uzunluklarda veri setleri kullanılarak, veri uzunluğunun eğitim işlemine etkisi ve dolayısıyla test sonucuna etkisi gözlemlenmek istenmiştir. 1MB'dan 1 milyon veri uzunluğuna kadar farklı kombinasyonlar denenmiştir. En başarılı test sonucuna 1 milyon veri uzunluğunda %75 eğitim verisi kullanıldığında rastlanılmıştır. Elde edilen en yüksek başarılı test sonucu %75, en düşük test sonucu %90 eğitim %10 test oranında kullanılan 1MB'lık veridir. 1MB ile 1 milyon veri uzunluğu arasında kalan diğer tüm veri uzunluğu ve eğitim verisi oranlarında ise ortalama %50 ve çevresi birbirine yakın değerler elde edilmiştir.

Son olarak test edilen yöntemimiz Discriminant Analiz yöntemidir. Bu yöntem temel olarak PCA-Principle Component Analysis gibi bir boyut küçültme algoritması olduğundan diğer makine öğrenmesi metotları arasında en düşük performans sergileyen yöntem olmuştur. Tüm eğitim veri uzunluklarında ve farklı oranlarda eğitim verisi ile eğitim işlemi yapılmasına rağmen elde edilen sonuçlar minimal farklar ile %25 oranında kalmıştır. Mevcut sistemlerde yapay zekâ eklentisi olmadan dahi elde edilen başarılı anahtar uzlaşı sonuçları benzer başarı oranları içerdiğinden bu yöntemin iyileştirme işlemlerinde başarısız olduğunu aktarabiliriz.

Tasarladığımız sinir ağında 3 ara katman kullanılarak son katmanda bir softmax fonksiyonuna yer verilmiştir. Tasarlanan sistem temelde diğer yöntemlere göre çok daha az veri ile eğitilmiştir. Geri beslemeli eğitim sisteminde eğitim oranı olarak 0.01 seviyesi kullanılmış ve yöntem içi farklılık gözlemek için farklı tekrar sayıları tercih edilmiştir. 10,100 ve 1000 tekrarlı eğitim işlemleri yapılmıştır. 20 bin ve 50 bin uzunluğunda veriler ile eğitilen sistem sonuç olarak tüm kombinasyonlarda ortalama değere yakın sonuçlar vermiştir.

V. SONUÇ VE ÖNERİLER

Tez çalışmasında var olan makine öğrenmesi metotlarına ek olarak kendi tasarımımız olan bir yapay sinir ağı geliştirilerek mevcut yöntemlere göre kıyaslaması yapılmak istenmiştir. Yapay sinir ağları temel olarak içerebildikleri çoklu katmanlar ve her katmanda yer alan çoklu nöronlar sayesinde lineer olmayan çözümler üretebilmektedir. Her bir nöronda farklı bir aktivasyon fonksiyonu tercih edilebilir, kullanılan aktivasyon fonksiyonlarının temelde bir makine öğrenmesi yöntemi gibi çalıştığını düşündüğümüzde elde edebileceğimiz sonuçların diğer yöntemlere göre daha başarılı sonuçlar olabileceğini öngörebiliriz. Yapay sinir ağları kullanılarak elde edilen en başarılı tahmin sonucu %62 iken ortalama başarılı tahmin oranı %60,34 seviyesinde kalmıştır. Maksimum başarı oranına göre kıyaslama yapılmak istenildiğide kullanılan eğitim verisi oranlarına göre birinci, tüm eğitim oranlarına göre yöntemler arasında üçüncü olmuştur. Ortalama başarı sıralamasına göre ise tüm yöntemler arasında %20 daha fazla başarı göstererek birinci sırada yer almıştır.

Yapılan çalışamalar sonucunda üretilen sistem Qbit üretimi yapan karşı tarafın verilerini elindeki veriler üzerinden tahmin etmeye çalışmaktadır. Simülasyon ortamında elde edilen bu seviyedeki yüksek başarılar, geliştirilmesi mümkün olma durumunda gerçek sistemlerde test edilmesi ve kullanılması gerekmektedir. Mevcut anahtar dağıtımı protokollerine entegre edilmeli ve performans için tekrar testlerden geçmesi gerekmektedir. Elde edilen yüksek başarı oranları, mevcut sistemin başarı oranları ile kıyaslandığında yapılan çalışmaların literatürün güncel sınırını ilerletici değer taşıdığı düşünülmektedir.

Tezimizin 4. bölümünde yer alan blokzincir teknolojilerinin kuantum teknolojilerine ve kuantum anahtar dağıtımı teknolojilerine entegrasyonu üzerine çalışmalara başlanılmıştır. Teori aşamasında olan bu çalışmalara öneriler 4. bölümde yer alan çalışmalarımızda örnek olarak gösterilebilir. Yakın zamanda sağlayacağı teknik ve ticari getirileri göz önünde bulundurulduğunda

gündelik hayatımızda kullanılabilir ürünlerin çıkacağı bir alan olduğu tahmin edilebilmektedir. Blokzincir sistemlerinin herkese açık ve merkeziyetçi olmayan sistemler olarak tanıtılması, mevcut sistemin belirli bir amaç için özel amaçlar için ve kısıtlı gruplar için kullanılamayacağı anlamına gelmemektedir. Doktora tezimizde önerdiğimiz özel tasarım olan bu sistemde taraflar harici kesimlerin defter içeriklerine erişimi olmayacağından sistemin güvenilirliği fiber kablolar ile aktarım yapılan sisteme yakın olacağı düşünülmektedir. Geliştirilmek istenilen mevcut sistemlerden farkı, kurulacak kapalı blokzincir sisteminin daha uzun mesafelerde veri aktarımını kayıpsız olarak gerçekleştirebilecek olmasıdır. Fiber kablo içeren altyapı sistemlerinde veri kaybı ve dış etmenlerden dolayı artan artık bit değerlerinin böylelikle azaltılması sağlanabilecektir. Doktora tezimizde yapılan iyileştirmeler göz önüne alındığında önerilen blokzincir tabanlı sistem ile gündelik hayatımızda entegrasyonu daha kolay ve hızlı olan bir sistem kolayca kullanıma alınabilecektir.

VI. KAYNAKÇA

MAKALELER

ABUSHGRA, A. A. (2022). "Variations of QKD Protocols Based on Conventional System Measurements: A Literature Review", **Cryptography**, cilt 6, sayı 12.

ADNAN, M. H., AHMAD, Z., HARUN, N. Z. (2022). "Quantum Key Distribution for 5G Networks: A Review, State of Art and Future Directions", **Future Internet**, cilt 14, sayı 73.

AHN, J., KWON, H.-Y., AHN, B., PARK, K., KİM, T., LEE, M.-K., KİM, J., CHUNG, J. (2022). "Toward Quantum Secured Distributed Energy Resources: Adoption of Post-Quantum Cryptography (PQC) and Quantum Key Distribution (QKD)", **Energies**, cilt 15, sayı 714.

AKHTAR, M. M., KHAN, M. Z., AHAD, M. A., NOORWALİ, A., RİZVİ, D. R., CHAKRABORTY, C. (2021). "Distributed ledger technology based robust access control and real-time synchronization for consumer electronics", **PeerJ Computer Science,** cilt 7:e566.

ALİ, A., AHMED, M., KHAN, A., ANJUM, A., ILYAS, M., HELFERT, M. (2021). "VisTAS: blockchain-based visible and trusted remote authentication system", **PeerJ Computer Science**, cilt 7:e516.

ALİEV, H., KİM, H., CHOİ, S. (2020). "A Scalable and Secure Group Key Management Method for Secure V2V Communication", **Sensors**, cilt 20, sayı 6137.

AKLİLU, Y. T., DİNG, J. (2022). "Survey on Blockchain for Smart Grid Management, Control, and Operation", **Energies**, cilt 15, sayı 193.

ALSHOWKAN, M., ELLEİTHY, K., ODEH, A., ABDELFATTAH, E. (2013). "A new algorithm for three-party Quantum key distribution", **Third International Conference on Innovative Computing Technology (INTECH 2013)",** ss. 208-212.

ALVAREZ, R., CABALLERO-GİL, C., SANTONJA, J., ZAMORA, A. (2017). "Algorithms for Lightweight Key Exchange", **Sensors**, cilt 17, sayı 1517.

AMPATZİS, M., ANDRONİKOS, T. (2021). "QKD Based on Symmetric Entangled Bernstein-Vazirani", **Entropy**, cilt 23, sayı 870.

ARMANUZZAMAN, M., ALAM, K. M. R., HASSAN, M. M., MORİMOTO, Y. (2017). "A secure and efficient data transmission technique using quantum key distribution", **4th International Conference on Networking, Systems and Security (NSysS)**, ss. 1-5.

ASİF, M., AZİZ, Z., BİN AHMAD, M., KHALİD, A., WARİS, H. A., GİLANİ, A. (2022). "Blockchain-Based Authentication and Trust Management Mechanism for Smart Cities", **Sensors**, cilt 22, sayı 2604.

AVİS, C., JANG, J. (2022). "Understanding the Origin of the Hysteresis of High-Performance Solution Processed Polycrystalline SnO2 Thin-Film Transistors and Applications to Circuits", **Membranes**, cilt 12, sayı 7.

BELGHAZİ, Z., BENAMAR, N., ADDAİM, A., KERRACHE, C. A. (2019). "Secure WiFi-Direct Using Key Exchange for IoT Device-to-Device Communications in a Smart Environment", **Future Internet**, cilt 11, sayı 251.

BENNETT, C. H. (1992). "Quantum cryptography using any two nonorthogonal states", **Phys. Rev. Lett.**, cilt 68, sayı 3121.

BENNETT, C. H., BRASSARD, G. (1984). "Quantum cryptography: Public key distribution and coin tossing", **Theoretical Computer Science**, cilt 560, sayı 1.

BOAKYE-BOATENG, K., LASHKARİ, A. H. (2019). "Securing GOOSE: The Return of One-Time Pads", **International Carnahan Conference on Security Technology (ICCST)**, ss. 1-8.

BOHR, N. (1928). "The Quantum Postulate and the Recent Development of Atomic Theory1", **Nature**, cilt 121.

CAİ, Z., LİU, S., HAN, Z., WANG, R., HUANG, Y. (2021). "A Quantum Blind Multi-Signature Method for the Industrial Blockchain", **Entropy**, cilt 23, sayı 1520.

CAO, W.-F., ZHEN, Y.-Z., ZHENG, Y.-L., ZHAO, S., XU, F., Lİ, L., CHEN, Z.-B., LİU, N.-L., CHEN, K. (2020). "Open-Destination Measurement-Device-Independent Quantum Key Distribution Network", **Entropy**, cilt 22, sayı 1083.

CHİN, Z. H., YAP, T. T. V., TAN, I. K. T. (2022). "Genetic-Algorithm-Inspired Difficulty Adjustment for Proof-of-Work Blockchains", **Symmetry**, cilt 14, sayı 609.

CARDOSO-ISİDORO, C., DELGADO, F. (2022). "Shared Quantum Key Distribution Based on Asymmetric Double Quantum Teleportation", **Symmetry**, cilt 14, sayı 713.

CHEN, D., LU, W., XİNG, W., WANG, N. (2019). "An Untraceable Data Sharing Scheme in Wireless Sensor Networks", **Sensors**, cilt 19, sayı 114.

CHOİ, E., CHOİ, Y., PARK, N. (2022). "Blockchain-Centered Educational Program Embodies and Advances 2030 Sustainable Development Goals", **Sustainability**, cilt 14, sayı 3761.

CHOUDHARY, K., GABA, G. S., BUTUN, I., KUMAR, P. (2020). "MAKE-IT—A Lightweight Mutual Authentication and Key Exchange Protocol for Industrial Internet of Things", **Sensors**, cilt 20, sayı 5166.

COCHRAN, R. D., GAUTHİER, D. J. (2021). "Qubit-Based Clock Synchronization for QKD Systems Using a Bayesian Approach", **Entropy**, cilt 23, sayı 988.

COLLİNİ, E., WONG, C., WİLK, K., CURMİ, P. M. G., BRUMER, P., SCHOLES, G. D. (2010). "Coherently wired light-harvesting in photosynthetic marine algae at ambient temperature", **Nature**, cilt 463.

CROİTORU, A., ISAR, A. (2022). "Time Evolution of Quantum Coherence of Two Bosonic Modes in Noisy Environments", **J Russ Laser Res**, cilt 43.

DAMİSA, U., NWULU, N. I. (2022). "Blockchain-Based Auctioning for Energy Storage Sharing in a Smart Community", **Energies**, cilt 15, sayı 1954.

EJAZ, A., SHOUKAT, I. A., IQBAL, U., RAUF, A., KANWAL, A. (2021). "A secure key dependent dynamic substitution method for symmetric cryptosystems", **PeerJ Computer Science**, cilt 7:e587.

EKERT, A. K. (1991). "Quantum cryptography based on Bell's theorem", **Phys. Rev. Lett.**, cilt 67, sayı 661.

ENGEL, G., CALHOUN, T., READ, E., AHN, T.-K., MANČAL, T., CHENG, Y.-C., BLANKENSHİP, R. E., FLEMİNG, G. R. (2007). "Evidence for wavelike energy transfer through quantum coherence in photosynthetic systems", **Nature**, cilt 446.

ESCRİBANO PABLOS, J. I., GONZÁLEZ VASCO, M. I., MARRİAGA, M. E., PÉREZ DEL POZO, Á. L. (2020). "Compiled Constructions towards Post-

Quantum Group Key Exchange: A Design from Kyber", **Mathematics**, cilt 8, sayı 1853.

FRİEDMAN, J., PATEL, V., CHEN, W., TOLPYGO, S. K., LUKENS, J. E. (2000). "Quantum superposition of distinct macroscopic states", **Nature**, cilt 406.

FURTAK, J. (2020). "Cryptographic Keys Generating and Renewing System for IoT Network Nodes—A Concept", **Sensors**, cilt 20, sayı 5012.

GATABAZİ, P., KABERA, G., MBA, J. C., PİNDZA, E., MELESSE, S. F. (2022). "Cryptocurrencies and Tokens Lifetime Analysis from 2009 to 2021", **Economies**, cilt 10, sayı 60.

GAO, W., YANG, L., ZHANG, D., LİU, X. (2022). "Quantum Identity-Based Encryption from the Learning with Errors Problem", **Cryptography**, cilt 6, sayı 9.

GOUMİDİ, H., HAROUS, S., ALİOUAT, Z., GUEROUİ, A. M. (2021). "Lightweight Secure Authentication and Key Distribution Scheme for Vehicular Cloud Computing", **Symmetry**, cilt 13, sayı 484.

GOZZARD, D. R., WALSH, S., WEİNHOLD, T. (2021). "Vulnerability of Satellite Quantum Key Distribution to Disruption from Ground-Based Lasers", **Sensors**, cilt 21, sayı 7904.

HORNG, J. H., CHANG, C. C., Lİ, G. L., LEE, W. K., HWANG, S. O. (2021). "Blockchain-Based Reversible Data Hiding for Securing Medical Images", **Journal of Healthcare Engineering**, cilt. 2021.

HUANG, D., LİU, S., ZHANG, L. (2021). "Secure Continuous-Variable Quantum Key Distribution with Machine Learning", **Photonics**, cilt 8, sayı 511.

HUSSEİN, A. F., ALZUBAİDİ, A. K., HABASH, Q. A., JABER, M. M. (2019). "An Adaptive Biomedical Data Managing Scheme Based on the Blockchain Technique", **Applied Sciences**, cilt 9, sayı 2494.

HUSSAİN, M., JAVED, W., HAKEEM, O., YOUSAFZAİ, A., YOUNAS, A., AWAN, M. J., NOBANEE, H., ZAİN, A. M. (2022). "Blockchain-Based IoT Devices in Supply Chain Management: A Systematic Literature Review", **Sustainability**, cilt 13, sayı 13646.

HWANG, T., LEE, K., Lİ, C. (2007). "Provably Secure Three-Party Authenticated Quantum Key Distribution Protocols", **in IEEE Transactions on Dependable and Secure Computing**, cilt 4, sayı 1.

JİNG, F., LİU, W., KONG, L., HE, C. (2021). "Improving the Performance of Continuous-Variable Measurement-Device-Independent Quantum Key Distribution via a Noiseless Linear Amplifier", **Entropy**, cilt 23, sayı 1691.

KİM, M., MOON, J., WON, D., PARK, N. (2020). "Revisit of Password-Authenticated Key Exchange Protocol for Healthcare Support Wireless Communication", **Electronics,** cilt 9, sayı 733.

KO, K.-K., JUNG, E.-S. (2021). "Development of Cybersecurity Technology and Algorithm Based on Quantum Computing", **Appl. Sci.**, cilt 11, sayı 9085.

KWAK, S., LEE, J., KİM, J., OH, H. (2022). "EggBlock: Design and Implementation of Solar Energy Generation and Trading Platform in Edge-Based IoT Systems with Blockchain", **Sensors**, cilt 22, sayı 2410.

LEE, H.-N. (2022). "New Trends in Blockchain Technology", **Applied Science**, cilt 12, sayı 3212.

LEE, D.-H., LEE, I.-Y. (2018). "Dynamic Group Authentication and Key Exchange Scheme Based on Threshold Secret Sharing for IoT Smart Metering Environments", **Sensors**, cilt 18, sayı 3534.

Lİ, Y., WANG, Y., MAO, Y., PENG, W., JİN, D., GUO, Y. (2021). "Continuous-Variable Quantum Key Distribution Based on Heralded Hybrid Linear Amplifier with a Local Local Oscillator", **Entropy**, cilt 23, sayı 1395.

LİANG, H., ZHANG, G., HOU, W., HUANG, P., LİU, B., Lİ, S. (2021). "A Novel Asymmetric Hyperchaotic Image Encryption Scheme Based on Elliptic Curve Cryptography", **Applied Science**, cilt 11, sayı 5691.

LİN, C.-H., HU, G.-H., CHAN, C.-Y., YAN, J.-J. (2021). "Chaos-Based Synchronized Dynamic Keys and Their Application to Image Encryption with an Improved AES Algorithm", **Applied Science**, cilt 11, sayı 1329.

LİN, H.-Y. (2019). "A Novel Dual Authenticated Encryption Scheme Suitable for Social Networking Services", **Applied Science**, cilt 9, sayı 1452.

LİN, T., HUAN, Z., SHİ, Y., YANG, X. (2022). "Implementation of a Smart Contract on a Consortium Blockchain for IoT Applications", **Sustainability**, cilt 14, sayı 3921.

LİU, C., ZHU, C., Lİ, Z., NİE, M., YANG, H., PEİ, C. (2021). "Continuous-Variable Quantum Secret Sharing Based on Thermal Terahertz Sources in Inter-Satellite Wireless Links", **Entropy**, cilt 23, sayı 1223.

LİU, L., WANG, Y., ZHANG, J., YANG, Q. (2019). "A Secure and Efficient Group Key Agreement Scheme for VANET", **Sensors**, cilt 19, sayı 482.

LİZAMA-PEREZ, L.A., LÓPEZ, R., J.M. (2021). "Non-Invertible Public Key Certificates", **Entropy**, cilt 23, sayı 226.

LO, O., BUCHANAN, W.J., SAYEED, S., PAPADOPOULOS, P., PİTROPAKİS, N., CHRYSOULAS, C. (2022). "GLASS: A Citizen-Centric Distributed Data-Sharing Model within an e-Governance Architecture", **Sensors**, cilt 22, sayı 2291.

LU, Y.-F., JİANG, M.-S., WANG, Y., ZHANG, X.-X., LİU, F., ZHOU, C., Lİ, H.-W., TANG, S.-B., WANG, J.-Y., BAO, W.-S. (2021). "Practical Analysis of Sending or Not-Sending Twin-Field Quantum Key Distribution with Frequency Side Channels", **Applied Science**, cilt 11, sayı 9560.

MAİLLOUX, L. O., GRİMAİLA, M. R., HODSON, D. D., ENGLE, R., MCLAUGHLİN, C., BAUMGARTNER, G. (2017). "Modeling, Simulation, and Performance Analysis of Decoy State Enabled Quantum Key Distribution Systems", **Appl. Sci.**, cilt 7, sayı 212.

MAO, H.-K., QİAO, Y.-C., Lİ, Q. (2021). "High-Efficient Syndrome-Based LDPC Reconciliation for Quantum Key Distribution", **Entropy**, sayı 23, cilt 1440.

MAWLOOD HUSSEİN, S., LÓPEZ RAMOS, J. A., ÁLVAREZ BERMEJO, J. A. (2020). "Distributed Key Management to Secure IoT Wireless Sensor Networks in Smart-Agro", **Sensors**, cilt 20, sayı 2242.

MEİDUTE-KAVALİAUSKİENE, I., YAZDİ, A. K., MEHDİABADİ, A. (2022). "Integration of Blockchain Technology and Prioritization of Deployment Barriers in the Blood Supply Chain", **Logistics**, cilt 6, sayı 21.

MELHEM, M. Y., KİSH, L.B. (2019). "A Static-loop-current Attack Against the Kirchhoff-Law-Johnson-Noise (KLJN) Secure Key Exchange System", **Applied Sciences**, cilt 9, sayı 666.

MENG, Y., Lİ, J. (2021). "Data Sharing Mechanism of Sensors and Actuators of Industrial IoT Based on Blockchain-Assisted Identity-Based Cryptography", **Sensors**, cilt 21, sayı 6084.

MESNAGER, S., SINAK, A., YAYLA, O. (2020). "Threshold-Based Post-Quantum Secure Verifiable Multi-Secret Sharing for Distributed Storage Blockchain", **Mathematics**, cilt 8, sayı 2218.

MİHALKOVİCH, A., SAKALAUSKAS, E., LUKSYS, K. (2020). "Key Exchange Protocol Defined over a Non-Commuting Group Based on an NP-Complete Decisional Problem", **Symmetry**, cilt 12, sayı 1389.

MİHARA, T. (2012). "Quantum Steganography Embedded Any Secret Text without Changing the Content of Cover Data, Journal of Quantum Information Science", cilt 2 sayı 1.

MOORE, G. E. (1965). "Cramming more components onto integrated circuits", **Electronics**, cilt 38, sayı 8.

MOR, T., RENNER, R. (1983). "Preface to Special Issue on Quantum Cryptography", **Natural Computing**, cilt 13, sayı 4.

MUDULİ, K., RAUT, R., NARKHEDE, B. E., SHEE, H. (2022). "Blockchain Technology for Enhancing Supply Chain Performance and Reducing the Threats Arising from the COVID-19 Pandemic", **Sustainability**, cilt 14, sayı 3290.

NARESH, V.S., NASRALLA, M.M., REDDİ, S., GARCÍA-MAGARİÑO, I. (2020). "Quantum Diffie–Hellman Extended to Dynamic Quantum Group Key Agreement for e-Healthcare Multi-Agent Systems in Smart Cities", **Sensors**, cilt 20, sayı 3940.

NGUYEN, B. M., DAO, T., DO, B. (2020). "Towards a blockchain-based certificate authentication system in Vietnam", **PeerJ Computer Science**, cilt 6:e266.

PARK, Y.-H., KİM, Y., LEE, S.-O., KO, K. (2021). "Secure Outsourced Blockchain-Based Medical Data Sharing System Using Proxy Re-Encryption", **Applied Science**, cilt 11, sayı 9422.

PEECHARA, R. R., SUCHARİTA, V. (2021). "A chaos theory inspired, asynchronous two-way encryption mechanism for cloud computing", **PeerJ Computer Science**, cilt 7:e628.

PENNİNO, D., PİZZONİA, M., VİTALETTİ, A., ZECCHİNİ, M. (2022). "Blockchain as IoT Economy Enabler: A Review of Architectural Aspects", **J. Sens. Actuator Netw**, cilt 11, sayı 20.

POLAS, M. R. H., KABİR, A. I., SOHEL-UZ-ZAMAN, A. S. M., KARİM, R., TABASH, M. I. (2022). "Blockchain Technology as a Game Changer for Green Innovation: Green Entrepreneurship as a Roadmap to Green Economic Sustainability in Peru", **J. Open Innov. Technol. Mark. Complex**, cilt 8, sayı 62.

PRANTO, T., H., NOMAN, A. A., MAHMUD, A., HAQUE, A. B. (2021). "Blockchain and smart contract for IoT enabled smart agriculture", **PeerJ Computer Science**, cilt 7:e407.

RİVERO-GARCÍA, A., SANTOS-GONZÁLEZ, I., HERNÁNDEZ-GOYA, C., CABALLERO-GİL, P., YUNG, M. (2017). "Patients' Data Management System Protected by Identity-Based Authentication and Key Exchange", **Sensors**, cilt 17, sayı 733.

ROY, S., KHATWANİ, C. (2017). "Cryptanalysis and Improvement of ECC Based Authentication and Key Exchanging Protocols", **Cryptography**, cilt 1, sayı 9.

SANDA, O., PAVLİDİS, M., POLATİDİS, N. (2022). "A Regulatory Readiness Assessment Framework for Blockchain Adoption in Healthcare", **Digital**, cilt 2.

SHAMİR, A. (1979). "How to share a secret, Commun", **ACM**, cilt 22, sayı 11.

SHİH, D.-H., WU, T.-W., SHİH, M.-H., CHEN, G.-W., YEN, D.C. (2022). "Hyperledger Fabric Access Control for Industrial Internet of Things", **Applied Science**, cilt 12, sayı 3125.

STULMAN, A., STULMAN, A. (2019). "Secured by Fluctuating Topology Using the Fluctuating Topology of MANETs to Secure Key Exchange", **Electronics**, cilt 8, sayı 1172.

SUN, S., HUANG, A. (2022). "A Review of Security Evaluation of Practical Quantum Key Distribution System", **Entropy**, cilt 24, sayı 260.

SUN, X., KULİCKİ, P., SOPEK, M. (2021). "Logic Programming with Post-Quantum Cryptographic Primitives for Smart Contract on Quantum-Secured Blockchain", **Entropy**, cilt 23, sayı 1120.

TAKAOĞLU, F., ALSHAHRANİ, A., AJLOUNİ, N., AJLOUNİ, F., AL KASASBAH, B., ÖZYAVAŞ A. (2022). "Robust Nonlinear Non-Referenced Inertial Frame Multi-Stage PID Controller for Symmetrical Structured UAV", **Symmetry**, cilt 14, sayı 689.

TAKAOĞLU, M., ÖZER, Ç., PARLAK, E. (2019). "Blokzinciri Teknolojisi ve Türkiye'deki Muhtemel Uygulanma Alanları", **Uluslararası Doğu Anadolu Fen Mühendislik ve Tasarım Dergisi**, cilt 1, sayı 2.

TAKAOĞLU, M., ÖZYAVAŞ, A., AJLOUNİ, N., ALSHAHRANİ, A., ALKASASBEH, B. (2021). "A Novel and Robust Hybrid Blockchain and Steganography Scheme", **Applied Science**, cilt 11, sayı 10698.

TSAİ, C.-W., YANG, C.-W., LİN, J., CHANG, Y.-C., CHANG, R.-S. (2021). "Quantum Key Distribution Networks: Challenges and Future Research Issues in Security", **Applied Sciences**, cilt 11, sayı 3767.

VARAVALLO, G., CARAGNANO, G., BERTONE, F., VERNETTİ-PROT, L., TERZO, O. (2022). "Traceability Platform Based on Green Blockchain: An Application Case Study in Dairy Supply Chain", **Sustainability**, cilt 14, sayı 3321.

WANG, B., Lİ, Z. (2021). "Healthchain: A Privacy Protection System for Medical Data Based on Blockchain", **Future Internet**, cilt 13, sayı 247.

WANG, J., CHANG, L., CHEN, H., ZHU, Z. (2022). "Networking Feasibility of Quantum Key Distribution Constellation Networks", **Entropy**, cilt 24, sayı 298.

WANG, H., ZHAO, Y., NAG, A. (2019). "Quantum-Key-Distribution (QKD) Networks Enabled by Software-Defined Networks (SDN)", **Applied Science**, cilt 9, sayı 2081.

WANG, P., Lİ, X. (2021). "TEDL: A Text Encryption Method Based on Deep Learning", **Applied Sciences**, cilt 11, sayı 1781.

WANG, X., LİU, W., WU, T., GUO, C., ZHANG, Y., ZHAO, S., DONG, C. (2021). "Free Space Measurement Device Independent Quantum Key Distribution with Modulating Retro-Reflectors under Correlated Turbulent Channel", **Entropy**, cilt 23, sayı 1299.

WANG, Y., FAN, R., LİANG, X., Lİ, P., HEİ, X. (2022). "Trusted Data Storage Architecture for National Infrastructure", **Sensors**, cilt 22, sayı 2318.

WEN, X., Lİ, Q., MAO, H., WEN, X., CHEN, N. (2021). "An Improved Slice Reconciliation Protocol for Continuous-Variable Quantum Key Distribution", **Entropy**, cilt 23, sayı 1317.

WOOTTERS, W. K., ZUREK, W. H. (1982). "A Single Quantum Cannot Be Cloned", **Nature**, cilt 299.

WU, T., PAN, Q., LİN, C., SHİ, L., ZHAO, S., ZHANG, Y., WANG, X., DONG, C. (2021). "Influence of Source Parameters on the Polarization Properties of

Beams for Practical Free-Space Quantum Key Distribution", **Entropy**, cilt 23, sayı 1224.

XİE, J., ZHANG, L., WANG, Y., HUANG, D. (2022). "Deep Neural Network Based Reconciliation for CV-QKD", **Photonics**, cilt 9, sayı 110.

XU, S., Lİ, Y., WANG, Y., MAO, Y., WU, X., GUO, Y. (2021). "Security Analysis of a Passive Continuous-Variable Quantum Key Distribution by Considering Finite-Size Effect", **Entropy**, cilt 23, sayı 1698.

XU, S., Lİ, Y., WANG, Y., MAO, Y., ZUO, Z., RUAN, X., GUO, Y. (2021). "Noiseless Attenuation for Continuous-Variable Quantum Key Distribution over Ground-Satellite Uplink", **Applied Science**, cilt 11, sayı 11289.

YEOM, S., CHOİ, S., CHİ, J., PARK, S. (2021). "Blockchain-Based Employment Contract System Architecture Allowing Encrypted Keyword Searches", **Electronics**, cilt 10, sayı 1086.

YU, B., Lİ, X., ZHAO, H. (2021). "PoW-BC: A PoW Consensus Protocol Based on Block Compression", **KSII Transactions on Internet and Information Systems**, cilt 15, sayı 4.

YUAN, E., WANG, L., CHENG, S., AO, N., GUO, Q. (2020). "A Key Management Scheme Based on Pairing-Free Identity Based Digital Signature Algorithm for Heterogeneous Wireless Sensor Networks", **Sensors**, cilt 20, sayı 1543.

ZENG, G., ZHANG, W. (2000). "Identity verification in quantum key distribution", **Physical Review A**, cilt 61, sayı 022303.

ZHANG, L., ZHANG, Z., WANG, W., JİN, Z., SU, Y., CHEN, H. (2021). "Research on a Covert Communication Model Realized by Using Smart Contracts in Blockchain Environment", **in IEEE Systems Journal**, cilt 16, sayı 2.

ZHANG, S., LİU, J., ZENG, G., ZHANG, C., ZHOU, X., WANG, Q. (2021). "Machine Learning-Assisted Measurement Device-Independent Quantum Key Distribution on Reference Frame Calibration", **Entropy**, cilt 23, sayı 1242.

ZHANG, Q., LİU, Y., YU, X., ZHAO, Y., ZHANG, J. (2022). "Topology-Abstraction-Based Protection Scheme in Quantum Key Distribution Networks with Partially Trusted Relays", **Photonics**, cilt 9, sayı 239.

ZHANG, W. (2019). "Information Conservational Security with "Black Hole" Keypad Compression and Scalable One-Time Pad—An Analytical Quantum

Intelligence Approach to Pre-and Post-Quantum Cryptography", **in IEEE Access**, cilt 913.

ZHENG, Y., SHİ, H., PAN, W., WANG, Q., MAO, J. (2022). "Security Analysis of Continuous-Variable Measurement-Device-Independent Quantum Key Distribution Systems in Complex Communication Environments", **Entropy**, cilt 24, sayı 127.

ZHU, M., HU, M., GUO, B. (2022). "Free-Space QKD with Modulating Retroreflectors Based on the B92 Protocol", **Entropy**, cilt 24, sayı 204.

ZOUGHALİAN, K., MARCHANG, J., GHİTA, B. (2022). "A Blockchain Secured Pharmaceutical Distribution System to Fight Counterfeiting", **Int. J. Environ. Res. Public Health**, cilt 19, sayı 4091.

ÖZGEÇMİŞ

Ad-Soyad **:** Faruk TAKAOĞLU

ÖĞRENİM DURUMU

- **Lisans** **:** İstanbul Aydın Üniversitesi
  Mimarlık-Mühendislik Fakültesi
  Bilgisayar Mühendisliği (İngilizce)
- **Yüksek Lisans** **:** İstanbul Aydın Üniversitesi
  Fen Bilimleri Enstitüsü
  Bilgisayar Mühendisliği

MESLEKİ DENEYİM

2015 - 2016	**İstanbul Aydın Üniversitesi**
2016 - Devam Ediyor	**TÜBİTAK**

Yabancı Diller

İngilizce

TEZDEN TÜRETİLEN YAYINLAR, SUNUMLAR VE PATENTLER

- Takaoğlu, F.; Alshahrani, A.; Ajlouni, N.; Ajlouni, F.; Al Kasasbah, B.; Özyavaş, A. Robust Nonlinear Non-Referenced Inertial Frame Multi-Stage PID Controller for Symmetrical Structured UAV. Symmetry 2022, 14, 689. https://doi.org/10.3390/sym14040689 **(Doktora yayın şartının sağlanması amacıyla Lisansüstü Enstitüsünce tezimizden türetilen yayın olarak kayda alınmıştır.)**