T.C.

ÇANAKKALE ONSEKİZ MART ÜNİVERSİTESİ

LİSANSÜSTÜ EĞİTİM ENSTİTÜSÜ

FİZİK ANABİLİM DALI

KUANTUM TEMELLİ BİLGİ GÜVENLİĞİ

DOKTORA TEZİ

Ercan ÇAĞLAR

Tez Danışmanı

Prof. Dr. İhsan YILMAZ

ÇANAKKALE – 2024

T.C.
ÇANAKKALE ONSEKİZ MART ÜNİVERSİTESİ
LİSANSÜSTÜ EĞİTİM ENSTİTÜSÜ

FİZİK ANABİLİM DALI

KUANTUM TEMELLİ BİLGİ GÜVENLİĞİ

DOKTORA TEZİ

ERCAN ÇAĞLAR

Tez Danışmanı
Prof. Dr. İhsan YILMAZ

ÇANAKKALE – 2024

T.C.
ÇANAKKALE ONSEKİZ MART ÜNİVERSİTESİ
LİSANSÜSTÜ EĞİTİM ENSTİTÜSÜ

Ercan ÇAĞLAR tarafından Prof. Dr. İhsan YILMAZ yönetiminde hazırlanan ve **29/01/2024** tarihinde aşağıdaki jüri karşısında sunulan "**Kuantum Temelli Bilgi Güvenliği**" başlıklı çalışma, Çanakkale Onsekiz Mart Üniversitesi Lisansüstü Eğitim Enstitüsü **Fizik Anabilim Dalı**'nda D**OKTORA TEZİ** olarak oy birliği ile kabul edilmiştir.

Jüri Üyeleri	**İmza**
Prof. Dr. İhsan YILMAZ (Danışman)	……
Prof. Dr. İsmail TARHAN	……
Prof. Dr. Abdulsamet HAŞILOĞLU	……
Doç. Dr. Can AKTAŞ	……
Dr. Öğr. Üyesi Ali AKMAN	……

Tez No : 10607169
Tez Savunma Tarihi : 29/01/2024

……
Prof. Dr. Ahmet Evren ERGİNAL
Enstitü Müdürü

../../2024

ETİK BEYAN

Çanakkale Onsekiz Mart Üniversitesi Lisansüstü Eğitim Enstitüsü Tez Yazım Kuralları'na uygun olarak hazırladığım bu tez çalışmasında; tez içinde sunduğum verileri, bilgileri ve dokümanları akademik ve etik kurallar çerçevesinde elde ettiğimi, tüm bilgi, belge, değerlendirme ve sonuçları bilimsel etik ve ahlak kurallarına uygun olarak sunduğumu, tez çalışmasında yararlandığım eserlerin tümüne uygun atıfta bulunarak kaynak gösterdiğimi, kullanılan verilerde herhangi bir değişiklik yapmadığımı, bu tezde sunduğum çalışmanın özgün olduğunu, bildirir, aksi bir durumda aleyhime doğabilecek tüm hak kayıplarını kabullendiğimi taahhüt ve beyan ederim.

Ercan ÇAĞLAR
29/01/2024

TEŞEKKÜR

Bu tezin gerçekleştirilmesinde, çalışmam boyunca benden bir an olsun yardımlarını esirgemeyen, yeni fikirler bulmak adına ufkumu açan, ülkesine faydalı bir akademisyen olmam için rehberlik eden saygı değer danışman hocam Prof. Dr. İhsan YILMAZ'a, değerli fikirleriyle çalışmama yön verdikleri için tez izleme jürimde yer alan Prof. Dr. İsmail TARHAN ve Doç. Dr. Can AKTAŞ'a, fikirleri ile çalışmalarıma destek olan sevgili dostum Doç. Dr. Engin ŞAHİN'e, doktora eğitimim esnasında bilgi birikimlerini benimle paylaşan Prof. Dr. Hüseyin ÇAVUŞ ve Doç. Dr. Melis ULU DOĞRU'ya, yorum ve yönlendirmeleriyle tezime katkı sunan tezimin juri üyeleri Prof. Dr. Abdulsamet HAŞILOĞLU ve Dr. Öğr. Üyesi Ali AKMAN hocalarıma teşekkürlerimi sunarım.

Çalışmalarım boyunca gerek Türkçe gerekse yabancı dil konusunda desteklerini esirgemeyen kız kardeşim Aysun ERBAŞ'a, hayatımın her evresinde bana destek olan değerli aile üyelerim babam Cemil, annem Şerife ve ağabeyim Cüneyt'e sonsuz teşekkürlerimi sunarım.

Ercan ÇAĞLAR

Çanakkale, Ocak 2024

ÖZET

KUANTUM TEMELLİ BİLGİ GÜVENLİĞİ

Ercan ÇAĞLAR
Çanakkale Onsekiz Mart Üniversitesi
Lisansüstü Eğitim Enstitüsü
Fizik Anabilim Dalı Doktora Tezi
Danışman: Prof. Dr. İhsan YILMAZ
29/01/2024, 75

Bu tez çalışmasında, kuantum hesaplamaya dayalı bir güvenli iletişim yöntemi önerilmiştir. Güvenli iletişim için katılımcıların aynı gizli anahtara sahip olması gerekir. Paylaşılmayan gizli anahtar, yerel olarak katılımcılar tarafından üretilir. Her katılımcının gizli anahtarı oluşturacak kuantum kapıları bilmesi gerekir. Katılımcılardan biri diğerine kuantum takviyeli öğrenme ile kuantum kapıları öğretir. Öğrenme eyleminin güvenliği rotasyon kapısı ile sağlanır. Kuantum durumundaki her kubite farklı açılar kullanılarak rotasyon kapısı uygulanır. Böylece farklı genliklere sahip bir süperpozisyon durumu elde edilir. Bu nedenle iletişimi dinleyen üçüncü bir katılımcı faydalı bir bilgi elde edemez. Kuantum takviyeli öğrenmenin ardından iki hata kontrolü gerçekleştirilir. Farklı seçilen kapılar hata kontrolleri yapılarak sistemden çıkarılır. Bu sayede her iki tarafın da aynı kapılara sahip olması sağlanır. Bundan sonra her iki taraf da aynı anahtarı oluşturacak bilgiye sahip olacaktır. Katılımcılar sahip oldukları bilgileri güvenli bir iletişim yöntemi için kullanırlar. Geliştirilen yöntem daha önce yapılan çalışmalarla karşılaştırılmıştır. Yöntem, IBM Qiskit kullanılarak simüle edildikten sonra simülasyon sonuçları tartışılmıştır. Son olarak da önerilerde bulunulmuştur.

Anahtar Kelimeler: Kuantum Takviyeli Öğrenme, Anahtar Üretimi, Kuantum Anahtar Dağıtımı, Kuantum Kriptografi

ABSTRACT

INFORMATION SECURITY BASED ON FUNDAMENTAL OF QUANTUM

Ercan ÇAĞLAR
Çanakkale Onsekiz Mart University
School of Graduate Studies
Doctoral Dissertation in Physics
Supervisor: Prof. Dr. İhsan YILMAZ
01/29/2024, 75

In this thesis, a secure communication method based on quantum computing is proposed. For secure communication, participants must have the same secret key. The non-shared secret key is generated locally by the participants. Each participant must know the quantum gates that will generate the secret key. One of the participants teaches quantum gates to the other by using quantum reinforcement learning. The safety of the learning action is ensured by the rotation gate. A rotation gate is applied to each qubit in the quantum state by using different angles. Thus, a superposition state with different amplitudes is obtained. Therefore, eavesdropper cannot obtain any useful information. After quantum reinforcement learning, two error checks are performed. The incorrect gates are canceled through error checks. With the error checks, it is ensured that both parties have the same gates. Thus, both parties will have the information to generate the same key. The participants use the information they have for a secure communication method. The method, that was developed, has been compared with previous studies. After the method was simulated by using IBM Qiskit,, the simulation results has been discussed. Finally, suggestions has been made.

Keywords: Quantum Reinforcement Learning, Key Generation, Quantum Key Distribution, Quantum Cryptography

İÇİNDEKİLER

Sayfa No

JURİ ONAY SAYFASI i
ETİK BEYAN ii
TEŞEKKÜR iii
ÖZET iv
ABSTRACT v
İÇİNDEKİLER vi
SİMGELER VE KISALTMALAR viii
TABLOLAR DİZİNİ ix
ŞEKİLLER DİZİNİ x

BİRİNCİ BÖLÜM
GİRİŞ

1.1. Kuantum Mekaniğinin Temelleri 2
1.2. Kuantum Kapılar 4
1.2.1.Birim (Identity) Kapı 7
1.2.2. Pauli X Kapısı 8
1.2.3. CNOT Kapısı 9
1.2.4. Hadamard (H) Kapısı 10
1.2.5. Ry Kapısı 10
1.3. Kuantum Takviyeli Öğrenme 12

İKİNCİ BÖLÜM
ÖNCEKİ ÇALIŞMALAR

2.1. Klasik Yapay Sinir Ağları ile Anahtar Dağıtımı 14
2.2. Kuantum Kriptografi 16
2.2.1. Kuantum Anahtar Dağıtım Protokolleri 16
BB84 Kuantum Anahtar Dağıtımı Protokolü: 17
B92 Kuantum Anahtar Dağıtımı Protokolü: 22

Dolanık Tabanlı Kuantum Anahtar Dağıtımı Protokolleri: 26
Sürekli Değişken Kuantum Anahtar Dağıtımı Protokolleri: 27
Yarı Kuantum Anahtar Dağıtımı Protokolleri: 28
2.2.2. Kuantum Steganografi Çalışmaları 28
2.3. Kuantum Takviyeli Öğrenme Çalışmaları 29

ÜÇÜNCÜ BÖLÜM
MATERYAL VE YÖNTEM

3.1.Kuantum Takviyeli Öğrenme ile Anahtar Üretimi 32
3.1.1. Anahtar Üretimi için Gerekli Kapıların Öğretilmesi 34
3.1.2. Anahtar için Hata Kontrolü 42
Birim (Identity)-NOT Hata Kontrolü: 43
Tarafların CNOT ve Birim/NOT Hata Kontrolü: 48
3.1.3. Anahtar Üretimi 54
3.2. Güvenli İletişim Yöntemi: 55

DÖRDÜNCÜ BÖLÜM
ARAŞTIRMA BULGULARI

4.1. Kuantum Takviyeli Öğrenme ile Anahtar Üretimi Yönteminin Önceki Yöntemlerle Karşılaştırılması 59
4.2. Kuantum Takviyeli Öğrenme ile Anahtar Üretimi Simülasyonu 61

BEŞİNCİ BÖLÜM
SONUÇ VE ÖNERİLER

5.1. Güvenlik Analizi 66
5.2. Kuantum Takviyeli Öğrenme ile Anahtar Üretimi Simülasyon Sonuçları 68
5.3. Sonuçlar 70
KAYNAKÇA 71
EKLER I
EK 1. PATENT BELGESİ II
EK 2. PATENTLE TÜRKİYE 3. ÜNİVERSİTELER PATENT YARIŞMASI ÖDÜL III
ÖZGEÇMİŞ IV

SİMGELER VE KISALTMALAR

$\|\psi\rangle$	Kuantum Durum (Quantum State)
I	Birim Kapı (Identity Gate)
X	Pauli X Kapısı (Pauli X Gate)
Y	Pauli Y Kapısı (Pauli Y Gate)
Z	Pauli Z Operatörü (Pauli Z Gate)
H	Hadamard Kapısı (Hadamard Gate)
$CNOT$	Kontrollü Değil Kapısı (Controlled NOT Gate)
$SWAP$	Değişim Kapısı (SWAP Gate)
$\otimes$	Tensörel Çarpım (Tensor Product)
$\oplus$	Modül ikiye göre toplama (XOR Gate)
KAD	Kuantum Anahtar Dağıtımı (Quantum Key Distribution - QKD)
RSA	Rivest, Shamir ve Adleman Açık Anahtarlı Algoritması (Rivest-Shamir-Adleman Public Key Algorithm)
BB84	Bennett ve Brassard'ın dört durumlu KAD protokolü (Bennett and Brassard's four-state QKD protocol)
B92	Bennett'in iki durumlu KAD protokolü (Bennett's two-state QKD protocol)
E91	Ekert'in dolanık temelli KAD protokolü (Ekert's entanglement based QKD protocol)
BBM92	Bennett, Brassard ve Mermi'in dolanık temelli KAD protokolü (Bennett, Brassard and Mermi's entanglement based QKD protocol)
MKS	Markov Karar Süreci (Markov Decision Process - MDP)
KTÖ	Kuantum Takviyeli Öğrenme (Quantum Reinforcement Learning - QRL)
KFD	Kuantum Fourier Dönüşümü (Quantum Fourier Transform - QFT)

TABLOLAR DİZİNİ

Tablo No	Tablo Adı	Sayfa No
Tablo 1	Bir kubite uygulanan temel kuantum kapılar ve matris gösterimleri……...	5
Tablo 2	İki kubite uygulanan temel kuantum kapılar ve matris gösterimleri……...	5
Tablo 3	Bloch küre üzerinde rotasyon kapıları ve matris gösterimleri…..	6
Tablo 4	Bell Durumları……..	26
Tablo 5	Alice ve Bob'un farklı kapıları seçtiği durumlar……...	42
Tablo 6	Simülasyon sonuçları……	69

ŞEKİLLER DİZİNİ

Şekil No	Şekil Adı	Sayfa No
Şekil 1	Bloch küre……..	4
Şekil 2	Takviyeli Öğrenmede Ajan ve Çevre etkileşimi…….	13
Şekil 3	Eve var olmadığı durumda BB84 protokolünün çalışması…….	19
Şekil 4	Eve'nin var olduğu durumda BB84 protokolünün çalışması……..	20
Şekil 5	Eve var olmadığı durumda B92 protokolünün çalışması……	24
Şekil 6	Eve'nin var olduğu durumda B92 protokolünün çalışması……	25
Şekil 7	Kuantum Takviyeli Öğrenme ile Anahtar Üretimi…….	33
Şekil 8	Anahtarların yerel olarak üretilmesi örneği……	55
Şekil 9	Güvenli İletişim Yöntemi Örneği……..	58
Şekil 10	Simülasyon sonuçlarının grafik gösterimi……..	69

BİRİNCİ BÖLÜM
GİRİŞ

İnsanlık var olduğundan beri bilgi, rakiplerimize karşı üstün olmamızı sağlamıştır. Bu nedenle bilginin güvenli bir şekilde saklanması ve taşınması gerekmektedir. Bilgi teknolojilerinin gelişmesi ile beraber bilgiyi bir yerden başka bir yere transfer etmek kolaylaşmıştır ve bilgi iletimi sırasında güvenliğin önemi artmıştır. Bilginin gizli bir şekilde iletilmesi üzerine yapılan çalışmalar kriptografi olarak adlandırılır.

Bilgi, gönderen ve alıcı adını verdiğimiz iki kullanıcı arasında iletilir. Gönderen, bilgiyi şifreleyerek gönderir. Alıcı, şifreli bilginin şifresini çözerek orijinal bilgiye ulaşır. Şifreleme ve şifre çözme işlemleri için anahtar adı verilen veriye ihtiyacımız vardır. "Gizli anahtar" olarak adlandırdığımız bu anahtarın, kullanıcılar tarafından paylaşılması gerekmektedir. Anahtarın üçüncü bir kullanıcı tarafından ele geçirilmemesi için anahtarın paylaşılması yüksek güvenlik gerektirmektedir. Aynı anahtarın her iletişimde kullanılması, üçüncü bir kullanıcının anahtarı tahmin etmesi için gerekli hesaplamaları yapabileceği verileri elde etmesine neden olabilir. Bu nedenle anahtarın sadece bir kere kullanılması gerekmektedir. Bu durum her iletişim için yeni bir anahtarı gerektirir. Bu anahtarın her defasında güvenli iletilmesinin gerekliliği anahtar dağıtım problemi ortaya çıkmıştır.

Anahtar dağıtım problemi için çözüm yöntemlerinden biri olarak kullanılan RSA algoritması, Rivest vd. (1978) tarafından geliştirilmiştir. Açık anahtarlı kriptografi yöntemi olan RSA algoritmasının geliştirilmesi, geleneksel kriptografi için önemli bir adım olmuştur. RSA algoritmasının güvenliği, büyük sayıların asal çarpanlarına ayrılmasının zorluğuna dayanmaktadır. Shor (1994) algoritması, kuantum teknolojilerinin kullanılması ile büyük sayıların asal çarpanlarının tespit edilebileceğini kanıtlamıştır. Shor'un algoritması, kuantum teknolojilerinin yaygın olarak kullanılır hale gelmesi ile bugün güvenli olarak kabul edilen kriptografi yöntemlerinin işlevini yitireceğini göstermiştir.

İlk olarak Feynman (1982), kuantum mekaniği ilkelerine dayanan bir bilgisayar fikrini ortaya atmıştır. Shor'un algoritmasından önce kuantum mekaniği ilkelerine dayanan güvenlik yöntemleri geliştirilmeye başlanmıştır. Shor'un algoritması, güvenlik yöntemlerini geliştirmek için kuantum teknolojilerinin kullanılmasının gerekliliğini ortaya

koymuştur. Kuantum mekaniği ilkelerine dayanan ilk Kuantum Anahtar Dağıtımı (KAD - Quantum Key Distribution - QKD) protokolü olan BB84, Bennett ve Brassard (1984) tarafından önerilmiştir. Bennett (1992), dört durum kullanan BB84 protokolüne alternatif olarak ortogonal olmayan iki durumu kullanan B92 protokolünü geliştirmiştir. İlk kuantum dolanık tabanlı KAD olan E91, Ekert (1991) tarafından önerilmiştir. Bennett vd. (1992), kuantum dolanıklık temelli BBM92 protokolünü geliştirmişlerdir. Günümüze kadar birçok araştırmacı, kuantum mekaniği ilkelerini kullanarak anahtar dağıtımı için çeşitli yöntemler geliştirmişlerdir.

KAD sistemlerinde temel amaç bir kullanıcıdan diğer kullanıcıya anahtar bilgisini güvenli bir şekilde iletmektir. Güvenlik zafiyetine neden olan konu, gönderme işleminin nasıl yapıldığıdır. Bu tez çalışmasında anahtar bilgisini göndermek yerine, anahtarın her iki kullanıcı tarafından yerel olarak oluşturulmasını sağlayan bir model geliştirilmiştir. Anahtarlar, yerel olarak Identity, NOT ve CNOT kapıları kullanılarak oluşturulmaktadır. Her iki kullanıcının hangi kubite hangi kapının uygulanacağını bilmesi gerekmektedir. Bu nedenle taraflardan biri diğerine, kullanılacak olan kapıları öğretmektedir. Öğrenme eylemini Kuantum Takviyeli Öğrenme(KTÖ - Quantum Reinforcement Learning - QRL) kullanılarak gerçekleştirilmektedir.

Tezin birinci bölümünde kuantum mekaniğinin temellerinden, kuantum kapılardan ve kuantum takviyeli öğrenmeden bahsedilmiştir. İkinci bölümde kuantum kriptografi, kuantum takviyeli öğrenme ve yapay sinir ağları ile anahtar dağıtımına ilişkin daha önceki çalışmalar incelenmiştir. Üçüncü bölümde yerel olarak aynı gizli anahtarın üretilebilmesi için kuantum takviyeli öğrenme ile anahtar üretimi modeli ortaya konmuştur. Ayrıca bu bölümde önerilen modeli kullanan bir güvenli iletişim yöntemi sunulmuştur. Dördüncü bölümde geliştirilen model daha önceki çalışmalar ile kıyaslanmış ve sözde kod olarak sunulmuştur. Beşinci bölümde ise güvenlik ve simülasyon sonuçlarının analizi yapılarak sonuç ve önerilerde bulunulmuştur.

1.1. Kuantum Mekaniğinin Temelleri

Yaşamış olduğumuz dünyada büyük nesneler arasında olan etkileşim, olaylar ve benzeri durumlar “Klasik Mekanik” diğer bir deyişle “Klasik Fizik” ile açıklanır. 20.

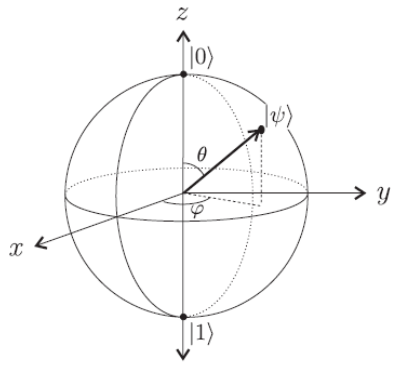
yüzyılın ilk yarısında, bilim adamları klasik mekaniğin siyah cisim ışıması, fotoelektrik gibi doğa olaylarını yani atom altı parçacıkların davranışlarını açıklamakta yetersiz olduğunu farketmiştir. Bu durum bilim insanlarını yeni teorik modellerin arayışına itmiştir. Açıklanamayan doğa olaylarını anlamlandırmak için yapılan çalışmaların sonunda, atom altı parçacıkların davranışlarını inceleyen "Kuantum Mekaniği" ya da "Kuantum Fiziği" adını verdiğimiz yeni bir fizik dalı ortaya çıkmıştır (Ural, 2021: 15).

Kuantum mekaniği çalışmalarının bilişim teknolojiler üzerinde de etkileri olmuştur. İlk kuantum bilgisayar fikrinin ortaya atılmasıyla süperpozisyon, dolanıklık, teleportasyon, süperyoğun kodlama, terslenebilirlik, kopyalanamama teoremi, dolanıklık transferi gibi kuantum teknolojilerinin üstünlükleri ortaya çıkmıştır. İkili bilgi bağlamında bir kuantum durumun temel bazları olan $|0\rangle$ ve $|1\rangle$ değerlerini aynı anda içermesi durumuna "Süperpozisyon" denilmektedir. Başlangıçta bazı özellikleri ilişkili olan ikili veya daha çoklu sistemlerin mesafeden bağımsız olarak başlangıçtaki ilişki durumlarının geçerli olması "Dolanıklık" olarak adlandırılır. İkili veya çoklu dolanık durumlar kullanılarak, kuantum bilgi ışık hızında gönderilebilme işlemine "Işınlama (teleportasyon)" denilmektedir. Klasik iki bitten oluşan verimizin tek bir dolanık kubit kullanılarak gönderildiği iletişim tekniğine "Süperyoğun Kodlama" ismi verilmektedir. Bir kuantum duruma aynı operatörün arka arkaya iki kere uygulanması sonucu başlangıç kuantum durumunun elde edilmesine "Terslenebilirlik" denilmektedir. Bir kuantum durumun, temel bazlardaki genliklerinin aynı değeri içerdiği bağımsız bir kopyasının oluşturulamaması "Kopyalanamama Teoremi" olarak adlandırılır. Kuantum durumların kopyalanamaması güvenlik yöntemi olarak KAD protokollerinin ortaya atılmasındaki en büyük etkenlerden birisidir. Üç veya daha fazla sistemin kendi aralarındaki dolanıkları kullanarak, sistemlerin bütününün dolanık hale getirilmesi işlemine "Dolanıklık Transferi" adı verilmektedir (Şahin,2019).

Klasik bilgisayar teknolojilerinde, bir veriyi temsil etmek için bit olarak adlandırılan 0 ya da 1 değerleri kullanılmaktadır. Bir bit, kesin olarak 0 ya da 1 değerine sahiptir. Kuantum teknolojilerinde ise bit yerine kubit kavramı kullanılmaktadır. Bir kubit, 0 ya da 1 değerini alabildiği gibi hem 0 hem de 1 değerini aynı anda içerebilir. Her iki değeri aynı anda içeren bu durum, "Kuantum Süperpozisyon" olarak adlandırılır. Bir kuantum bilgi durumu (kubit) temel bazlar cinsinden $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ şeklinde temsil

edilir ve bu temsilde dirac gösterimi (bra-ket) kullanılmaktadır. Burada $\alpha\ ve\ \beta$ genlik olarak adlandırılır ve genliklerin kareleri toplamı 1 olmalıdır ($\alpha^2 + \beta^2 = 1$). Genliklerin her ikiside sıfırdan farklı bir değere sahip ise kuantum durumumuz süperpozisyon durumundadır ve ölçüm sonucuna göre 0 ya da 1 değerinden birisi elde edilir. Hangi değerin elde edileceği belirsizdir. Bir kuantum durum süperpozsiyon durumunda değil ise genliğin biri 0 değerine sahip olduğunda diğeri mutlaka 1 değerine sahiptir. $|0\rangle$ ya da $|1\rangle$ temel bazlarından hangisinin genliği 1 ise kuantum durumu için genliği 1 olan duruma çökmüş denir ve ölçüm sonucunda %100 olarak o değeri verir. Örneğin $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ kuantum durumu için $\alpha = 1$ ve $\beta = 0$ değerine sahip ise ölçüm sonucu 0 olur ve $|0\rangle$ durumuna çöktüğü söylenir.

Süperiletkenler, ışığın polarizasyon durumları, atom altı parçacıkların spinleri ve enerji seviyeleri gibi fiziksel olgular ile kuantum durumlar temsil edilebilir. Bu tez çalışmasında, bir kuantum durum Bloch kürenin merkezinden yüzeyine giden bir birim vektör olarak temsil edilmektedir. Bloch kürenin kuzey kutbu, $|0\rangle$ yani spin yukarı ↑ denilen durum ile temsil edilir. Matris gösterimi ise $\begin{bmatrix}1\\0\end{bmatrix}$ şeklindedir. Bloch kürenin güney kutbu ise, $|1\rangle$ yani spin aşağı ↓ denilen durum ile temsil edilir. Matris gösterimi ise $\begin{bmatrix}0\\1\end{bmatrix}$ şeklindedir. Bloch küre Şekil 1'de gösterilmiştir.



Şekil 1. Bloch küre (Kaye vd., 2007)

1.2. Kuantum Kapılar

Klasik bilgisayarlarda bitler üzerinde işlem yapabilmek için mantık kapıları kullanılır. Kuantum bilgisayarlarda ise işlemleri gerçekleştirmek için kubitler üzerine kuantum kapılar uygulanır. Temel kapılar kullanılarak yeni kapılar üretilebilir. Tablo 1'de

bir kubitlik kuantum duruma uygulanan temel kuantum kapılar gösterilmiştir. Bir kubitlik kuantum durum $|0\rangle$ ya da $|1\rangle$ temel bazlarından biridir. Uygulanan kapı, kuantum durumun değerini değiştirebildiği gibi aynı kalmasını da sağlayabilir.

Tablo 1

Bir kubite uygulanan temel kuantum kapılar ve matris gösterimleri (Kaye vd., 2007; Nielsen ve Chuang, 2010; Şahin, 2019)

Kuantum Temel Kapı	Matris Gösterimi
Birim *I*	$I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$
Pauli *X*	$X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$
Pauli *Y*	$Y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}$
Pauli *Z*	$Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$
Hadamard	$H = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$
Genel Faz Kapısı	$S = \begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix}$
R_k Kapısı	$R_k = \begin{bmatrix} 1 & 0 \\ 0 & e^{2\pi i/2^k} \end{bmatrix}$

Tablo 2'de iki kubitlik kuantum duruma uygulanan temel kuantum kapılar gösterilmiştir. İki kubitlik kuantum durum, $|00\rangle, |01\rangle, |10\rangle$ ya da $|11\rangle$ durumlarından biridir. Kontrollü NOT kapısıda denen CNOT kapısı, birinci kubitin 1 değerine sahip olması halinde ikinci kubite NOT kapısını uygular. SWAP kapısı ise birinci ve ikinci kubitin yer değiştirmesini sağlar.

Tablo 2

İki kubite uygulanan temel kuantum kapılar ve matris gösterimleri (Kaye vd., 2007; Nielsen ve Chuang, 2010; Şahin, 2019)

Kuantum Temel Kapı	Matris Gösterimi
Kontrollü X	$CNOT = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$
SWAP Yer Değiştirme	$SWAP = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$

Tablo 3'de rotasyon kapıları gösterilmiştir. Rotasyon kapısı, bloch küre üzerinde temsil edilen bir kuantum duruma uygulandığında x, y ya da z ekseninde döndürülmesini sağlar.

Tablo 3

Bloch küre üzerinde rotasyon kapıları ve matris gösterimleri (Kaye vd., 2007; Nielsen ve Chuang, 2010; Şahin, 2019)

Kuantum Temel Kapı	**Matris Gösterimi**
$\boldsymbol{R_x}$ **operatörü** $\boldsymbol{X}$ **ekseni**	$R_x(\theta) = \begin{bmatrix} \cos\frac{\theta}{2} & -i\sin\frac{\theta}{2} \\ -i\sin\frac{\theta}{2} & \cos\frac{\theta}{2} \end{bmatrix}$
$\boldsymbol{R_y}$ **operatörü** $\boldsymbol{Y}$ **ekseni**	$R_y(\theta) = \begin{bmatrix} \cos\frac{\theta}{2} & -\sin\frac{\theta}{2} \\ \sin\frac{\theta}{2} & \cos\frac{\theta}{2} \end{bmatrix}$
$\boldsymbol{R_z}$ **operatörü** $\boldsymbol{Z}$ **ekseni**	$R_z(\theta) = \begin{bmatrix} e^{-i\frac{\theta}{2}} & 0 \\ 0 & e^{-i\frac{\theta}{2}} \end{bmatrix}$

Kuantum durumlar üzerine uygulanan tüm kapılar birimseldir. Bir kuantum duruma, herhangi bir kuantum kapının arka arkaya iki kere uygulanmasıyla kuantum durumun başlangıç değeri elde edilir. Bu durum kuantum kapının terslenebilir olduğunu gösterir. Bir kuantum kapının matris formunun hermitik eşleniği ile kendisinin çarpımı sonucunda birim matrisi elde edilmesi kuantum kapının birimsel olduğunu gösterir. Örneğin Y kapısının birimselliği aşağıdaki şekilde gösterilebilir.

$$Y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}$$

Y kapısına ait matrisin hermitik eşleniğini bulmak için eşlenik matrisin transpozesi elde edilir. Y kapısına ait eşlenik matris;

$$Y^* = \begin{bmatrix} 0 & i \\ -i & 0 \end{bmatrix}$$

şeklinde olur. Yukarıdaki matrisin transpozesi ise;

$$Y^{\dagger} = (Y^{*})^{T} = \left(\begin{bmatrix} 0 & i \\ -i & 0 \end{bmatrix}\right)^{T} = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}$$

olacaktır. Y ve $Y^{\dagger}$ matrisleri çarpılarak Y kapısının birimsel olduğu ispatlanır.

$$Y.Y^{\dagger} = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}\begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix} = \begin{bmatrix} -i^{2} & 0 \\ 0 & -i^{2} \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

Y ve $Y^{\dagger}$ matrislerini çarpımı sonucunda birimsel matrsi elde edildiği için Y kapısı birimseldir. Y kapısının terslenebilir olduğu aşağıdaki gibi gösterilir:

$$Y|0\rangle = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}\begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 0 \\ i \end{bmatrix} = i\begin{bmatrix} 0 \\ 1 \end{bmatrix} = i|1\rangle$$

$|0\rangle$ kuantum durumuna Y kapısı uygulandığı zaman $i|1\rangle$ durumunu elde edilir. $i|1\rangle$ durumuna Y kapısının uygulanması aşağıdaki gibi gösterilir:

$$Yi|1\rangle = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}\begin{bmatrix} 0 \\ i \end{bmatrix} = \begin{bmatrix} -i^{2} \\ 0 \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \end{bmatrix} = |0\rangle$$

Y kapısı birimsel olduğundan $|0\rangle$ durumuna arka arkaya iki Y kapısı uygulandığında tekrar $|0\rangle$ durumu elde edilir.

1.2.1.Birim (Identity) Kapı

Birim kapı I ile gösterilmektedir. Herhangi bir kuantum duruma uygulandığı zaman kuantum durum üzerinde herhangi bir değişiklik meydana getirmez. Matris gösterimi aşağıdaki gibidir:

$$I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

$|0\rangle$ ve $|1\rangle$ kuantum durumlarına I kapısını uygulanması aşağıdaki gibidir:

$$I|0\rangle = \begin{bmatrix}1 & 0\\ 0 & 1\end{bmatrix}\begin{bmatrix}1\\ 0\end{bmatrix} = \begin{bmatrix}1\\ 0\end{bmatrix} = |0\rangle$$

$$I|1\rangle = \begin{bmatrix}1 & 0\\ 0 & 1\end{bmatrix}\begin{bmatrix}0\\ 1\end{bmatrix} = \begin{bmatrix}0\\ 1\end{bmatrix} = |1\rangle$$

Kuantum durumlar baz durum olmak zorunda değildir. Süperpozisyon olarak adlandırılan $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ durumunda da olabilirler. Süperpozisyon durumuna I kapısının uygulanması aşağıdaki gibidir:

$$I|\psi\rangle = I\alpha|0\rangle + I\beta|1\rangle = \alpha\begin{bmatrix}1 & 0\\ 0 & 1\end{bmatrix}\begin{bmatrix}1\\ 0\end{bmatrix} + \beta\begin{bmatrix}1 & 0\\ 0 & 1\end{bmatrix}\begin{bmatrix}0\\ 1\end{bmatrix}$$
$$= \alpha\begin{bmatrix}1\\ 0\end{bmatrix} + \beta\begin{bmatrix}0\\ 1\end{bmatrix} = \alpha|0\rangle + \beta|1\rangle$$

1.2.2. Pauli *X* Kapısı

NOT kapısı olarak da adlandırılan Pauli X kapısı, uygulandığı kuantum durumun değilinin elde edilmesini sağlar. X ile gösterilmektedir. Matris gösterimi aşağıdaki gibidir:

$$X = \begin{bmatrix}0 & 1\\ 1 & 0\end{bmatrix}$$

$|0\rangle$ ve $|1\rangle$ kuantum durumlarına X kapısının uygulanması aşağıdaki gibidir:

$$X|0\rangle = \begin{bmatrix}0 & 1\\ 1 & 0\end{bmatrix}\begin{bmatrix}1\\ 0\end{bmatrix} = \begin{bmatrix}0\\ 1\end{bmatrix} = |1\rangle$$
$$X|1\rangle = \begin{bmatrix}0 & 1\\ 1 & 0\end{bmatrix}\begin{bmatrix}0\\ 1\end{bmatrix} = \begin{bmatrix}1\\ 0\end{bmatrix} = |0\rangle$$

Süperpozisyon durumundaki $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ kuantum durumuna X kapısının uygulanması aşağıdaki gibidir:

$$|\psi'\rangle = X|\psi\rangle = X\alpha|0\rangle + X\beta|1\rangle = \alpha\begin{bmatrix}0 & 1\\ 1 & 0\end{bmatrix}\begin{bmatrix}1\\ 0\end{bmatrix} + \beta\begin{bmatrix}0 & 1\\ 1 & 0\end{bmatrix}\begin{bmatrix}0\\ 1\end{bmatrix} = \alpha\begin{bmatrix}0\\ 1\end{bmatrix} + \beta\begin{bmatrix}1\\ 0\end{bmatrix}$$
$$= \alpha|1\rangle + \beta|0\rangle$$

$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ kuantum durumuna, X kapısı uyugulandıktan sonra $|0\rangle$ ve $|1\rangle$ baz durumlarının genlikleri değişir. Yani kuantum durumun değili elde edilmiş olur. Kuantum temel kapılar terslenebilir olduğuna göre $|\psi'\rangle = \alpha|1\rangle + \beta|0\rangle$ kuantum durumuna, X kapısı uygulandığı zaman başlangıç durumu $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ kuantum durumunun elde edileceği aşağıda gösterilmiştir:

$$|\psi\rangle = X|\psi'\rangle = X\alpha|1\rangle + X\beta|0\rangle = \alpha\begin{bmatrix}0 & 1\\ 1 & 0\end{bmatrix}\begin{bmatrix}0\\1\end{bmatrix} + \beta\begin{bmatrix}0 & 1\\ 1 & 0\end{bmatrix}\begin{bmatrix}1\\0\end{bmatrix} = \alpha\begin{bmatrix}1\\0\end{bmatrix} + \beta\begin{bmatrix}0\\1\end{bmatrix}$$
$$= \alpha|0\rangle + \beta|1\rangle$$

1.2.3. CNOT Kapısı

İki kubit üzerine uygulanan bir kapıdır. Kontrollü X ya da Kontrollü NOT olarak da adlandırılır. İlk kubit kontrol kubiti, ikinci kubit ise hedef kubit olarak adlandırılır. Kontrol kubitinin $|1\rangle$ değerine sahip olması durumda hedef kubite X kapısı uygulanır. Kontrol kubiti $|0\rangle$ değerine sahip ise hedef kubite bir etkisi bulunmamaktadır. $CNOT$ kapısının matris gösterimi aşağıdaki gibidir:

$$CNOT = \begin{bmatrix}1 & 0 & 0 & 0\\ 0 & 1 & 0 & 0\\ 0 & 0 & 0 & 1\\ 0 & 0 & 1 & 0\end{bmatrix}$$

İki kubitlik bir kuantum duruma $CNOT$ kapısının uygulanmasının genel gösterimi aşağıdaki gibidir:

$$CNOT|\psi\rangle = CNOT|a\rangle|b\rangle = |a\rangle|b + a\rangle$$

İki kubitlik olası tüm kuantum durumlara $CNOT$ kapısının uygulanması aşağıdaki gibidir:

$$CNOT|0\rangle|0\rangle = |0\rangle|0 \oplus 0\rangle = |0\rangle|0\rangle$$
$$CNOT|0\rangle|1\rangle = |0\rangle|1 \oplus 0\rangle = |0\rangle|1\rangle$$
$$CNOT|1\rangle|0\rangle = |1\rangle|0 \oplus 1\rangle = |1|1\rangle$$
$$CNOT|1\rangle|1\rangle = |1\rangle|1 \oplus 1\rangle = |1\rangle|0\rangle$$

Yukarıda görüldüğü üzere kontrol kubitinin $|0\rangle$ olduğu durumda hedef kubitte bir değişiklik olmamıştır. Kontrol kubitinin $|1\rangle$ olduğu durumda ise hedef kubitin değili alınmıştır.

1.2.4. Hadamard (H) Kapısı

Hadamard kapısının matris gösterimi, $|0\rangle$ ve $|1\rangle$ temel bazlarına uygulanması aşağıda gösterildiği gibidir:

$$H = \frac{1}{\sqrt{2}}\begin{bmatrix}1 & 1\\ 1 & -1\end{bmatrix}$$

$$|\psi_0^H\rangle = H|0\rangle = \frac{1}{\sqrt{2}}\begin{bmatrix}1 & 1\\ 1 & -1\end{bmatrix}\begin{bmatrix}1\\ 0\end{bmatrix} = \frac{1}{\sqrt{2}}\begin{bmatrix}1\\ 1\end{bmatrix} = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$$

$$|\psi_1^H\rangle = H|1\rangle = \frac{1}{\sqrt{2}}\begin{bmatrix}1 & 1\\ 1 & -1\end{bmatrix}\begin{bmatrix}0\\ 1\end{bmatrix} = \frac{1}{\sqrt{2}}\begin{bmatrix}1\\ -1\end{bmatrix} = \frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle$$

1.2.5. R_y Kapısı

Rotasyon kapısı, Bloch küre üzerindeki bir vektörü x, y, z ekseninden birine göre belirli bir açıyla döndürme eylemini gerçekleştirmektedir. Bu tez çalışmasında y eksenine göre döndürme eylemini gerçekleştiren R_y kapısı kullanılmaktadır. θ açısı ile uygulanacak R_y kapısının matris formu aşağıda gösterildiği gibidir:

$$R_y(\theta) = \begin{bmatrix}\cos\frac{\theta}{2} & -\sin\frac{\theta}{2}\\ \sin\frac{\theta}{2} & \cos\frac{\theta}{2}\end{bmatrix}$$

R_y kapısı, $|0\rangle$ ya da $|1\rangle$ değerine sahip bir kubite uygulandığı zaman kuantum durum süperpozisyon durumuna gelecektir. R_y kapısının, θ açısı ile $|0\rangle$ ve $|1\rangle$ temel bazlarına uygulanması aşağıda gösterildiği gibidir:

$$|\psi_0\rangle = R_y(\theta)|0\rangle = \begin{bmatrix}\cos\frac{\theta}{2} & -\sin\frac{\theta}{2}\\ \sin\frac{\theta}{2} & \cos\frac{\theta}{2}\end{bmatrix}\begin{bmatrix}1\\ 0\end{bmatrix} = \begin{bmatrix}\cos\frac{\theta}{2}\\ \sin\frac{\theta}{2}\end{bmatrix} = \cos\frac{\theta}{2}|0\rangle + \sin\frac{\theta}{2}|1\rangle \qquad (1.1)$$

$$|\psi_1\rangle = R_y(\theta)|1\rangle = \begin{bmatrix} \cos\frac{\theta}{2} & -\sin\frac{\theta}{2} \\ \sin\frac{\theta}{2} & \cos\frac{\theta}{2} \end{bmatrix} \begin{bmatrix} 0 \\ 1 \end{bmatrix} = \begin{bmatrix} -\sin\frac{\theta}{2} \\ \cos\frac{\theta}{2} \end{bmatrix} = -\sin\frac{\theta}{2}|0\rangle + \cos\frac{\theta}{2}|1\rangle \qquad (1.2)$$

Denklem 1.1'de elde edilen süperpozisyon durumundaki $|\psi_0\rangle$ kuantum durumunu tekrar temel baz $|0\rangle$ durumuna döndürebilmek için R_y kapısının $-\theta$ ile uygulanması gerekmektedir. Bu sayede Bloch küre üzerindeki vektörümüz temel baz $|0\rangle$'ın temsil edildiği kuzey kutbuna konumlanacaktır. $-\theta$ açısı ile uygulanacak R_y kapısının matris formu aşağıda gösterildiği gibidir.

$$R_y(-\theta) = \begin{bmatrix} \cos\frac{\theta}{2} & \sin\frac{\theta}{2} \\ -\sin\frac{\theta}{2} & \cos\frac{\theta}{2} \end{bmatrix}$$

R_y kapısının, $-\theta$ açısı ile $|\psi_0\rangle$ kuantum durumuna uygulanması aşağıda gösterildiği gibidir:

$$R_y(-\theta)|\psi_0\rangle = R_y(-\theta)\left(\cos\frac{\theta}{2}|0\rangle + \sin\frac{\theta}{2}|1\rangle\right) = \begin{bmatrix} \cos\frac{\theta}{2} & \sin\frac{\theta}{2} \\ -\sin\frac{\theta}{2} & \cos\frac{\theta}{2} \end{bmatrix} \begin{bmatrix} \cos\frac{\theta}{2} \\ \sin\frac{\theta}{2} \end{bmatrix}$$
$$= \begin{bmatrix} \cos^2\frac{\theta}{2} + \sin^2\frac{\theta}{2} \\ -\sin\frac{\theta}{2}\cos\frac{\theta}{2} + \cos\frac{\theta}{2}\sin\frac{\theta}{2} \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \end{bmatrix} = |0\rangle \qquad (1.3)$$

Denklem 1.2'de elde edilen süperpozisyon durumundaki $|\psi_1\rangle$ kuantum durumunu tekrar temel baz $|1\rangle$ durumuna döndürebilmek için R_y kapısının $-\theta$ ile uygulanması gerekmektedir. Bu sayede Bloch küre üzerindeki vektörümüz temel baz $|1\rangle$'ın temsil edildiği guney kutbuna konumlanacaktır. R_y kapısının, $-\theta$ açısı ile $|\psi_1\rangle$ kuantum durumuna uygulanması aşağıda gösterildiği gibidir:

$$R_y(-\theta)|\psi_1\rangle = R_y(-\theta)\left(-\sin\frac{\theta}{2}|0\rangle + \cos\frac{\theta}{2}|1\rangle\right) = \begin{bmatrix} \cos\frac{\theta}{2} & \sin\frac{\theta}{2} \\ -\sin\frac{\theta}{2} & \cos\frac{\theta}{2} \end{bmatrix} \begin{bmatrix} -\sin\frac{\theta}{2} \\ \cos\frac{\theta}{2} \end{bmatrix} \qquad (1.4)$$

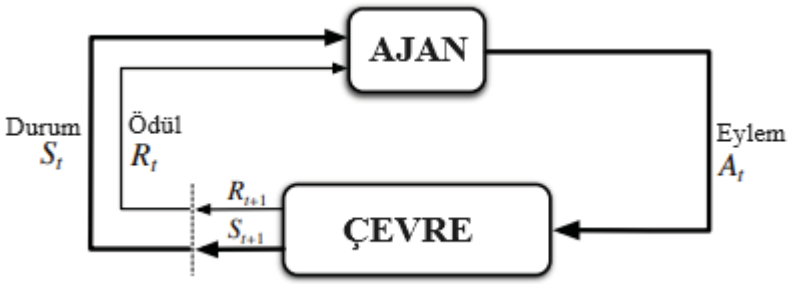
$$= \begin{bmatrix} -\cos\frac{\theta}{2}\sin\frac{\theta}{2} + \sin\frac{\theta}{2}\cos\frac{\theta}{2} \\ \sin^2\frac{\theta}{2} + \cos^2\frac{\theta}{2} \end{bmatrix} = \begin{bmatrix} 0 \\ 1 \end{bmatrix} = |1\rangle$$

Denklem 1.1 ve Denklem 1.2'de R_y kapısı kullanılarak temel bazlar, θ açısı ile döndürülerek süperpozisyon durumuna getirilir. Denklem 1.3 ve Denklem 1.4'de R_y kapısı kullanılarak süperpozisyon durumu, $-\theta$ açısı ile döndürülerek temel bazlar durumuna getirilir. Birçok akademik çalışmada bir kuantum durumu süperpozisyon durumuna getirmek için Hadamard kapısı uygulanır. Hadamard kapısı ile eşit genliklere sahip süperpozisyon durumu elde edilir. Ölçüm sonucu %50 olasılıkla 0 ve %50 olasılıkla 1 olacaktır. Kuantum duruma Hadamard kapısı uygulandığı biliniyorsa tekrar Hadamard kapısı uygulanarak başlangıç durumu elde edilebilir. Güvenli iletişim gözönüne alındığında Hadamard kapısı ile süperpozisyon durumuna getirilen bir kuantum durum, araya girip iletişimi dinleyen üçüncü tarafın eline geçebilir. Bu tez çalışmasında geliştirilen yöntemde bir kuantum durumu süperpozisyon durumuna getirmek için R_y kapısı kullanılmaktadır. Kullanılan açı sadece süperpozisyon durumunu oluşturan kullanıcı tarafından bilindiği için kuantum durumun başlangıç halini kimse elde edemez.

1.3. Kuantum Takviyeli Öğrenme

Bu tez çalışmasının diğer bir boyutu makine öğrenmenin bir türü olan takviyeli öğrenmedir. Öğrenme yöntemleri denetimli, denetimsiz ve takviyeli öğrenme olarak sınıflandırılır. Denetimli öğrenmede girdi ve çıktı verileri kullanılırken denetimsiz öğrenmede sadece girdi verileri kullanılır. Takviyeli öğrenme ise girdi-çıktı çiftlerini değerlendirmek için ödül olarak adlandırılan bir skaler değer kullanır (Dong vd., 2008).

Takviyeli öğrenme modelinde amaç, çevresi ile sahip olduğu etkileşimlere dayanarak performansını artıran bir sistem geliştirmektir. Bu performans artışı bir ödül ceza sistemine dayanır (Uğuz, 2019: 77). Ajan, t anındaki çevrenin durumu S_t'yi gözlemler ve A_t eylemini seçer. Daha sonra yaptığı seçimin ne kadar iyi olduğuna bağlı olarak bir R_t ödülü alır (Şekil 2). Öğrenme eyleminin performansı Markov Karar Sürecine (MKS - Markov Decision Process - MDP) dayanmaktadır.



Şekil 2 Takviyeli Öğrenmede Ajan ve Çevre etkileşimi (Uğuz, 2019: 78).

MKS beş faktörden oluşur: $\{S, A_{(i)}, p_{ij}(a), r_{(i,a)}, V, i, j \in S, a \in A_{(i)}\}$ burada: S, durum uzayıdır; $A_{(i)}$, i durumu için eylem uzayıdır; $p_{ij}(a)$, i durumundan j durumuna a eylemi ile geçiş olasılığıdır; r bir ödül fonksiyonudur, $r: \Gamma \rightarrow (-\infty, +\infty)$ burada $\Gamma = \{(i,a)|i \in S, a \in A_{(i)}\}$; V bir kriter fonksiyonu veya amaç fonksiyonudur (Dong vd., 2008). MKS, birbirini takip eden karar ve durumlardan oluşmaktadır. Takviyeli öğrenmenin başarılı olup olmadığı MKS'ye göre belirlenir. Günümüzde takviyeli öğrenme daha çok bir oyundaki en iyi hamleyi belirleme ya da robotik uygulamalarda kullanılmaktadır.

Bir KTÖ sistemi, MKS'deki faktörlerin Kuantum Mekaniği ile temsil edilmesi sonucu oluşur. Bu tez çalışmasında, MKS'ye göre S durum uzayı 2 kubit ile, A eylem uzayı $\{I, X, CNOT\}$ kapılarıyla, r ödül fonksiyonu $\{0,1\}$ ile temsil edilir. Birçok takviyeli öğrenme uygulaması, birbirinin ardına yapılan seçimleri kullanmaktadır. Yapılan seçim bir önceki seçime bağlıdır. Bu nedenle durum geçiş olasılığı $p_{ij}(a)$ ve amaç fonksiyonu V önem arz etmektedir. Bu tez çalışmasında her bir seçim birbirinden bağımsız ve birbirini etkilememektedir. Bu nedenle, MKS'nin faktörlerinden olan durum geçiş olasılığı $p_{ij}(a)$ ve amaç fonksiyonu V bu tez çalışmasında temsil edilmemiştir. Bu tez çalışmasında geliştirilen yöntemde temel amaç kullanıcıların güvenli iletişim için kullanılacak anahtarı yerel olarak oluşturmalarıdır. Gizli anahtarı üretecek kuantum kapılar KTÖ ile öğretilmektir. 2 kubitlik bir durum uzayı kullanılarak 1 adet kapı öğretilmektedir. N adet kapının öğrenilmesi için 2n kubitlik bir durum uzayı kullanılmaktadır.

İKİNCİ BÖLÜM
ÖNCEKİ ÇALIŞMALAR

Bu bölümde klasik yapay sinir ağları ile anahtar değişimi, kuantum kriptografi ve kuantum takviyeli öğrenmeye ilişkin önceki çalışmalardan bahsedilmiştir. Kuantum kriptografi üzerine yapılan çalışmalar KAD ve Kuantum Steganografi olarak iki başlıkta incelenmiştir. KAD protokolerine ilişkin çalışmalar ise kullanılan yönteme göre sınıflandırılmıştır.

2.1. Klasik Yapay Sinir Ağları ile Anahtar Dağıtımı

Herhangi bir kriptografik sistemin amacı, yetkisiz erişime sahip olabilecek diğer kişilere herhangi bir bilgi sızıntısı olmadan hedef kullanıcılar arasında bilgi alışverişidir. 1976'da Diffie & Hellmann, herhangi bir rakibin erişebileceği kamuya açık bir kanal üzerinden ortak gizli bir anahtarın oluşturulabileceğini bulmuştur. O zamandan beri sayı teorisine dayanan ve büyük hesaplama gücü gerektiren birçok açık anahtar şifrelemesi sunulmuştur. Ayrıca, açık anahtarın oluşturulmasıyla ilgili süreç çok karmaşık olmasının yanı sıra zaman almaktadır. Bu dezavantajların üstesinden gelmek için sinir ağları ortak gizli anahtar üretmek amacıyla kullanılabilir (Godhavari vd., 2005).

Kanter vd. (2002) tarafından sinir ağları teorisi ile kriptografi arasındaki bağlantı sunulmuştur. İki yapay sinir ağının bulunduğu sayısal simülasyonlarda sinir ağlarının senkronizasyonuyla gizli mesajların alışverişinde yeni bir yöntem olarak görülmektedir. Hebbian öğrenme kuralıyla eğitilen karşılıklı çıktılar, sinaptik ağırlıklarının antiparalel bir durumunu geliştirmektedir. Senkronize ağırlıklar, gizli verilerin güvenli bir şekilde iletilmesi için geçici bir anahtar değişim protokolü oluşturmak için kullanılır. Ağırlıkları takip etmek senkronizasyona göre zor bir problem olduğundan, protokolü ve herhangi bir veri iletiminin tüm ayrıntılarını bilen bir rakibin gizli mesajın şifresini çözme şansının olmadığı gösterilmiştir. Güvenli kanalın oluşturulmasının karmaşıklığı ağın boyutuyla doğrusaldır.

Godhavari vd. (2005), etkileşimli sinir ağlarına odaklandıkları kriptografi yöntemini geliştirmiştir. İletişim kuran her iki ağ da aynı giriş vektörünü alır, bir çıkış biti

üretir ve çıkış bitine göre eğitilir. Bu iki ağın dinamiğinin ve bunların ağırlık vektörlerinin, ağların aynı zamana bağlı ağırlıklara sahip bir duruma senkronize olduğu yeni bir olguyu sergilediği bulunmuştur. Karşılıklı öğrenme yoluyla bu senkronizasyon kavramı, genel bir kanal üzerinden gizli anahtar değişim protokolüne uygulanabilir.

Arvandi vd. (2006) tarafından yüksek performanslı veri şifreleme sağlamak için sinir ağı tabanlı bir simetrik şifre tasarım metodolojisi önerilmiştir. Önerilen yaklaşım, sinir ağlarının paralel işleme yeteneğini kriptografi amacıyla uygulamaya yönelik yeni bir girişimdir. Önerilen yöntem, sinir ağları yaklaşımını birleştirerek, gizli anahtarın uzunluğu üzerindeki kısıtlamayı ortadan kaldırır. Farklı kriptanaliz saldırılarına karşı dayanıklı olup verimli veri bütünlüğü ve kimlik doğrulama hizmetleri sağlar. Simetrik şifrenin tasarımı sunulmuş ve güvenliği analiz edilmiştir. Önerilen şifre tasarımının etkinliğini doğrulamak için simülasyon sonuçları sunulmaktadır.

Zhu vd. (2023), derin sinir ağı anahtar üretimine ve dinamik DNA kodlamasına dayanan süper kaotik bir görüntü şifreleme şeması önermiştir. İlk olarak, yalnızca metin içeren görüntülerden, metnin ana hattını çıkarmak için derin evrişimli sinir ağlarını kullanarak elde edilen bu değerler, kaotik sistemin başlangıç değerleri olarak kabul edilmektedir. Sonra şifreleme için kaotik diziyi elde etmek üzere süper kaotik Lorenz sistemi yinelenmektedir. Görüntü piksel matrisi için DNA kodlama kurallarını dinamik olarak seçmek üzere kaotik diziyi kullanır. Kaotik dizinin DNA kodlaması ve çalışması, görüntü piksel değerlerini değiştirmek için kullanılır. Son olarak şifrelemeyi gerçekleştirmek için dislokasyon ve difüzyon işlemleri gerçekleştirilir. Deneysel sonuçlar, önerilen görüntü şifreleme şemasının diferansiyel saldırılara ve çeşitli istatistiksel analizlere etkili bir şekilde direnebildiğini ve diğer algoritmalarla karşılaştırıldığında daha yüksek güvenliğe sahip olduğunu göstermektedir.

Niwa vd. (2023), evrişimsel sinir ağı tabanlı konuşma sınıflandırma görevleri için gizli anahtara sahip, gizliliği koruyan bir yöntem önermiştir. Son zamanlarda görüntü sınıflandırma araştırma alanlarında gizliliğin korunmasına ilişkin birçok yöntem geliştirilmiştir. Bunun aksine, konuşma sınıflandırması araştırma alanlarında bu riskleri dikkate alan çok az araştırma vardır. Konuşma sınıflandırmasında mahremiyetin korunmasına yönelik araştırmaları teşvik etmek amacıyla, evrişimsel sinir ağı tabanlı

konuşma sınıflandırma sistemlerinde gizli anahtara sahip bir şifreleme yöntemi sunulmuştur. Şifreleme yöntemi, rastgele tersinir bir matrise dayanmaktadır.

Kadir vd. (2023), kriptografik uygulamalarda kullanılan şifreleme anahtarlarını üretmek için kaotik zaman serisi tahmin modelini geliştirmiştir. Yapay sinir ağları, optimal katman tasarımı kullanılarak birleşik kaotik sistem örnekleriyle eğitilmiştir. Çok katmanlı algılayıcı, uzun kısa süreli bellek ve geçitli tekrarlayan birimler modellerinin performanslarını, kendi geliştirdikleri modelle karşılaştırmak amacıyla kaotik zaman serisi tahmini test edilmiştir. Bu üç model karşılaştırıldığında küçük farklılıklara rağmen neredeyse aynı sonuç elde edilmiştir.

2.2. Kuantum Kriptografi

Matematiksel modeller etrafında geliştirilen klasik kriptografik algoritmalar, kaba kuvvet saldırısı, çarpanlara ayırma problemi ve daha birçok güvenlik kusurundan muzdariptir. Bu nedenle, teknolojideki ilerlemeler nedeniyle klasik kriptografi, veri gizliliği ve güvenliği açısından güvenli bir seçenek gibi görülmemektedir. Kuantum kriptografisi adı verilen yeni bir teknolojiye doğru ilerlememizin nedeni de budur (Gruska, 1999).

Kuantum kriptografisi, gönderici ve alıcı arasında güvenli veri aktarımına izin veren kuantum fiziği olgusuna dayanmaktadır. Kuantum kriptografisi ağ güvenliği alanında bir devrim oluşturmaktadır. Kuantum kriptografisi, kriptografinin en son ve gelişmiş dalıdır ve temeli kuantum tekniklerinin iki ilkesine dayanır: Heisenberg'in belirsizlik ilkesi ve foton polarizasyonu ilkesi (Gisin vd., 2002).

2.2.1. Kuantum Anahtar Dağıtım Protokolleri

Kuantum anahtar dağıtımı, kuantum hesaplamanın en çok tartışılan konularından biridir. Sistem ortamdan yeterince izole edilemediği için kuantum bilgisayar yapımı oldukça zordur. Fakat fotonların kullanılması durumunda fiber optik kabloların ve hatta kablosuz ağların, kriptografi için gerekli olan anahtarların dağıtımı için uygun kanallar olduğu kanıtlanmıştır (Imre ve Balazs, 2005).

Gizli anahtar olarak adlandırılan 1 ve 0 lardan meydana gelen veri, bilginin şifrelenmesini ve şifresinin çözülmesini sağlamaktadır. Temelde yapılan işlem bitlerden oluşan iki verinin XOR işlemine tabi tutulmasıdır. Bu iki veriden bir tanesi gizli olarak paylaşmak istediğimiz mesaj iken diğeri gizli anahtardır. Gizli anahtara sahip olan herkes mesajı şifreler ve şifresini çözer. Bu nedenle yetkisiz kişiler iletişimi dinleyebilmek için gizli anahtarı ele geçirmeyi amaçlar. Her iletişim için aynı gizli anahtarın kullanılması sonucunda yetkisiz kişiler bir veri havuzu oluşturarak, gizli anahtarı tahmin edebilirler. Bu nedenle her iletişim için farklı gizli anahtar kullanılmalıdır. Bu durum gizli anahtarın güvenli bir şekilde paylaşılması problemine neden olur. Klasik kriptografide kullanılan anahtar dağıtım yöntemlerinin, kuantum hesaplama ile güvensiz hale geldiği kanıtlanmıştır. Bu nedenle araştırmacılar kuantum mekaniği ilkelerine dayalı, kuantum anahtar dağıtım yöntemleri geliştirmektedirler. Bu bölümde iletişimi başlatan gönderen taraf Alice, alıcı taraf Bob ve iletişimi yetkisiz olarak dinleyerek gizli bilgileri elde etmeye çalışan taraf ise Eve olarak adlandırılacaktır.

BB84 Kuantum Anahtar Dağıtımı Protokolü:

Anahtar dağıtımı için kuantum mekaniği ilkelerinin kullanıldığı ilk protokoldür. Bennett ve Brassad (1984) tarafından önerilmiştir. BB84, dört farklı polarizasyon durumu kullanır. Bunlar, 0^0, 45^0, 90^0 ve 135^0 polarizasyon durumlarıdır. Doğrusal ve Diyagonal olmak üzere iki farklı polarizasyon tabanı kullanarak foton polarize edilir. "0" değeri için polarizasyon durumları, Doğrusal taban kullanılması halinde 0^0 ve Diyagonal taban kullanılması halinde 45^0 olarak temsil edilir. "1" değeri için polarizasyon durumları, Doğrusal taban kullanılması halinde 90^0 ve Diyagonal taban kullanılması halinde 135^0 olarak temsil edilir. BB84 protokolünün algoritması aşağıda gösterilmiştir (Bennett ve Brassard, 1984):

Adım 1: Alice, 0 ve 1 değerlerini içeren n bitlik bir diziyi rastgele oluşturur. Her bir bit için farklı olmak üzere Doğrusal ya da Diyagonal bir polarizasyon tabanı seçer.

Adım 2: Alice, göndermek istediği bit değerini aşağıdaki gibi kodlayarak Bob'a gönderir:

a) Alice'in oluşturmuş olduğu bitin değeri "0" ve seçtiği taban Doğrusal ise Alice, fotonu 0^0 ile polarize ederek Bob'a gönderir.

b) Alice'in oluşturmuş olduğu bitin değeri "0" ve seçtiği taban Diyagonal ise Alice, fotonu 45^0 ile polarize ederek Bob'a gönderir.

c) Alice'in oluşturmuş olduğu bitin değeri "1" ve seçtiği taban Doğrusal ise Alice, fotonu 90^0 ile polarize ederek Bob'a gönderir.

d) Alice'in oluşturmuş olduğu bitin değeri "1" ve seçtiği taban Diyagonal ise Alice, fotonu 135^0 ile polarize ederek Bob'a gönderir.

Adım 3: Bob, her bir foton için Doğrusal ya da Diyagonal tabanlardan birini rastgele seçer. Alice'in polarize ederek gönderdiği foton, Bob'un seçmiş olduğu tabandan geçer. Eğer Bob, Alice'in tabanı ile aynı tabanı seçtiyse foton polarizasyonunu korur. Bob'un, Alice'den farklı bir taban seçmesi durumunda ise Bob'un seçtiği tabana ait açılara göre %50 olasılıkla "0" ya da %50 olasılıkla "1" olarak polarize hale gelecektir. Daha sonra Bob, fotonlarda kuantum ölçüm gerçekleştirir ve ölçüm sonuçlarını saklar.

Adım 4: Bob, seçmiş olduğu polarizasyon tabanlarını duyurur. Ölçüm sonuçlarını paylaşmaz.

Adım 5: Alice, Bob'un kendisi ile aynı seçtiği tabanlara ait indisleri duyurur. Bob, duyurulan indislere ait ölçüm sonuçlarını anahtar bitleri olarak saklar. Farklı tabanlardaki ölçüm sonuçlarını göz ardı eder.

Adım 6: Bob, anahtar bitlerinin bir kısmını duyurur. Amaç Eve'nin varlığını tespit etmektir.

Adım 7: Alice, Bob'un duyurduğu bitleri kendi bitleri ile karşılaştırır. Bitler aynı değere sahip ise iletişimin güvenli olduğunu onaylar. İlan edilen bitler atılarak kalan bitlerden gizli anahtar oluşturulur. Eğer bitler farklı değere sahip ise Eve'nin varlığı tespit edilmiş olur. Böylece anahtarın geçersiz olduğu duyurulur.

Şekil 3'de iletişimi dinleyen üçüncü bir tarafın var olmadığı durumda BB84 protokolünün çalışması örneklendirilmektedir. Anahtarı oluşturmak için 20 bit kullanıldığı

görülmektedir. 1., 4., 7., 11. ve 16. bitler için farklı tabanlar kullanıldığından bu bitler anahtara dahil edilmezler. Bu bitlerin dışında kalan bitler, kullanılarak anahtar oluşturulur.

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
Alice	⊞	⊠	⊞	⊞	⊞	⊠	⊠	⊞	⊠	⊠	⊞	⊠	⊞	⊞	⊠	⊞	⊞	⊠	⊞	⊠
	↕	↗	↔	↔	↕	↖	↗	↔	↖	↖	↕	↗	↔	↕	↗	↕	↕	↖	↔	↗
	1	0	0	0	1	1	0	0	1	1	1	0	0	1	0	1	1	1	0	0
Bob	⊠	⊠	⊞	⊠	⊞	⊠	⊞	⊞	⊠	⊠	⊠	⊠	⊞	⊞	⊠	⊠	⊞	⊠	⊞	⊠
	0	0	0	1	1	1	0	0	1	1	1	0	0	1	0	0	1	1	0	0
	*	0	0	*	1	1	*	0	1	1	*	0	0	1	0	*	1	1	0	0

Şekil 3. Eve var olmadığı durumda BB84 protokolünün çalışması (Çağlar vd., 2022)

Anahtar biti olarak kabul edilen 5. bit için aşağıdaki adımlar uygulanır:

Adım1: Alice, 1 bit değerini ve Doğrusal tabanı seçer.

Adım 2: Alice, Doğrusal tabanı kullanarak 1 bit değeri için fotonu 90^0 polarize eder ve Bob'a gönderir.

Adım 3: Bob, Doğrusal tabanı seçer ve ölçüm yapar. Ölçüm sonucu olarak 1 değerini elde eder.

Adım 4: Bob, seçmiş olduğu Doğrusal taban bilgisini Alice ile paylaşır.

Adım 5: Alice, aynı tabanı seçtiklerini tespit ederek Bob'a Bit'in geçerli olduğunu bildirir.

Anahtar biti olarak kabul edilmeyen 7. bit için ise aşağıdaki adımlar uygulanır:

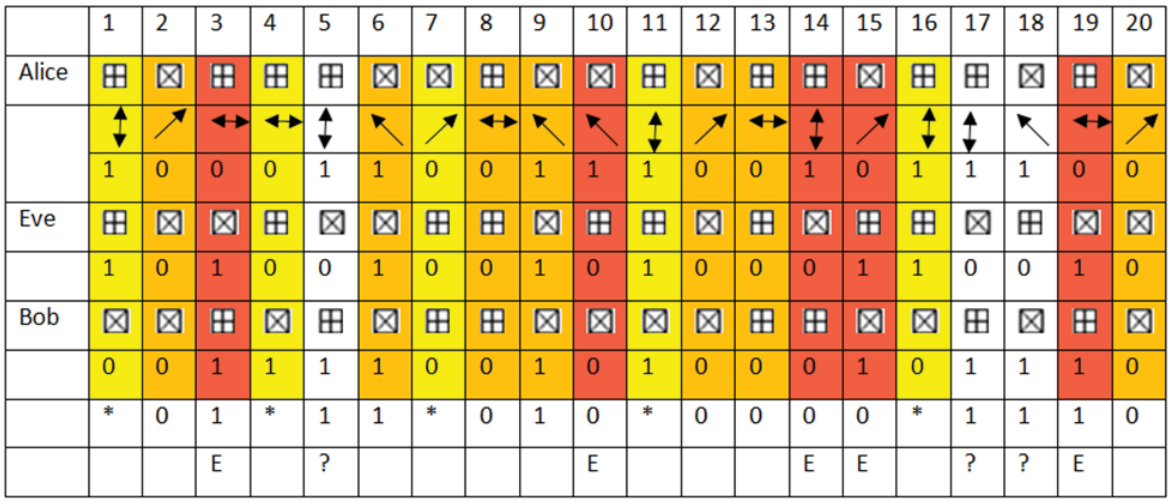
Adım1: Alice, 0 bit değerini ve Diyagonal tabanı seçer.

Adım 2: Alice, Diyagonal tabanı kullanarak 0 bit değeri için fotonu 45^0 polarize eder ve Bob'a gönderir.

Adım 3: Bob, Doğrusal tabanı seçer ve ölçüm yapar. Ölçüm sonucu olarak 0 değerini elde eder. Alice'in göndermiş olduğu foton Diyagonal tabana göre polarize edildiği için Bob'un uyguladığı Doğrusal taban, fotonun polarizasyonunun bozulmasına neden olur. 45^0 açı ile Doğrusal tabana gelen bir foton, %50 olasılıkla 0^0, %50 olasılıkla 90^0 ile polarize olur. Bob, ölçüm sonucu olarak %50 olasılıkla 0, %50 olasılıkla 1 değerini elde eder. Yani Bob'un, doğru bilgiyi elde etme olasılığı da %50'dir. Bu nedenle Bob'un seçmiş olduğu tabanı öğrenen Alice, ilgili biti geçersiz ilan eder.

Adım 4: Bob, seçmiş olduğu Doğrusal taban bilgisini Alice ile paylaşır.

Adım 5: Alice, farklı tabanı seçtiklerini tespit ederek Bob'a Bit'in geçersiz olduğunu bildirir.



Şekil 4 Eve'nin var olduğu durumda BB84 protokolünün çalışması (Çağlar vd., 2022)

Şekil 4'de iletişimi dinleyen üçüncü bir tarafın var olduğu durumda BB84 protokolünün çalışması örneklendirilmektedir. Burada Eve'nin amacı araya girip anahtar bilgisini elde etmektir. Bunun için Durdur-Tekrar gönder saldırısını yapar. Eve, Alice'in gönderdiği fotona kendi polarizasyon tabanının uygular ve sonrasında ölçüm yapar. Ölçüm sonucuna göre tekrar aynı polarizasyon tabanını kullanarak fotonu polarize ederek Bob'a gönderir. Alice, Bob ve Eve'nin seçmiş oldukları tabanlara göre aşağıdaki durumlar ortaya çıkar:

Durum 1: 2., 6., 8., 9., 12., 13. ve 20. bitler için Alice, Bob ve Eve, aynı polarizasyon tabanının seçmektedir. Bu bitler için Eve'nin varlığı tespit edilemez. Üç kullanıcı aynı polarizasyon tabanını seçtiği için Eve ve Bob, Alice'in elindeki orijinal bilgiyi doğru bir şekilde elde eder. Bu durumda BB84 protokolünün güvenlik açığı bulunduğundan B92 protokolü geliştirilmiştir.

Durum 2: 1., 4., 7., 11. ve 16. bitler için Alice ve Bob farklı polarizasyon tabanlarını seçmişlerdir. Bu durumda Eve'nin seçmiş olduğu polarizasyon tabanının önemi yoktur. Eve'nin varlığının tespit edilmesi beklenmez. Alice, farklı polarizasyon tabanları seçildiği için ilgili bitleri iptal eder.

Durum 3: Yukarıdaki durumların dışında kalan bitlerde Alice ve Bob aynı polarizasyon tabanını seçerken Eve farklı bir polarizasyon tabanı seçmiştir. Eve olmasaydı Alice ve Bob sorunsuz bir iletişim kuracak ve Bob, Alice'in elindeki orijinal bilgiyi elde edecekti. Fakat Eve'nin varlığı nedeniyle Alice'in göndermiş olduğu fotonun polarizasyonu bozulur. Eve, Alice'den farklı bir polarizasyon tabanı seçtiği için Alice'in göndermiş olduğu polarize edilmiş fotonu elde edemez. Kendi seçtiği tabana ve ölçüm sonucuna göre fotonu polarize ederek Bob'a gönderir. Eve'nin ve Bob'un polarizasyon tabanlarının farklı olması nedeniyle Bob, ölçüm sonucunda %50 olasılıkla 0 ya da %50 olasılıkla 1 elde eder. Başka bir deyişle Alice'in elindeki bitin değerini %50 olasılıkla elde eder. Bob, bu bit değerini duyurduğunda Alice, kendi bit değeri ile karşılaştırır. Bit değerleri farklıysa iletişimi dinleyen üçüncü bir kullanıcının varlığını ilan eder.

Şekil 4'teki 3. bit incelenirse Alice ve Bob'un Doğrusal, Eve'nin ise Diyagonal tabanı seçtiği görülür. Alice, 0 bit değeri için Doğrusal tabanı kullanarak fotonu 0^0 polarize ederek Bob'a gönderir. Eve, araya girip Diyagonal tabanı kullanır. Eve, ölçüm sonucu olarak %50 olasılıkla 1 elde eder. Eve, 1 bit değeri için Diyagonal tabanı kullanarak fotonu 135^0 polarize ederek Bob'a gönderir. Bob, Eve'nin polarizasyon tabanından farklı olarak Doğrusal tabanı seçmiştir. Ölçüm sonucu olarak %50 olasılıkla 1 değerini elde eder. Bob, ilgili bit için 1 değerini elde ettiğini duyurur. Alice, kendi elindeki bit değerinden farklı bir değer olması nedeniyle Eve'nin varlığını ilan eder.

Şekil 4'teki 5. bit incelenirse Alice ve Bob'un Doğrusal, Eve'nin ise Diyagonal tabanı seçtiği görülür. Alice, 1 bit değeri için Doğrusal tabanı kullanarak fotonu 90^0 polarize ederek Bob'a gönderir. Eve, araya girip Diyagonal tabanı kullanır. Eve, ölçüm sonucu olarak %50 olasılıkla 0 elde eder. Eve, 0 bit değeri için Diyagonal tabanı kullanarak fotonu 45^0 polarize ederek Bob'a gönderir. Bob, Eve'nin polarizasyon tabanından farklı olarak Doğrusal tabanı seçmiştir. Ölçüm sonucu olarak %50 olasılıkla 1 değerini elde eder. Bob, ilgili bit için 1 değerini elde ettiğini duyurur. Alice, kendi elindeki bit değeri ile aynı değere sahip oluğundan Eve'nin varlığını tespit edemez.

Her ne kadar BB84 protokolünde, Eve'nin tespit edilemediği durumlar olsa da güvenli kabul edilir. Anahtar boyutunun 1 bit olduğu varsayımında BB84 protokolünün güvensiz olduğu söylenebilir. 1 bit için Eve'nin varlığı tespit edilemeyebilir. Fakat 512 bit boyutunda bir anahtarı oluştururken Eve'nin tespit edilememesi çok düşük bir olasılıktır. Anahtar boyutu büyüdükçe Eve'nin tespit edilmesi ihtimali artar. Günümüzde BB84 protokolünü kullanan Kuantum Anahtar Dağıtım cihazları mevcuttur.

B92 Kuantum Anahtar Dağıtımı Protokolü:

Bennet (1992), BB84 protokolüne alternatif olarak ortogonal olmayan iki durum kullanan B92 protokolünü geliştirmiştir. B92 protokolü, BB84 protokolünde olduğu gibi foton polarizasyonu için Doğrusal ve Diyagonal polarizasyon tabanlarını kullanır. BB84 protokolünde Alice, Bob ve Eve aynı polarizasyon tabanını kullanıyorsa Eve'nin varlığı tespit edilemez. Bu problemi çözmek adına B92 protokolünde gönderici ile alıcı, ortogonal olmayan durumları birbiriyle eşleştirerek farklı polarizasyon durumlarını geçerli kabul eder. 0 bit değeri için Alice 0^0 ve Bob 135^0 polarizasyon durumunu kabul eder. 1 bit değeri için ise Alice 45^0 ve Bob 90^0 polarizasyon durumunu kabul eder. Bob, 0^0 ve 45^0 polarizasyon durumları için yaptığı ölçümleri geçerli kabul etmez. B92 protokolünün algoritması aşağıda gösterilmiştir (Bennet, 1992):

Adım 1: Alice, 0 ve 1 değerlerini içeren n bitlik bir diziyi rastgele oluşturur. Alice, 0 bit değeri için 0^0 ve 1 bit değeri için 45^0 polarizasyon durumlarını kullanarak polarize olmuş fotonları Bob'a gönderir.

Adım 2: Bob, her bir foton için Doğrusal ve Diyagonal polarizasyon tabanlarından rastgele birini seçer. Alice'in 0^0 polarizasyon ile göndermiş olduğu foton Doğrusal polarizasyon tabanı seçilirse 0^0 olarak kalır. Diyagonal polarizasyon tabanı seçilirse %50 olasılıkla 45^0, %50 olasılıkla 135^0 polarizasyon durumu meydana gelir. Alice'in 45^0 polarizasyon ile göndermiş olduğu foton ise Diyagonal polarizasyon tabanı seçilirse 45^0 olarak kalır. Doğrusal polarizasyon tabanı seçilirse %50 olasılıkla 0^0, %50 olasılıkla 90^0 polarizasyon durumu meydana gelir.

Adım 3: Bob, sadece 90^0 ve 135^0 polarizasyon durumunda yapılan ölçüm sonuçlarını kabul eder. Aynı polarizasyon tabanının kullanıldığı durumlarda Alice ve Bob'un polarizasyon durumları aynı olduğundan ilgili fotonlar için yapılan ölçüm sonuçları kabul edilmez. B92 protokolü, BB84 protokolündeki Eve'nin fark edilmediği durumları ortadan kaldırmayı amaçlar. Ölçüm sonuçlarına göre Bob, 90^0 polarizasyon durumu için bit değerini 1, 135^0 polarizasyon durumu için bit değerini 0 olarak kabul ederek anahtar oluşturur.

Adım 4: Bob, anahtar oluşturmak için kullandığı fotonların indislerini duyurur.

Adım 5: Eve'nin varlığını tespit etmek için Alice, kullandığı polarizasyon tabanlarının bir kısmını duyurur. Anahtarı oluşturmak için kullanılan fotonlar için Alice ve Bob'un farklı polarizasyon tabanları kullanmış olması beklenir. Bob, Alice'in duyurduğu tabanlar ile kendi seçtiği tabanları karşılaştırır. Kabul edilmiş anahtar bitleri için aynı polarizasyon tabanının seçildiği gözlenirse Eve'nin varlığı tespit edilir. Zira aynı polarizasyon tabanının seçildiği durumda Bob, Alice ile aynı polarizasyon durumunu elde edip ilgili fotonu reddetmesi gerekirken aksine kabul etmiştir. Bu durum Eve'nin araya girerek Alice'in fotonunun polarizasyonunu bozmuş olmasıyla açıklanır. Eve'nin varlığı tespit edildikten sonra anahtarın geçersiz olduğu ilan edilir.

Şekil 5'te Alice'in ve Bob'un seçimlerine ilişkin tüm olasılıkları gösteren B92 protokol örneği görülmektedir. Alice'in, 0 bit değeri için 0^0 polarizasyon durumu ile foton gönderdiği durumlar aşağıda ele alınmıştır:

Alice	0	0	0	1	1	1
	↔	↔	↔	↗	↗	↗
Bob	⊞	⊠	⊠	⊠	⊞	⊞
	↔	↗	↖	↗	↔	↕
	Geçersiz	Geçersiz	Geçerli	Geçersiz	Geçersiz	Geçerli

Şekil 5 Eve var olmadığı durumda B92 protokolünün çalışması (Çağlar vd., 2022)

Olasılık 1: Bob, Doğrusal polarizasyon tabanını seçerek ölçüm yaparsa %100 olasılıkla 0^0 polarizasyon durumunu elde eder. Bob, 0^0 polarizasyon durumu için ölçüm sonuçlarını anahtar biti olarak kabul etmez.

Olasılık 2: Bob, Diyagonal polarizasyon tabanını seçerek ölçüm yaparsa %50 olasılıkla 45^0 polarizasyon durumunu elde eder. Bob, 45^0 polarizasyon durumu için ölçüm sonuçlarını anahtar biti olarak kabul etmez.

Olasılık 3: Bob, Diyagonal polarizasyon tabanını seçerek ölçüm yaparsa %50 olasılıkla 135^0 polarizasyon durumunu elde eder. Bob, 135^0 polarizasyon durumu için ölçüm sonuçlarını anahtar biti olarak kabul eder. İlgili foton için anahtara 0 değerini ekler.

Alice'in, 1 bit değeri için 45^0 polarizasyon durumu ile foton gönderdiği durumlar aşağıda ele alınmıştır:

Olasılık 1: Bob, Diyagonal polarizasyon tabanını seçerek ölçüm yaparsa %100 olasılıkla 45^0 polarizasyon durumunu elde eder. Bob, 45^0 polarizasyon durumu için ölçüm sonuçlarını anahtar biti olarak kabul etmez.

Olasılık 2: Bob, Doğrusal polarizasyon tabanını seçerek ölçüm yaparsa %50 olasılıkla 0^0 polarizasyon durumunu elde eder. Bob, 0^0 polarizasyon durumu için ölçüm sonuçlarını anahtar biti olarak kabul etmez.

Olasılık 3: Bob, Doğrusal polarizasyon tabanını seçerek ölçüm yaparsa %50 olasılıkla 90^0 polarizasyon durumunu elde eder. Bob, 90^0 polarizasyon durumu için ölçüm sonuçlarını anahtar biti olarak kabul eder. İlgili foton için anahtara 1 değerini ekler.

Alice	0	0	0	0	0	0	0	0	0
	↔	↔	↔	↔	↔	↔	↔	↔	↔
Eve	⊞	⊞	⊞	⊠	⊠	⊠	⊠	⊠	⊠
	↔	↔	↔	↗	↗	↗	↖	↖	↖
Bob	⊞	⊠	⊠	⊠	⊞	⊞	⊠	⊞	⊞
	↔	↗	↖	↗	↔	↕	↖	↔	↕
	?	?	0	?	?	1	0	?	1
B92	Geçersiz	Geçersiz	Geçerli	Geçersiz	Geçersiz	Dinleme Var	Geçerli	Geçersiz	Dinleme Var

Şekil 6 Eve'nin var olduğu durumda B92 protokolünün çalışması (Çağlar vd., 2022)

Şekil 6'da Alice'in 0 bit değerini 0^0 polarizasyon durumu ile gönderdiği durum için Eve'nin ve Bob'un seçimlerine ait tüm olasılıkları görülmektedir.

Durum 1: Bob, 0^0 ve 45^0 polarizasyon durumları için yapılacak ölçüm sonuçlarını anahtara bit olarak eklemez. Bu fotonlar geçersiz kabul edildiğinden Eve'nin varlığı sorgulanmaz.

Durum 2: Bob, 135^0 polarizasyon durumları için yapılacak ölçüm sonuçlarını anahtar biti olarak ekler. Bob, Alice ile farklı tabanlar kullandığı için kabul edilen bu fotonlarda Eve'nin varlığı tespit edilemez.

Durum 3: Bob, 90^0 polarizasyon durumları için yapılacak ölçüm sonuçlarını anahtar biti olarak ekler. Alice bu fotonlar için kullanmış olduğu Doğrusal polarizasyon tabanını duyurursa Bob, Eve'nin varlığını tespit eder. Bob, Doğrusal tabanı kullanarak 90^0 polarizasyon durumunu elde eder. Alice, Doğrusal tabanı kullandığına göre 0^0 polarizasyon durumlu bir foton gönderir. Alice ve Bob aynı polarizasyon tabanını kullandığı için Bob'un %100 olasılıkla 0^0 polarizasyon durumunu elde etmesi beklenir. Bob'un 90^0 polarizasyon durumunu elde etmesinin tek yolu, Diyagonal tabanda üretilen bir fotonun Bob'a gönderilmesidir. Bunu gönderen Alice olmadığına göre Eve araya girerek Alice'in fotonunun polarizasyonunu bozmuştur. Bob, Eve'nin varlığını duyurur.

Dolanık Tabanlı Kuantum Anahtar Dağıtımı Protokolleri:

Dolanıklık, kuantum dünyasının en akıl almaz özelliğidir. Birbirinden çok uzak iki parçacık gizemli bir şekilde birbirine bağlıdır. Bir parçacığa yapılan herhangi bir müdahale diğer parçacıkta anında bir değişikliğe neden olur (Aczel, 2018: 11). Dolanık fotonlar Bell durumları ile gösterilir. Bir Bell durumunu üretmek için iki kubit kullanılır. İlk olarak birinci kubite Hadamard kapısı uygulanır. Daha sonra iki kubite CNOT kapısı uygulanır (Ural, 2021: 103). Tablo 4'de Bell durumları gösterilmiştir.

Tablo 4

Bell Durumları (Nielsen ve Chuang, 2010)

İki Kubit	Bell Durumları
$\|00\rangle$	$\|B_{00}\rangle = \frac{\|00\rangle + \|11\rangle}{\sqrt{2}}$
$\|01\rangle$	$\|B_{01}\rangle = \frac{\|01\rangle + \|10\rangle}{\sqrt{2}}$
$\|10\rangle$	$\|B_{10}\rangle = \frac{\|00\rangle - \|11\rangle}{\sqrt{2}}$
$\|11\rangle$	$\|B_{11}\rangle = \frac{\|01\rangle - \|10\rangle}{\sqrt{2}}$

Ekert (1991), kuantum dolanıklığa dayanan E91 protokolünü önermiştir. Bu protokolde birbiriyle dolanık iki foton kullanılır. Dolanık foton, üretici bir kaynaktan her iki kullanıcıya gönderildiği gibi dolanık fotonları üreten kaynak, bu kullanıcılardan biri de olabilir. Gönderme işlemi için kuantum kanal kullanılır. Kuantum dolanıklığın doğası gereği dolanık foton çiftinin üçüncü bir kopyası oluşturulamaz. Her iki kullanıcı da her bir fotonu Z (Doğrusal) ya da X (Diyagonal) tabanında ölçer. Ölçüm yapılan tabanlar her bir foton için rastgele belirlenir. Açık bir kanal vasıtasıyla ölçüm için kullanılan tabanlar paylaşılır. Aynı tabanların kullanıldığı fotonlar için yapılan ölçüm sonuçlarına göre anahtar oluşturulur (Ural, 2021: 187, İpekoğlu vd., 2009: 87).

Bennett vd. (1992), sahte bir dolanıklık kaynağının değiştirilmesi de dâhil olmak üzere genel saldırılara karşı güvenli ve Bell teoremine dayanmayan kuantum dolanıklık

temelli bir protokol önermiştir. Protokolün BB84'e eşdeğer olduğu gösterilmiştir. Gao vd. (2006), dolanıklık transferine dayalı bir kuantum anahtar dağıtım protokolü önermiştir. İki kullanıcı sıradan parçacıkları ikişer ikişer seçip Bell ölçümleri gerçekleştirerek gizlice dinlemeyi tespit edebilir ve güvenli anahtarı elde edebilir. Birlikte ölçülen iki parçacık rastgele seçildiğinden güvenliği sağlamak için alternatif ölçümlere ya da Bell durumlarının rotasyonlarına ihtiyaç yoktur.

Perumangatt vd. (2015), fotonların polarizasyonunu ve yörünge açısal momentumunu kullanarak üç parçacıklı dolanıklık oluşturmak için bir şema sunmuştur. Oluşturulan durumun, polarizasyon ve yörünge açısal momentum tarafından tanımlanan iki kubitlik bir durumu ışınlamak için kullanılabileceği gösterilmiştir. Önerilen kuantum sistemi aynı zamanda yeni ve verimli bir kuantum anahtar dağıtımı protokolünü tanımlamak için de kullanılır.

Sürekli Değişken Kuantum Anahtar Dağıtımı Protokolleri:

Bencheikh vd. (2001), gizli kuantum anahtarlarının oluşturulması için sürekli değişkenlere sahip yeni bir kuantum şifreleme protokolü önermiştir. Protokol; dejenere olmayan, parametrik amplifikasyon tarafından üretilen iki modlu elektromanyetik alanın Einstein-Podolsky-Rosen dolanık çiftlerine dayanmaktadır. Kuantum dalgalanmaların anlık ölçümleri, gizli anahtarın rastgele bitlerini sağlar. Yetkisiz ölçümler nedeniyle dolanıklığın geri döndürülemez şekilde değiştirilmesi, kuantum anahtar dağıtımını gizli dinleme saldırılarına karşı korur.

Wang vd. (2015) tarafından geliştirilen sürekli değişken kuantum anahtar dağıtım sistemi, gerçek dünya koşullarında 25 MHz hızında çalışmaktadır. Yüksek hıza ulaşmak için, 300 MHz'e kadar maksimum bant genişliğine sahip bir homodin detektörü ve 25 Mbps'ye kadar işlem hızına sahip, optimum yüksek verimli bir hata düzeltme algoritması kullanılır. Sistemin stabilitesini optimize etmek için, yeni bir faz dengeleme algoritması, bir polarizasyon geri besleme algoritması ve modülatörler üzerinde ilgili stabilite yöntemini içeren birkaç temel teknik geliştirilmiştir. Geliştirilen sistem, 50 km iletim mesafesi boyunca 52 Kbps nihai gizli anahtar hızıyla 12 saatten fazla test edilmiştir.

Yarı Kuantum Anahtar Dağıtımı Protokolleri:

Yu vd. (2014) tarafından kimliği doğrulanmış klasik kanalları kullanmadan, ilk kimliği doğrulanmış yarı kuantum anahtar dağıtımı protokolü önerilmiştir. Gelişmiş kuantum cihazlara sahip gönderici, iki katılımcı arasında ana gizli anahtarın önceden paylaşılmasıyla, yalnızca klasik işlemleri gerçekleştirebilen alıcıya çalışan anahtarı iletebilir. Doğrulanmış yarı kuantum anahtar dağıtım fikri, güvenlik sistemlerinde anahtar yönetim sorununu da kolaylaştıran bir anahtar hiyerarşisinin kurulmasını sağlar. Önerilen protokol birçok iyi bilinen saldırıdan korunur. Li vd. (2016) tarafından ise daha iyi kubit verimliliği sağlayan ve daha az sayıda önceden anahtar paylaşımı gerektiren kimliği doğrulanmış yarı kuantum anahtar dağıtım protokolü önerilmiştir.

Hajji ve Baz (2021) tarafından önerilen 3 boyutlu kuantum durumlarına dayalı yarı kuantum anahtar dağıtım protokolü koşulsuz güvenliği sağlar. Kuantum kanal gürültüsünün bir fonksiyonu olarak asimptotik senaryoda anahtar hızı için bir alt sınır türeterek, bu protokolün önceki 2 boyutlu yarı kuantum anahtar dağıtımı protokolüyle karşılaştırıldığında çok daha fazla gürültü toleransıyla gizli anahtar hızını iyileştirdiği bulunmuştur. Sonuçları, tam kuantum anahtar dağıtım protokolüne benzer şekilde, sistemin boyutunu artırmanın yarı kuantum anahtar dağıtımında da gürültü toleransını artırabileceği gözlenmiştir.

2.2.2. Kuantum Steganografi Çalışmaları

Steganografi mesajın varlığının gizlenmesi ile ilgili yöntemlerle uğraşır. Steganografi tek başına kullanıldığı gibi kriptografik yöntemlerle birlikte de kullanılabilir (Afacan, 2016: 41). Görüntü, ses ya da metin dosyalarının içerisine mesaj gizlenerek güvenli bir şekilde karşı tarafa mesaj gönderilir. Kuantum steganografi ise kuantum mekaniği ilkelerine göre temsil edilen görüntü, ses ya da metin dosyalarının içerisine mesajın gizlenmesi ile gerçekleştirilir.

Filigranlama, farklı uygulamalarda kullanılmak üzere filigran bitlerinin multimedya verilerine fark edilemeyecek şekilde yerleştirilmesidir. Filigranlama uygulamalarından olan telif hakkı koruması, başkalarının telif hakkı talebinde bulunmasını engellemek

amacıyla taşıyıcıdaki mal sahibi hakkındaki bilgileri gizleyen en belirgin kullanımdır. Heidari vd. (2017) tarafından geliştirilen çalışmada, RGB görüntülerde sahibinin imzasını temel alan yeni bir kör kuantum telif hakkı koruma yöntemi önerilmiştir. Yöntem, RGB kanallarından birini gösterge olarak kullanırken kalan iki kanal, sahibine ilişkin bilgilerin yerleştirilmesi için kullanılır. Yöntemde sahibinin imzası metin olarak değerlendirilmektedir. Bu nedenle, renkli görüntüye filigran olarak gömmek için metnin ASCII karakter kümesini temel alan yeni bir kuantum temsili sunulmuştur.

Şahin ve Yılmaz (2018a), çok dalga boylu kuantum görüntüleri için LSBq tabanlı yeni bir kuantum steganografi algoritması önermiştir. Yapılan çalışmada kapak görselinin içerisine hem metin hem de ikili görsel mesajlar yerleştirilmiştir. Simülasyon ve analiz sonuçları, önerilen algoritmanın steganografi algoritmalarının gereksinimlerini karşıladığını göstermektedir. Yetkisiz bir kişinin, gömülü bir bilgiyi bilinen yöntemlerle çıkarmaya çalıştığında anlamsız bilgiler elde ettiği görülmektedir. Sonuçlar, stego görüntüsüne birden fazla saldırı uygulandığında algoritmanın saldırılara karşı dayanıklı olduğunu göstermektedir.

Şahin ve Yılmaz (2018b) tarafından kuantum görüntülerin gösterim yöntemi olan NEQR yönteminin güvenliği için kör trent ile Kuantum Fourier Dönüşümü (KFD - Quantum Fourier Transform - QFT) kullanılarak şifreleme ve dağıtım protokolü önerilmiştir. Protokolde imzayı alıcılarla paylaşmak için KFD ve anahtarlar kullanılmıştır. Yani tüm üyeler yalnızca KFD'nün şifrelenmiş çıktısı olan imza bilgilerini bilir. Bu sayede protokolün güvenliği arttırılmış olur. Ayrıca protokolün güvenliği, KFD çıkış kubitlerinin kör trent permütasyonu ile yeniden sıralanmasıyla sağlanır.

2.3. Kuantum Takviyeli Öğrenme Çalışmaları

Kuantum hesaplamanın ortaya çıkışı, araştırmacıların mevcut birçok çalışmaya kuantum devresini uygulamasını sağlar. Kuantum devresi ve kuantum diferansiyel programlama kullanılarak Kuantum Makine Öğrenimi gibi birçok araştırma yürütülmektedir. Özellikle kuantum takviyeli öğrenme, kuantum makine öğreniminin olasılığını test etmek için iyi bir alandır ve birçok araştırma yapılmaktadır (Kwak vd., 2021).

Takviyeli öğrenme, makine öğreniminde en hızlı büyüyen alanlardan biridir. Biyotıp, nesnelerin interneti, lojistik, robotik kontrol vb. alanlarda büyük başarılar elde etmiştir. Ancak mühendislik uygulamaları için hâlâ öğrenme sürecinin nasıl hızlandırılacağı, keşif ve sömürü arasındaki dengenin nasıl sağlanacağı gibi pek çok zorluk bulunmaktadır. Özellikle süper bilgisayarlarda karmaşık problemleri klasik yöntemlere göre daha hızlı çözebilen kuantum teknolojisi, takviyeli öğrenmede bu zorlukların üstesinden gelmemiz için bize yeni bir paradigma sağlamaktadır. (Hu vd., 2021).

Dong vd. (2006) tarafından beş kubitin kontrol problemini inceleyerek kuantum kontrol problemi için kuantum süperpozisyon ilkesine dayanan yeni bir kuantum takviyeli öğrenme algoritması önerilmiştir. Simüle edilen sonuç, kuantum takviyeli öğrenmenin, hızlı öğrenme yoluyla en uygun kontrol dizisini etkili bir şekilde bulabileceğini göstermektedir.

Dong vd. (2008) tarafından yapılan çalışmada, kuantum teorisi ile takviyeli öğrenmenin birleştirilmesiyle yeni bir kuantum takviyeli öğrenme yöntemi önerilmiştir. Geleneksel takviyeli öğrenmedeki durum (eylem), KTÖ'deki öz durum (öz eylem) olarak tanımlanır. Durum (eylem) seti, bir kuantum süperpozisyon durumuyla temsil edilebilir. Öz durum (öz eylem), kuantum ölçümünün çöküş varsayımına göre simüle edilerek kuantum durumunun rastgele gözlenmesiyle elde edilebilir. Öz eylemin olasılığı, ödüllere göre paralel olarak güncellenen olasılık büyüklüğü tarafından belirlenir. KTÖ'nin yakınsama, optimallik ve keşif ile sömürü arasında dengeleme gibi bazı ilgili özellikleri de analiz edilmiştir. KTÖ'nin olasılık genliğini kullanarak keşif ve sömürü arasında iyi bir denge sağladığını ve kuantum paralelliği yoluyla öğrenmeyi hızlandırabildiği gösterilmiştir.

Dong vd. (2012) tarafından otonom mobil robotların navigasyon kontrolü için yeni bir kuantumdan takviyeli öğrenme algoritması önerilmiştir. KTÖ algoritması, olasılıksal bir eylem seçim politikasını ve kuantum ölçümünde çökme fenomeni yoluyla yeni bir güçlendirme stratejisini benimser. KTÖ'nin öğrenme oranları ve başlangıç durumları açısından geleneksel takviyeli öğrenmeye göre daha sağlam olduğu gösterilmiştir. Daha sonra KTÖ yaklaşımı gerçek bir mobil robotun navigasyon kontrolüne uygulanmıştır. Simülasyon ve deneysel sonuçlar, önerilen yaklaşımın etkinliğini göstermektedir.

Kwak vd. (2021) tarafından yapılan çalışma, değişken kuantum devresi kullanılarak kuantum takviyeli öğrenme kavramını tanıtmanın yanı sıra uygulama ve deneyler yoluyla da kanıtlanmıştır. Öncelikle kuantum takviyeli öğrenmenin arka plan bilgisi ve çalışma prensibi sunulmuştur. Daha sonra PennyLane kütüphanesi kullanılarak uygulama gerçekleştirilmiştir.

Niraula vd. (2021), kanser hastalarının tedavisinde doz tepkisini tahmin edebilen ve optimal bir doz ayarlaması önerebilen yeni bir kuantum derin takviyeli öğrenme algoritması geliştirmiştir. Hu vd. (2021) ise optimal kontrol için kuantum takviyeli öğrenme algoritmasını geliştirmiştir. Bu algoritmada, takviyeli öğrenmenin durumları ve eylemleri kuantum teknolojisiyle gösterilir. Daha sonra, kuantize edilmiş teknoloji yoluyla keşif ve sömürü arasındaki dengeyi etkili şekilde sağlayan olasılık yükseltme yöntemi sunulur.

Kumar vd. (2023), e-mobilite için Blockchain ve Kuantum Takviyeli Öğrenme tabanlı optimize edilmiş Enerji Ticareti modelini sunmuştur. Park ve Kim (2023) tarafından ise kuantum sinir ağı tabanlı merkezi kritik ve çok oyunculu ağlardan ilham alan kuantum hesaplama tabanlı, çok etmenli takviyeli öğrenme algoritması önerilmiştir.

Neumann vd. (2023), bir gridi geçmek için en uygun politikayı bulmak ve bunları klasik derin takviyeli öğrenme yaklaşımıyla karşılaştırmak için kuantum tavlamayı ve kuantum kapıları temel alan iki adet yaklaşım ortaya atmıştır. Bu üç yaklaşım, deterministik eylemler yerine stokastik eylemlere izin vererek ve müfredat öğrenimi adı verilen yeni bir öğrenme tekniği tanıtılarak genişletilmiştir. Müfredat öğrenimi ile ortamın karmaşıklığı kademeli olarak arttırıldığında, beklenen ödül üzerinde olumlu bir etkisinin olduğu tespit edilmiştir. İki kuantum yaklaşımı için ihtiyaç duyulan eğitim adımı sayısının klasik yaklaşıma göre daha düşük olduğu gözlenmiştir.

ÜÇÜNCÜ BÖLÜM
MATERYAL VE YÖNTEM

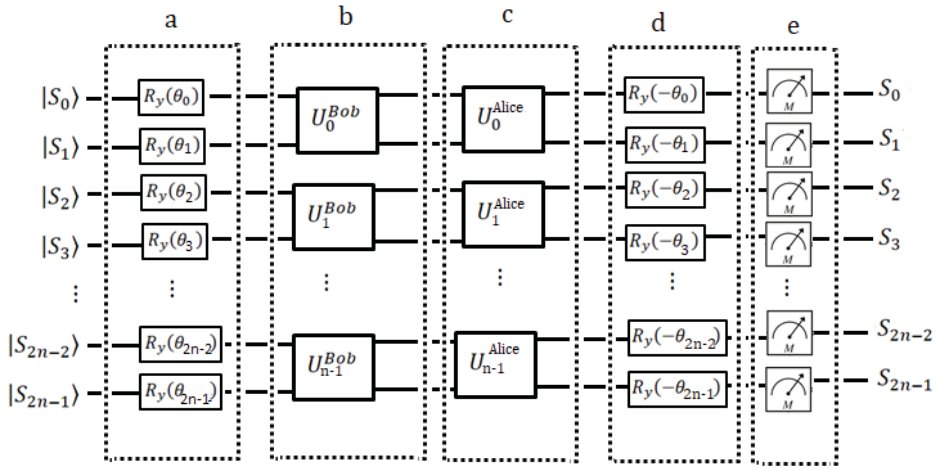
Bu bölümde KTÖ ile anahtar üretimi için bir model önerilmektedir. Bu modelde gizli anahtarın nasıl üretileceğinin bilgisi, kuantum teknolojileri kullanılarak öğretilmektedir. Öğrenme eylemi için MKS'nin öğeleri kuantum mekaniği ilkelerine göre temsil edilmektedir. Model iki tane hata kontrolü içermektedir. Son olarak güvenli iletişim için bir yöntem sunulmuştur. Bu bölümde sunulan bilgiler, International Journal Of Information Security Science dergisinin 2023 yılı 12(2) cilt sayısında "Secure Communication Based On Key Generation With Quantum Reinforcement Learning" başlıklı makale olarak yayınlanmıştır. Bu çalışma, Türk Patent ve Marka kurumu tarafından TR 2021 019962 B patent numarası ile tescillenmiştir. Ayrıca Patentle Türkiye 3. Üniversiteler Patent Yarışması'nda 7.'lik ödülüne layık görülmüştür.

3.1.Kuantum Takviyeli Öğrenme ile Anahtar Üretimi

Geleneksel takviyeli öğrenmede olduğu gibi, KTÖ'de ajan, durum uzayı ve ödül olmak üzere üç ana unsurdan oluşmaktadır. Bir KTÖ sistemi oluşturmak için MKS'deki faktörler, kuantum mekaniğinin ilkeleri aracılığıyla temsil edilir. Takviyeli öğrenme algoritmalarındaki durumlar ve eylemler, KTÖ'de ortogonal bazlar olarak temsil edilir. KTÖ'de bunlara öz durumlar ve öz eylemler denir (Dong vd., 2008). Bu tez çalışmasında MKS'ne göre, S durum uzayı iki kubit ile, A eylem uzayı Identity (I), NOT (X), CNOT ile, ödül fonksiyonu {0,1} ile gösterilmektedir. Gerek geleneksel gerekse kuantum takviyeli öğrenme çalışmalarında seçilen eylemler birbirini takip etmektedir. Yapılan seçim bir önceki seçime bağlıdır. Bu tez çalışmasında ise eylem uzayında yapılan her seçim bağımsızdır ve bir diğer seçimi etkilemez. Yapılan seçim bir kuantum kapıdır. İki kubitlik bir kuantum durum kullanılarak bir adet kuantum kapı öğretilmektedir. 2n kubitlik kuantum durum ile n tane kuantum kapı öğretilmektedir. Bu n kuantum kapı n bitlik gizli anahtarı oluşturmak için kullanılır.

Bu tez çalışması için geliştirilen KTÖ yöntemi, iki kullanıcının veri transferi için kuantum kanal kullanmaktadır. Kuantum kanalın çevreden etkilenmediği ve veri kaybı olmadığı kabul edilmiştir. İletişimi başlatan gönderen taraf Alice, alıcı taraf Bob ve

iletişimi yetkisiz olarak dinleyerek gizli bilgileri elde etmeye çalışan taraf ise Eve olarak adlandırılmıştır.



Şekil 7. Kuantum Takviyeli Öğrenme ile Anahtar Üretimi a. Alice'in, kuantum duruma rotasyon kapısını uygulaması. b. Bob'un, kuantum duruma aday kapıları uygulaması. c. Alice'in, Bob tarafından değiştirilen kuantum duruma kendi kapılarını uygulaması. d. Alice'in, kuantum duruma negatif açı ile rotasyon kapısının uygulaması. e. Alice'in, kuantum durumu ölçmesi.

Alice ve Bob, KTÖ için aşağıdaki adımları takip eder(Şekil 7):

Adım 1: Alice, 2n kubitlik kuantum durum hazırlar.Alice, Identity (I), NOT (X), CNOT kapıları arasından n tane seçim yapar. Rotasyon kapısı için 2n tane açıya karar verir.

Adım 2: Alice, her bir kubit için farklı açı kullanarak kuantum duruma 2n tane rotasyon kapısı uygular (Şekil 7a).

Adım 3: Bob, n adet aday kapı seçer ve Alice'in gönderdiği kuantum duruma bu kapıları uygular (Şekil 7b).

Adım 4: Alice, kuantum duruma kendi kapılarını uygular. Bob ve Alice!in aynı kapıyı uyguladığı kubitler Şekil 7a'daki kuantum duruma gelir. Eğer bir kapı kuantum duruma arka arkaya iki kere uygulanırsa kuantum durum başlangıç durumuna geri gelir (Şekil 7c).

Adım 5: Alice, Adım 2'de kullandığı açıların negatifini kullanarak kuantum duruma rotasyon kapısı uygular. Bob ve Alice'in aynı kapıyı uyguladıkları kubitler başlangıçta hazırlandıkları gibi olurlar (Şekil 7d).

Adım 6: Alice, kuantum durumunu ölçtükten sonra ölçüm sonucunu kuantum durumunu oluşturmak için kullandığı veri seti ile karşılaştırır. Ölçüm sonucuna göre ödül değeri belirlenir (Şekil 7e).

3.1.1. Anahtar Üretimi için Gerekli Kapıların Öğretilmesi

Bu bölümde gizli anahtarı oluşturmak için kullanılan kapılar Alice tarafından KTÖ ile Bob'a öğretilir. Her kapı birbirinden bağımsız olarak öğretilir. N kapı için n farklı öğrenme eylemi gerçekleştirilir. Alice, {I, X, CNOT} kapıları içerisinden gizli anahtarı oluşturmak için kullanacağı n tane kapıyı rastgele belirler. Alice'in seçmiş olduğu kapılar aşağıda gösterildigi gibidir:

$$U_i^{Bob} = u_0^b, u_1^b, \dots, u_{n-1}^b \,;\, u_i^b \in \{\mathrm{I}, \mathrm{X}, \mathrm{CNOT}\}\,;\;\; i = 1 \dots n-1 \tag{3.1}$$

Bob, {I, X, CNOT} kapıları içerisinden rastgele n tane aday kapı seçer. Bob'un amacı Alice'in seçtiği kapıyı seçebilmektir. Yaptığı seçimin doğru olup olmadığı Alice'in vereceği ödül değerine göre belirlenecektir. Bob'un seçmiş olduğu kapılar aşağıda gösterildiği gibidir:

$$U_i^{Bob} = u_0^b, u_1^b, \dots, u_{n-1}^b \,;\, u_i^b \in \{\mathrm{I}, \mathrm{X}, \mathrm{CNOT}\}\,;\;\; i = 1 \dots n-1 \tag{3.2}$$

Alice, n tane kapı için 2n kubitlik kuantum durumu aşağıdaki gibi hazırlar:

$$\begin{aligned} &\mathrm{S} = s_0 s_1 \dots s_{2n-1}\,;\; s_i \in \{0,1\}; i = 0 \dots 2\mathrm{n}-1 \\ &|\psi\rangle = |s_0 s_1 s_2 s_3 \dots s_{2n-2} s_{2n-1}\rangle \end{aligned} \tag{3.3}$$

Alice, $|\psi\rangle$ kuantum durumuna farklı açılarda 2n tane rotasyon kapısını uygulayarak farklı genliklerdeki süperpozisyon durumunu aşağıdaki gibi elde eder:

$$
\begin{aligned}
&|\psi'\rangle = R_y(\theta)|\psi\rangle = \otimes_{i=0}^{2n-1} R_y(\theta_i)|s_i\rangle \\
&= R_y(\theta_0)|s_0\rangle \otimes R_y(\theta_1)|s_1\rangle \otimes .. \otimes R_y(\theta_{2n-2})|s_{2n-2}\rangle \otimes R_y(\theta_{2n-1})|s_{2n-1}\rangle \\
&= |s'_0 s'_1 s'_2 s'_3 .. s'_{2n-2} s'_{2n-1}\rangle \quad , \quad s' = \alpha|0\rangle + \beta|1\rangle
\end{aligned} \tag{3.4}
$$

Alice, elde etmiş olduğu $|\psi'\rangle$ kuantum durumunu Bob'a gönderir. Denklem 3.4'deki gibi süperpozisyon durumundaki bir kuantum durum ölçüldüğü zaman 0 ya da 1 değerlerinden birisi elde edilir. Eve ya da Bob, $|\psi'\rangle$ kuantum durumunu ölçtüğü zaman Denklem 3.3'deki $|\psi\rangle$ kuantum durumunu elde edemezler. Böylece veri güvenliği sağlanmış olur.

$$
\begin{aligned}
&|\psi''\rangle = U_i^{Bob}|\psi'\rangle = \otimes_{i=0}^{n-1} u_i^b |s'_{2i} s'_{2i+1}\rangle \\
&= u_0^b|s'_0 s'_1\rangle \otimes u_1^b|s'_2 s'_3\rangle \otimes \ldots \otimes u_{n-1}^b|s'_{2n-2} s'_{2n-1}\rangle \\
&= |s'_0 s''_1 s'_2 s''_3 .. s'_{2n-2} s''_{2n-1}\rangle
\end{aligned} \tag{3.5}
$$

Bob, $|\psi'\rangle$ kuantum durumuna aday kapıları Denklem 3.5'teki gibi uygular. Aday kapılar {I, X, CNOT}kapıları içerisinden seçilmiştir: CNOT kapısı iki kubite uygulanan bir kapıdır. İlk kubit kontrol kubitidir, ikinci kubit ise hedef kubittir. Kontrol kubitinin 1 değerine sahip olmasına göre hedef kubite NOT kapısı uygulanır. $|s'_0\rangle, |s'_2\rangle, \ldots, |s'_{2n-2}\rangle$ kubitleri kontrol kubitleri olarak adlandırılır. $|s'_1\rangle, |s'_3\rangle, \ldots, |s'_{2n-1}\rangle$ kubitleri ise hedef kubitleri olarak adlandırılır. I ve X kapıları için kontrol kubiti kullanılmayacak olduğundan kapılar 2 kubitlik duruma I⊗I ve I⊗X olarak uygulanır.

Bob, elde ettiği $|\psi''\rangle$ kuantum durumunu Alice gönderir. Alice, $|\psi''\rangle$ kuantum durumuna kendi kapılarını aşağıdaki gibi uygular:

$$
\begin{aligned}
&|\psi'''\rangle = U_i^{Alice}|\psi''\rangle = \otimes_{i=0}^{n-1} u_i |s'_{2i} s''_{2i+1}\rangle \\
&= u_0|s'_0 s''_1\rangle \otimes u_1|s'_2 s''_3\rangle \otimes \ldots \otimes u_{n-1}|s'_{2n-2} s''_{2n-1}\rangle \\
&= |s'_0 s'''_1 s'_2 s'''_3 .. s'_{2n-2} s'''_{2n-1}\rangle
\end{aligned} \tag{3.6}
$$

Alice, Denklem 3.6'daki $|\psi'''\rangle$ kuantum durumunu elde eder. Kuantum kapılar terslenebilir kapılardır. Bir kuantum duruma arka arkaya iki kere aynı kapı uygulanırsa, kuantum durumun başlangıç değeri elde edilir. Alice ve Bob tarafından aynı kapılar

seçildiği zaman kuantum durum Denklem 3.4'deki gibi olur. Farklı kapılar seçildiğinde Denklem 3.4'deki kuantum durumdan farklı bir kuantum durum elde edilir. Başka bir deyişle, s_1''' ve s_1' birbirine eşitse aynı kapı kullanılır. Eğer s_1''' ve s_1' birbirine eşit değilse farklı bir kapı kullanılır. Bir sonraki adımda Alice, negatif açılarla rotasyon kapısını $|\psi'''\rangle$ kuantum durumuna aşağıdaki gibi uygular:

$$\begin{aligned}
&|\psi''''\rangle = R_y(-\theta)|\psi'''\rangle = \otimes_{i=0}^{2n-1} R_y(-\theta_i)|s_i'''\rangle \\
&= R_y(-\theta_0)|s_0'\rangle \otimes R_y(-\theta_1)|s_1'''\rangle \otimes \ldots \otimes R_y(-\theta_{2n-2})|s_{2n-2}'\rangle \otimes R_y(-\theta_{2n-1})|s_{2n-1}'''\rangle \\
&= |s_0'' s_1'''' s_2'' s_3'''' \ldots s_{2n-2}'' s_{2n-1}''''\rangle \\
&S' = s_0'' s_1'''' s_2'' s_3'''' \ldots s_{2n-2}'' s_{2n-1}''''
\end{aligned} \tag{3.7}$$

Denklem 3.4'deki kuantum duruma negatif açı ile rotasyon kapısı uygulanırsa kuantum durum, süperpozisyon durumundan kurtulur. Fakat Alice ve Bob'un farklı kapıları uyguladıkları kubitlerin genlikleri bozulduğu için bu kubitler süperpozisyon halinde kalırlar. Süperpozisyon durumundaki kubitler ölçüldüğü zaman 0 veya 1 sonucunu verir. Alice, bir sonraki adımda Denklem 3.7'deki kuantum durumu ölçer. Alice, ölçüm sonucu olarak 2n bitlik klasik bir veri elde eder. Alice, Denklem 3.7'de elde edilen 2n bitlik klasik veri ile Denklem 3.3'deki 2n bitlik klasik veriyi karşılaştırır. Alice, aynı değere sahip bitler için ödül değerini "1", farklı değere sahip bitler için ise ödül değerini "0" olarak belirler. Alice, ödül değerini Bob'a gönderir. Daha sonra Denklem 3.3'deki $|\psi\rangle$ kuantum durumunu yeniden oluşturur ve adımları tekrarlar. Bob, yeni kuantum durum için ödül değeri "1" olan kubitlere uygulanan kapıları değiştirmez. Ödül değeri "0" olan kubitlere uygulanan kapıları değiştirir. Daha önce seçtiğinden farklı bir kapı seçer. Bu algoritma tüm ödül değerleri "1" olana kadar tekrarlanır. Tüm ödül değerleri "1" olduğu zaman kontrol kubitinin gözden geçirilmesi gerekmektedir. Kontrol kubitinin 0 değerine sahip olması durumunda $CNOT$ ve I kapıları aynı işlemi yapar. 1 değerine sahip olması durumunda ise CNOT ve X kapıları aynı işlemi yapar. Bu nedenle kontrol kubitine NOT kapısını uygulanarak adımlar tekrarlanır. Alice ve Bob, aynı kapıları seçtiyse ödül değerlerinin tamamı "1" olarak kalır. Daha sonra hata kontrolleri başlatılır. Eğer ödül değeri 0 olan bitler var ise onlar 1 olana kadar algoritmanın adımları tekrar edilir.

Alice ve Bob'un aynı kapıyı seçtiği durumlarda öğrenme çıktısının değeri %100 olasılıkla 1 olur. Aynı kapıyı seçtikleri zaman genlikler korunacağı için ölçüm sonucu

Alice'in kendi oluşturduğu bitin değeri olur. Eve'nin araya girmesi durumunda genlikler bozulur. Alice ve Bob aynı kapıyı seçmiş olsa bile genlikler bozulduğu için ölçüm sonucu Alice'in kendi oluşturduğu bitin değerinden farklı olabilir. Bu durumda Alice ve Bob, aynı kapıyı seçmiş olsa bile ödül değeri 0 olur. Araya gireni tespit etmek için her bir tekrarda Alice, ödül değeri 0 olan kapıların %50 sini duyurur. Bob, duyurulan kapılar ile kendi kapılarını karşılaştırır. Eğer iki kapı birbirinin aynısı ise Bob, Eve'nin varlığını duyurur.

n=4 değeri için yukarıdaki adımlar aşağıdaki gibi örneklendirilebilir:

Adım 1: Alice, $U_i^{Alice} = \{X, CNOT, I, X\}$ gibi dört tane kapıya sahip olsun. Alice, dört kapı için $|\psi\rangle = |01101011\rangle$ gibi sekiz kubitlik kuantum durum oluşturur.

Adım 2: Alice, $|\psi\rangle$ kuantum durumuna her bir kubite farklı açı olacak şekilde rotasyon kapısını uygular. Fakat bu örnek için tüm kubitlere $\frac{\pi}{3}$ açısıyla rotasyon kapısı uygulanmıştır. $|0\rangle$ durumuna rotasyon kapısının uygulanması $R_y\left(\frac{\pi}{3}\right)|0\rangle = \cos\frac{\pi}{6}|0\rangle + \sin\frac{\pi}{6}|1\rangle = \frac{\sqrt{3}}{2}|0\rangle + \frac{1}{2}|1\rangle$ ve $|1\rangle$ durumuna rotasyon kapısının uygulanması $R_y\left(\frac{\pi}{3}\right)|1\rangle = -\sin\frac{\pi}{6}|0\rangle + \cos\frac{\pi}{6}|1\rangle = -\frac{1}{2}|0\rangle + \frac{\sqrt{3}}{2}|1\rangle$ şeklinde olur.

Alice, kuantum duruma rotasyon kapısını uyguladıktan sonra kuantum durumu Bob'a gönderir.

$$
\begin{aligned}
&|\psi'\rangle = \otimes_{i=0}^{2n-1} R_y\left(\frac{\pi}{3}\right)|01101011\rangle \\
&= \left(\frac{\sqrt{3}}{2}|0\rangle + \frac{1}{2}|1\rangle\right) \otimes \left(-\frac{1}{2}|0\rangle + \frac{\sqrt{3}}{2}|1\rangle\right) \\
&\otimes \left(-\frac{1}{2}|0\rangle + \frac{\sqrt{3}}{2}|1\rangle\right) \otimes \left(\frac{\sqrt{3}}{2}|0\rangle + \frac{1}{2}|1\rangle\right) \\
&\otimes \left(-\frac{1}{2}|0\rangle + \frac{\sqrt{3}}{2}|1\rangle\right) \otimes \left(\frac{\sqrt{3}}{2}|0\rangle + \frac{1}{2}|1\rangle\right) \\
&\otimes \left(-\frac{1}{2}|0\rangle + \frac{\sqrt{3}}{2}|1\rangle\right) \otimes \left(-\frac{1}{2}|0\rangle + \frac{\sqrt{3}}{2}|1\rangle\right)
\end{aligned}
$$

$$= \left(-\frac{\sqrt{3}}{4}|00\rangle + \frac{3}{4}|01\rangle - \frac{1}{4}|10\rangle + \frac{\sqrt{3}}{4}|11\rangle\right)$$
$$\otimes \left(-\frac{\sqrt{3}}{4}|00\rangle - \frac{1}{4}|01\rangle + \frac{3}{4}|10\rangle + \frac{\sqrt{3}}{4}|11\rangle\right)$$
$$\otimes \left(-\frac{\sqrt{3}}{4}|00\rangle - \frac{1}{4}|01\rangle + \frac{3}{4}|10\rangle + \frac{\sqrt{3}}{4}|11\rangle\right)$$
$$\otimes \left(\frac{1}{4}|00\rangle - \frac{\sqrt{3}}{4}|01\rangle - \frac{\sqrt{3}}{4}|10\rangle + \frac{3}{4}|11\rangle\right)$$

Adım 3: Bob, n tane aday kapı seçer ve kapıları kuantum duruma uygular. Daha sonra kuantum durumu Alice gönderir.

$$U_i^{Bob} = \{CNOT, CNOT, I, X\}$$
$$|\psi''\rangle = CNOT\left(-\frac{\sqrt{3}}{4}|00\rangle + \frac{3}{4}|01\rangle - \frac{1}{4}|10\rangle + \frac{\sqrt{3}}{4}|11\rangle\right)$$
$$\otimes CNOT\left(-\frac{\sqrt{3}}{4}|00\rangle - \frac{1}{4}|01\rangle + \frac{3}{4}|10\rangle + \frac{\sqrt{3}}{4}|11\rangle\right)$$
$$\otimes (I \otimes I)\left(-\frac{\sqrt{3}}{4}|00\rangle - \frac{1}{4}|01\rangle + \frac{3}{4}|10\rangle + \frac{\sqrt{3}}{4}|11\rangle\right)$$
$$\otimes (I \otimes X)\left(\frac{1}{4}|00\rangle - \frac{\sqrt{3}}{4}|01\rangle - \frac{\sqrt{3}}{4}|10\rangle + \frac{3}{4}|11\rangle\right)$$
$$= \left(-\frac{\sqrt{3}}{4}|00\rangle + \frac{3}{4}|01\rangle - \frac{1}{4}|11\rangle + \frac{\sqrt{3}}{4}|10\rangle\right)$$
$$\otimes \left(-\frac{\sqrt{3}}{4}|00\rangle - \frac{1}{4}|01\rangle + \frac{3}{4}|11\rangle + \frac{\sqrt{3}}{4}|10\rangle\right)$$
$$\otimes \left(-\frac{\sqrt{3}}{4}|00\rangle - \frac{1}{4}|01\rangle + \frac{3}{4}|10\rangle + \frac{\sqrt{3}}{4}|11\rangle\right)$$
$$\otimes \left(\frac{1}{4}|01\rangle - \frac{\sqrt{3}}{4}|00\rangle - \frac{\sqrt{3}}{4}|11\rangle + \frac{3}{4}|10\rangle\right)$$

Adım 4: Alice kendi kuantum kapılarını, kuantum duruma uygular.

$$U_i^{Alice} = \{X, CNOT, I, X\}$$

$$|\psi'''\rangle = U_i^{Alice}|\psi''\rangle$$

$$= (I\otimes X)\left(-\frac{\sqrt{3}}{4}|00\rangle + \frac{3}{4}|01\rangle - \frac{1}{4}|11\rangle + \frac{\sqrt{3}}{4}|10\rangle\right)$$

$$\otimes CNOT\left(-\frac{\sqrt{3}}{4}|00\rangle - \frac{1}{4}|01\rangle + \frac{3}{4}|11\rangle + \frac{\sqrt{3}}{4}|10\rangle\right)$$

$$\otimes (I\otimes I)\left(-\frac{\sqrt{3}}{4}|00\rangle - \frac{1}{4}|01\rangle + \frac{3}{4}|10\rangle + \frac{\sqrt{3}}{4}|11\rangle\right)$$

$$\otimes (I\otimes X)\left(\frac{1}{4}|01\rangle - \frac{\sqrt{3}}{4}|00\rangle - \frac{\sqrt{3}}{4}|11\rangle + \frac{3}{4}|10\rangle\right)$$

$$= \left(-\frac{\sqrt{3}}{4}|01\rangle + \frac{3}{4}|00\rangle - \frac{1}{4}|10\rangle + \frac{\sqrt{3}}{4}|11\rangle\right)$$

$$\otimes \left(-\frac{\sqrt{3}}{4}|00\rangle - \frac{1}{4}|01\rangle + \frac{3}{4}|10\rangle + \frac{\sqrt{3}}{4}|11\rangle\right)$$

$$\otimes \left(-\frac{\sqrt{3}}{4}|00\rangle - \frac{1}{4}|01\rangle + \frac{3}{4}|10\rangle + \frac{\sqrt{3}}{4}|11\rangle\right)$$

$$\otimes \left(\frac{1}{4}|00\rangle - \frac{\sqrt{3}}{4}|01\rangle - \frac{\sqrt{3}}{4}|10\rangle + \frac{3}{4}|11\rangle\right)$$

$$= \left[\frac{\sqrt{3}}{2}|0\rangle\otimes\left(\frac{\sqrt{3}}{2}|0\rangle - \frac{1}{2}|1\rangle\right) + \frac{1}{2}|1\rangle\otimes\left(-\frac{1}{2}|0\rangle + \frac{\sqrt{3}}{2}|1\rangle\right)\right]$$

$$\otimes \left(-\frac{1}{2}|0\rangle + \frac{\sqrt{3}}{2}|1\rangle\right)\otimes\left(\frac{\sqrt{3}}{2}|0\rangle + \frac{1}{2}|1\rangle\right)$$

$$\otimes \left(-\frac{1}{2}|0\rangle + \frac{\sqrt{3}}{2}|1\rangle\right)\otimes\left(\frac{\sqrt{3}}{2}|0\rangle + \frac{1}{2}|1\rangle\right)$$

$$\otimes \left(-\frac{1}{2}|0\rangle + \frac{\sqrt{3}}{2}|1\rangle\right)\otimes\left(-\frac{1}{2}|0\rangle + \frac{\sqrt{3}}{2}|1\rangle\right)$$

Alice ve Bob'un aynı kapıyı uyguladıkları kubitlerin, Adım 2'deki formuna geri döndüğü görülmektedir. Bob, ilk iki kubit için $CNOT$ kapısını uygulamıştır. Alice ise, ilk iki kubit için X kapısını seçip $(I\otimes X)$ şeklinde uygulamıştır. Alice ve Bob, farklı kapıları uyguladıkları için diğer kubitlerin aksine ilk iki kubitin Adım 2 ve Adım 4'deki formları bir birinden farklıdır. İlk iki kubitin başlangıç değeri $|01\rangle$'dir. İlk iki kubite sırasıyla Alice $R_y\left(\frac{\pi}{3}\right)$, Bob $CNOT$ ve Alice $(I\otimes X)$ kapılarını uygulamıştır. Alice son olarak $R_y\left(-\frac{\pi}{3}\right)$

kapısını uygular. Eğer ilk iki kubite Alice ve Bob, aynı kapıları uygularsa, $R_y\left(-\frac{\pi}{3}\right)$ kapısının uygulanmasından sonra $|01\rangle$ elde edilmesi gerekir. Fakat ilk iki kubitin genlikleri bozulduğu için başlangıç değeri tekrar elde edilememektedir. İlk iki kubit süperpozisyondan kurtulamamaktadır. Alice ve Bob'un aynı kapıyı seçtiği kubitler ise $R_y\left(-\frac{\pi}{3}\right)$ kapısı uygulandıktan sonra süperpozisyondan kurtulup tekrar başlangıç değerlerine gelirler.

Adım 5: Alice, kuantum duruma negatif açı ile rotasyon kapısını uygular.

$$|\psi''''\rangle = R_y(-\theta)|\psi'''\rangle$$

$$= \left(R_y\left(-\frac{\pi}{3}\right) \otimes R_y\left(-\frac{\pi}{3}\right)\right)$$

$$\left[\frac{\sqrt{3}}{2}|0\rangle \otimes \left(\frac{\sqrt{3}}{2}|0\rangle - \frac{1}{2}|1\rangle\right) + \frac{1}{2}|1\rangle \otimes \left(-\frac{1}{2}|0\rangle + \frac{\sqrt{3}}{2}|1\rangle\right)\right]$$

$$\otimes R_y\left(-\frac{\pi}{3}\right)\left(-\frac{1}{2}|0\rangle + \frac{\sqrt{3}}{2}|1\rangle\right) \otimes R_y\left(-\frac{\pi}{3}\right)\left(\frac{\sqrt{3}}{2}|0\rangle + \frac{1}{2}|1\rangle\right)$$

$$\otimes R_y\left(-\frac{\pi}{3}\right)\left(-\frac{1}{2}|0\rangle + \frac{\sqrt{3}}{2}|1\rangle\right) \otimes R_y\left(-\frac{\pi}{3}\right)\left(\frac{\sqrt{3}}{2}|0\rangle + \frac{1}{2}|1\rangle\right)$$

$$\otimes R_y\left(-\frac{\pi}{3}\right)\left(-\frac{1}{2}|0\rangle + \frac{\sqrt{3}}{2}|1\rangle\right) \otimes R_y\left(-\frac{\pi}{3}\right)\left(-\frac{1}{2}|0\rangle + \frac{\sqrt{3}}{2}|1\rangle\right)$$

$$= \left(R_y\left(-\frac{\pi}{3}\right) \otimes R_y\left(-\frac{\pi}{3}\right)\right)$$

$$\left[\frac{\sqrt{3}}{2}|0\rangle \otimes \left(\frac{\sqrt{3}}{2}|0\rangle - \frac{1}{2}|1\rangle\right) + \frac{1}{2}|1\rangle \otimes \left(-\frac{1}{2}|0\rangle + \frac{\sqrt{3}}{2}|1\rangle\right)\right]$$

$$\otimes|1\rangle \otimes|0\rangle \otimes|1\rangle \otimes|0\rangle \otimes|1\rangle \otimes|1\rangle$$

$$|\psi''''\rangle = \left(\frac{3}{8}|00\rangle - \frac{2-3\sqrt{3}}{8}|01\rangle - \frac{\sqrt{3}}{4}|10\rangle + \frac{3+2\sqrt{3}}{8}|11\rangle\right) \otimes |101011\rangle$$

Aynı kapıların uygulandığı kubitlerin süperpozisyondan kurtulup başlangıç değerine döndüğü görülmektedir. Fakat ilk iki kubit süperpozisyondan kurtulamamıştır.

Adım 6: Alice, Adım 5'teki kuantum durumu ölçer.

Alice, $|\psi''''\rangle = \left|\left(\frac{3}{8}|00\rangle - \frac{2-3\sqrt{3}}{8}|01\rangle - \frac{\sqrt{3}}{4}|10\rangle + \frac{3+2\sqrt{3}}{8}|11\rangle\right) \otimes |101011\rangle\right.$ kuantum durumuna sahiptir. $|\psi''''\rangle$ kuantum durumunun ölçülmesinden sonra Alice ölçüm sonucu olarak, "00101011", "01101011", "10101011" ya da "11101011" değerlerinden birine sahiptir.

Ölçüm sonucunun "00101011" olduğu kabul edilerek "01101011" ve "00101011" karşılaştırılır. İkinci kubitlerin birbirinden farklı olduğu açıkça görülmektedir. Alice'in başlangıç verisinde ikinci kubitin değeri "1" iken ölçüm sonucunda "0"'dır. Alice, ikinci kubit için ödül değerini "0" olarak belirler. Diğer kubitlerin ölçüm sonucundaki değerleri ile başlangıç verisindeki değerlerinin aynı olduğu görülmektedir. Bu nedenle Alice, bu kubitlerin ödül değerini "1" olarak belirler. Alice, Bob'a "10111111" ödül değerini gönderir. İkinci kubitin ödül değerinin sıfır olmasından dolayı Alice, yeni bir kuantum durum oluşturur ve adımları tekrar eder. Bob, yeni kuantum durumda ödül değeri "1" olan kubitler için daha önce uyguladığı kapıları uygular. Yani, ödül değeri "1" olan kubitler için kapıları değiştirmez. Ödül değeri "0" olan kubitler için ise uygulanan kapıyı değiştirmesi gerekmektedir. Bob, ilgili kubit için daha önce uygulamadığı kapılar içerisinden bir seçim yapar. Bob, birinci tekrarda ilk iki kubit için $CNOT$ kapısını seçmişti. İkinci tekrarda Bob, I ya da X kapılarından birini seçer. Alice ve Bob, tüm ödül değerleri "1" olana kadar işlemleri tekrar eder.

Ölçüm sonucunun "01101011" olduğu kabul edilerek "01101011" ve "01101011" karşılaştırılır. Her iki veri aynı olduğundan dolayı, Alice tüm ödül değerlerini "1" olarak işaretler. Kontrol kubitinin "1" olduğu durumda X ve $CNOT$ kapısı, "0" olduğu durumda ise I ve $CNOT$ kapısı aynı işlevi görmektedir. Farklı kapılar seçildiği halde ödül değerinin "1" olduğu durumlar Tablo 5'de gösterilmiştir. Alice, $|\psi\rangle$ kuantum durumundaki kontrol kubitine NOT kapısını uyguladıktan sonra adımları tekrar eder. Bob, ödül değeri olarak "1" aldığı için yapmış olduğu kapı seçimlerinden hiçbir değişiklik yapmaz. Kontrol kubitine NOT kapısı uygulandıktan sonra yapılan tekrarda Alice ve Bob'un farklı kapılara sahip olduğu ilgili kubitler için ödül değerinin "0" olması beklenmektedir. Bob, ödül değeri "0" olan kubitler için ilgili kapıları değiştirir. Fakat rotasyon kapısının uygulanması nedeniyle kuantum durum süperpozisyon halindedir. Süperpozisyon hali ödül değerinin "1" olarak alınmasına neden olabilir. Verilen örnek incelendiği zaman NOT kapısı

uygulandıktan sonra da ödül değerinin "1" olduğu görülmektedir. İlk iki kubit için Alice X kapısını, Bob ise $CNOT$ kapısını seçmiştir. Kontrol kubiti "0" olduğu için Bob hedef kubit üzerinde bir değişiklik yapmazken, Alice X kapısını uygulamıştır. Ödül değeri "0" olması beklenirken süperpozisyondan dolayı ödül değeri "1" olmuştur. Kontrol kubitine NOT kapısı uygulandıktan sonra yapılan tekrarda, Alice'in X kapısı ve Bob'un $CNOT$ kapısı aynı davranışı uygular. Kontrol kubiti "1" olduğu için her ikisi de hedef kubite NOT işlemi uygular. Bu nedenle ödül, %100 olasılıkla "1" değerine sahip olur. Kuantum durumlarının süperpozisyon ilkesi Bob'un yanlış kapıyı kabul etmesine neden olmuştur. Bölüm 3.1.2'deki hata kontrolleri yoluyla kabul edilen yanlış kapılar tespit edildikten sonra iptal edilir.

Tablo 5

Alice ve Bob'un farklı kapıları seçtiği durumlar

İlk Kuantum Durum*	**Bob**		**Alice**	**Son Kuantum Durum**	**Ödül**
$\|00\rangle$	I	$\|00\rangle$	CNOT	$\|00\rangle$	1
$\|10\rangle$	I	$\|10\rangle$	CNOT	$\|11\rangle$	0
$\|01\rangle$	I	$\|01\rangle$	CNOT	$\|01\rangle$	1
$\|11\rangle$	I	$\|11\rangle$	CNOT	$\|10\rangle$	0
$\|10\rangle$	X	$\|11\rangle$	CNOT	$\|10\rangle$	1
$\|00\rangle$	X	$\|01\rangle$	CNOT	$\|01\rangle$	0
$\|11\rangle$	X	$\|10\rangle$	CNOT	$\|11\rangle$	1
$\|01\rangle$	X	$\|00\rangle$	CNOT	$\|00\rangle$	0

$* \ |q_0 q_1\rangle, q_0 : Kontrol\ kubit \ \ q_1 : Hedef\ kubit$

3.1.2. Anahtar için Hata Kontrolü

Bir önceki bölümde kuantum mekaniği ilkelerinden kaynaklı olarak Bob'un yanlış kapıları kabul edebileceği görülmüştür. Bu hataların nedeni Alice ve Bob'un farklı kapıları seçmeleridir. İki katılımcının bu yanlış kapıları tespit ederek iptal etmeleri gerekmektedir. Bunun gerçekleştirilebilmesi için iki farklı hata kontrolü gerekmektedir. Birinci hata kontrolü, taraflardan birinin I diğerinin ise X kapısını seçtiği durumları tespit eder. Diğer

hata kontrolü ise taraflardan birinin $CNOT$ diğerinin ise I ya da X kapısını seçtiği durumları tespit eder.

Birim (Identity)-NOT Hata Kontrolü:

Bu hata kontrol yöntemi, taraflardan birinin I, diğerinin X kapısını seçtiği durumları tespit etmek içindir. Her iki taraf da Kuantum hesaplama ile gizli anahtarı oluşturur. Bu gizli anahtar, mesajın XOR işlemiyle şifrelenmesi için kullanılır. Şifrelenmiş mesajların aşağıdaki adımlarda belirtildiği gibi değiştirilmesi yoluyla yanlış kapılar tespit edilir. Daha sonra hatalı kapılar katılımcılar tarafından iptal edilir.

Alice ve Bob aşağıdaki gibi kapılara sahiptirler:

$$U_i^{Alice} = u_0, u_1, .., u_{n-1}\,; u_i \in \{\mathrm{I}, \mathrm{X}, \mathrm{CNOT}\}\,;\ \ i = 1 \ldots n-1$$
$$U_i^{Bob} = u_0^b, u_1^b, \ldots, u_{n-1}^b\,; u_i^b \in \{\mathrm{I}, \mathrm{X}, \mathrm{CNOT}\}\,;\ \ i = 1 \ldots n-1$$

Birim (Identity)-NOT Hata Kontrolü için algoritma aşağıdaki gibidir:

Adım 1: Alice, 2n kubitlik bir kuantum durum hazırlar ve gizli anahtarı oluşturur.

$$\mathrm{S} = s_0 s_1 \ldots s_{2n-1}\,;\ s_i \in \{0,1\}; i = 0 \ldots 2\mathrm{n}-1$$
$$|\psi\rangle = |s_0 s_1 s_2 s_3 \ldots s_{2n-2} s_{2n-1}\rangle \qquad (3.8)$$
$s_0, s_2, \ldots, s_{2n-2}$ (Kontrol Kubitler), $s_1, s_3, \ldots, s_{2n-1}$ (Hedef Kubitler)

Adım 2: Alice, $s_0, s_2, \ldots, s_{2n-2}$ kubitlerini kontrol kubiti olarak kabul ederek kendi kapılarını $|\psi\rangle$ kuantum durumuna uygular.

$$|\psi'\rangle = U_i^{Alice}|\psi\rangle = \otimes_{i=0}^{n-1} u_i |s_{2i} s_{2i+1}\rangle$$
$$= u_0|s_0 s_1\rangle \otimes u_1|s_2 s_3\rangle \otimes \ldots \otimes u_{n-1}|s_{2n-2} s_{2n-1}\rangle \qquad (3.9)$$
$$= |s_0 s_1' s_2 s_3' .. s_{2n-2} s_{2n-1}'\rangle$$

Adım 3: Alice, $|\psi'\rangle$ kuantum durumundaki hedef kubitleri ölçerek gizli anahtarı elde eder.

$$\mathrm{K}^{Alice} = k_0 k_1 \dots k_{n-1}\ ;\ \mathrm{k}_i\ \in \{0,1\}; i = 0 \dots \mathrm{n}-1 \tag{3.10}$$

Adım 4: Alice, gizli anahtarı oluşturmak için kullandığı kuantum durumun aynısını tekrar oluşturur ve Bob'a gönderir. Bob, $s_0, s_2, \dots, s_{2n-2}$ kubitlerini kontrol kubiti olarak kabul ederek kendi kapılarını $|\psi\rangle$ kuantum durumuna uygular.

$$\begin{aligned} |\psi'\rangle &= U_i^{Bob}|\psi\rangle = \otimes \, {}^{n-1}_{i=0} u_i^b |s_{2i} s_{2i+1}\rangle \\ &= u_0^b |s_0 s_1\rangle \otimes u_1^b |s_2 s_3\rangle \otimes \dots \otimes u_{n-1}^b |s_{2n-2} s_{2n-1}\rangle \\ &= |s_0 s_1'' s_2 s_3'' .. s_{2n-2} s_{2n-1}''\rangle \end{aligned} \tag{3.11}$$

Adım 5: Bob, kuantum durumu ölçer. Bob, hedef kubitlerde yaptığı ölçümün sonucunu gizli anahtar olarak saklar. Bob, kontrol kubitlerinde yaptığı ölçümün sonucunu $ControlBits^{Bob}$ isimli dizide saklar.

$$\begin{aligned} \mathrm{K}^{Bob} &= k_0^{Bob} k_1^{Bob} \dots k_{n-1}^{Bob}\ ;\ k_i^{Bob}\ \in \{0,1\}; i = 0..\mathrm{n}-1 \\ ControlBits^{Bob} &= \ s_0, s_2, \dots, s_{2n-2}\ ;\ \mathrm{s}_{2i}\ \in \{0,1\}; i = 0..\mathrm{n}-1 \end{aligned} \tag{3.12}$$

Alice ve Bob, kendilerine ait kapıları $|\psi\rangle$ kuantum durumuna uygulayarak bir gizli anahtar üretir. Her ikisi de aynı kapılara sahipse oluşturulan gizli anahtarın aynı olması gerekir. Her ikisi de aynı gizli anahtara sahipse, birinin şifrelemiş olduğu metnin şifresi diğeri tarafından çözülebilir. Her ikisi de mesajı şifrelemek ve şifresini çözmek için klasik bitler üzerinde XOR işlemini kullanır.

Adım 6: Alice, mesaj için n bit klasik veri hazırlar.

$$\mathrm{M} = m_0 m_1 \dots m_{n-1}\ ;\ \mathrm{m}_i\ \in \{0,1\}; i = 0 \dots \mathrm{n}-1 \tag{3.13}$$

Adım 7: Alice, Denklem 3.13'deki mesaja ve Denklem 3.10'daki gizli anahtara XOR işlemini uygulayarak Denklem 3.14'deki şifreli mesajı elde eder.

$$\mathrm{C} = (k_0 \oplus m_0)(k_1 \oplus m_1) \dots (k_{n-1} \oplus m_{\mathrm{n}-1}) \tag{3.14}$$

$$\mathrm{C} = c_0 c_1 \dots c_{n-1}\ ;\ \ \mathrm{c}_i\ \in \{0,1\};\ i = 0 \dots \mathrm{n}-1$$

Adım 8: Alice, şifreli mesajı Bob'a gönderir. Bob, kendi anahtarını kullanarak orijinal mesaja ulaşmalıdır. Bob, Denklem 3.14'deki şifreli mesaja ve Denklem 3.12'deki gizli anahtara XOR işlemini uygulayarak Denklem 3.15'deki şifresi çözülmüş mesajı elde eder.

$$\begin{aligned} &\mathrm{M}' = \left(k_0^{Bob} \oplus c_0\right)\left(k_1^{Bob} \oplus c_1\right) \dots \left(k_{n-1}^{Bob} \oplus c_{n-1}\right) \\ &\mathrm{M}' = m_0' m_1' \dots m_{n-1}'\ ;\ m_i' \in \{0,1\}; i = 0 \dots \mathrm{n}-1 \end{aligned} \tag{3.15}$$

Adım 9: Bob, Denklem 3.12'deki $ControlBits^{Bob}$ dizisinde saklanan bitleri kontrol kubiti olarak ve Denklem 3.15'deki M' mesajının bitlerini hedef kubit olarak kullanarak Denklem 3.16 daki $|\varphi\rangle$ kuantum durumunu hazırlar. Bob, hazırlamış olduğu bu kuantum duruma kendi kapılarını uygular.

$$\begin{aligned} &|\varphi\rangle = |s_0 m_0' s_2 m_1' \dots s_{2n-2} m_{n-1}'\rangle\ ;\ \ s_{2i}\ \in \{0,1\};\ m_i'\ \in \{0,1\}; i = 0..\mathrm{n}-1 \\ &|\varphi'\rangle = U_i^{Bob}|\varphi\rangle = \otimes_{i=0}^{n-1} u_i^b |s_{2i} m_i'\rangle \\ &= u_0^b |s_0 m_0'\rangle \otimes u_1^b |s_2 m_1'\rangle \otimes \dots \otimes u_{n-1}^b |s_{2n-2} m_{n-1}'\rangle \\ &= |s_0 m_0'' s_2 m_1'' \dots s_{2n-2} m_{n-1}''\rangle \end{aligned} \tag{3.16}$$

Adım 10: Bob, Denklem 3.16'daki $|\varphi'\rangle$ kuantum durumun hedef kubitlerini ölçer ve ölçüm sonucunda ikinci gizli anahtar $\mathrm{K}^{Bob'}$'nü elde eder.

$$\mathrm{K}^{Bob'} = k_0^{Bob'} k_1^{Bob'} \dots k_{n-1}^{Bob'}\ ;\ k_i^{Bob'}\ \in \{0,1\}; i = 0..\mathrm{n}-1 \tag{3.17}$$

Adım 11: Bob, Denklem 3.15 deki şifresi çözülmüş mesaja ve Denklem 3.17'deki gizli anahtara XOR işlemini uygulayarak Denklem 3.18'deki şifreli mesajı elde eder.

$$\begin{aligned} &\mathrm{C}' = \left(k_0^{Bob'} \oplus m_0'\right)\left(k_1^{Bob'} \oplus m_1'\right) \dots \left(k_{n-1}^{Bob'} \oplus m_{n-1}'\right) \\ &\mathrm{C}' = c_0' c_1' \dots c_{n-1}'\ ;\ c_i' \in \{0,1\};\ i = 0 \dots \mathrm{n}-1 \end{aligned} \tag{3.18}$$

Adım 12: Bob, Denklem 3.18'deki şifreli mesajı Alice gönderir. Alice, Denklem 3.8'deki kontrol kubitlerini ve Denklem 3.13'deki orijinal mesaj M'nin bitlerini hedef kubit olarak kullanarak Denklem 3.19'daki $|\Phi\rangle$ kuantum durumunu hazırlar. Alice, hazırlamış olduğu bu kuantum duruma kendi kapılarını uygular.

$$
\begin{aligned}
&|\Phi\rangle = |s_0 m_0 s_2 m_1 \dots s_{2n-2} m_{\mathrm{n}-1}\rangle\,;\ \ \mathrm{s}_{2i} \in \{0,1\};\ m_{\mathrm{i}} \in \{0,1\}; i = 0..\mathrm{n}-1 \\
&|\Phi'\rangle = U_i^{Alice}|\Phi\rangle = \otimes \textstyle\sum_{i=0}^{n-1} u_i |s_{2i} m_i\rangle \\
&= u_0|s_0 m_0\rangle \otimes u_1|s_2 m_1\rangle \otimes \dots \otimes u_{n-1}|s_{2n-2} m_{\mathrm{n}-1}\rangle \\
&= |s_0 m_0''' s_2 m_1''' \dots s_{2n-2} m_{n-1}'''\rangle
\end{aligned}
\tag{3.19}
$$

Adım 13: Alice, Denklem 3.19'daki $|\Phi'\rangle$ kuantum durumunun hedef kubitlerin ölçer ve ölçüm sonucunda gizli anahtar $\mathrm{K}^{Alice'}$'nü elde eder.

$$
\mathrm{K}^{Alice'} = k'_0 k'_1 \dots k'_{n-1}\,;\ \mathrm{k}'_i \in \{0,1\}; i = 0\dots\mathrm{n}-1 \tag{3.20}
$$

Adım 14: Denklem 3.17'deki $\mathrm{K}^{Bob'}$ ve Denklem 3.20'deki $\mathrm{K}^{Alice'}$ aynı değere sahiptir. Alice, Denklem 3.18'deki şifreli mesaja ve Denklem 3.20'deki gizli anahtara XOR işlemini uygulayarak Denklem 3.21'deki şifresi çözülmüş mesajı elde eder.

$$
\begin{aligned}
&\mathrm{M}^4 = (k'_0 \oplus c'_0)(k'_1 \oplus c'_1) \dots (k'_{n-1} \oplus c'_{n-1}) \\
&\mathrm{M}^4 = m_0^4 m_1^4 \dots m_{n-1}^4\ ;\ m_i^4 \in \{0,1\}; i = 0\dots\mathrm{n}-1
\end{aligned}
\tag{3.21}
$$

Denklem 3.15'deki M' mesajı ile Denklem 21'deki M^4 mesajı aynı değere sahiptir. Alice, Bob'un M' mesajına sahiptir. Alice, orijinal mesaj M ile M^4 mesajını karşılaştırır. Alice, farklı bitlere ait olan kapıları yanlış kapı olarak işaretler. Alice, Bob'a yanlış kapıları bildirir ve her ikisi de yanlış kapıları iptal eder.

$n = 4$ değeri için aşağıdaki gibi örneklendirilebilir:

Alice ve Bob'un kapıları $U_i^{Alice} = \{X, CNOT, I, X\}, U_i^{Bob} = \{I, CNOT, I, X\}$ olsun.

Adım 1: $|\psi\rangle = |01110110\rangle$

Adım 2: $|\psi'\rangle = U_i^{Alice}|\psi\rangle = (I \otimes X)|01\rangle \otimes CNOT|11\rangle \otimes (I \otimes I)|01\rangle \otimes (I \otimes X)|10\rangle$

$= |00\rangle \otimes |10\rangle \otimes |01\rangle \otimes |11\rangle = |00100111\rangle$

Adım 3: $\mathrm{K}^{Alice} = 0011$

Adım 4: $|\psi'\rangle = U_i^{Bob}|\psi\rangle = (I \otimes I)|01\rangle \otimes CNOT|11\rangle \otimes (I \otimes I)|01\rangle \otimes (I \otimes X)|10\rangle$

$= |01\rangle \otimes |10\rangle \otimes |01\rangle \otimes |11\rangle = |01100111\rangle$

Adım 5: $\mathrm{K}^{Bob} = 1011$, $ControlBits^{Bob} = 0101$

Adım 6: $M = 1011$

Adım 7: $\mathrm{K}^{Alice} = 0011$, M=1011

$\mathrm{C} = (0 \oplus 1)(0 \oplus 0)(1 \oplus 1)(1 \oplus 1) = 1000$

Adım 8: $\mathrm{K}^{Bob} = 1011$, $\mathrm{C} = 1000$

$\mathrm{M}' = (1 \oplus 1)(0 \oplus 0)(1 \oplus 0)(1 \oplus 0) = 0011$

Alice'in Adım 6'daki orijinal mesajı, Bob'un Adım 8'deki şifresi çözülmüş mesajıyla karşılaştırıldığı zaman ilk bitlerinin farklı olduğu görülmektedir. Bu, iki tarafın gizli anahtarlarındaki ilk bitin birbirinden farklı olduğu anlamına gelir. Dolayısı ile iki kullanıcının ilk bit için kullanmış oldukları kapılar farklıdır. Bu nedenle bu anahtar bitini üreten kapının iptal edilmesi gerekmektedir. Alice ya da Bob, kapının iptal edilmesi konusunda bir karar verememektedir. Çünkü diğeri kullanıcının mesajının ne olduğunu bilmemektedirler. Alice $M = 1011$ mesajına ve Bob $M' = 0011$ mesajına sahiptir. Karar verebilmek için taraflardan birinin hem M hem de M' mesajına sahip olması gerekmektedir. Bob'un M' mesajını Alice'e doğru şekilde göndermesi sağlanmalıdır. Bunun için Bob ve Alice'in aynı anahtara sahip olması gerekmektedir. Verilen örnekte Alice'in Adım 3'deki anahtarı, Bob'un Adım 5'deki anahtarıyla karşılaştırıldığında anahtarların ilk bitinin farklı olduğu görülmektedir. Bob, M' mesajının ilk biti ile hazırladığı hedef kubite kendi kapısını uygular.

$\mathrm{M}' = 0011$, $U_i^{Bob} = \{I, CNOT, I, X\}$

$I|0\rangle = |0\rangle$

Bob, $|0\rangle$ durumunu ölçtüğü zaman ölçüm sonucu olarak "0" değeri elde eder. Alice, M mesajının ilk biti ile hazırladığı hedef kubite kendi kapısını uygular.

M=1011, $U_i^{Alice} = \{X, CNOT, I, X\}$

$X|1\rangle = |0\rangle$

Alice, $|0\rangle$ durumunu ölçtüğü zaman ölçüm sonucu olarak "0" değeri elde eder. Alice ve Bob aynı bit değerini üretirler. Alice ve Bob, hedef kubitleri olarak sahip oldukları mesajı (M, M') kullanırlarsa aynı anahtarı üretebilirler.

Adım 9: $\mathrm{ControlBits^{Bob}} = 0101\ ;\ \mathrm{M'} = 0011\ ;\ \mathrm{U_i^{Bob}} = \{\mathrm{I}, \mathrm{CNOT}, \mathrm{I}, \mathrm{X}\}$

$|\varphi\rangle = |00100111\rangle$

$|\varphi'\rangle = \mathrm{U_i^{Bob}}|\varphi\rangle = (\mathrm{I}\otimes\mathrm{I})|00\rangle\otimes\mathrm{CNOT}|10\rangle\otimes(\mathrm{I}\otimes\mathrm{I})|01\rangle\otimes(\mathrm{I}\otimes\mathrm{X})|11\rangle$

$= |00\rangle\otimes|11\rangle\otimes|01\rangle\otimes|10\rangle = |00110110\rangle$

Adım 10: $\mathrm{K^{Bob'}} = 0110$

Adım 11: $\mathrm{M'} = 0011\ ;\ \mathrm{K^{Bob'}} = 0110$

$\mathrm{C'} = (0\oplus0)(1\oplus0)(1\oplus1)(0\oplus1) = 0101$

Adım 12: $\mathrm{ControlBits^{Alice}} = 0101\ ;\ \mathrm{M} = 1011\ ;\ \mathrm{U_i^{Alice}} = \{\mathrm{X}, \mathrm{CNOT}, \mathrm{I}, \mathrm{X}\}$

$|\Phi\rangle = |01100111\rangle$

$|\Phi'\rangle = \mathrm{U_i^{Alice}}|\Phi\rangle = (\mathrm{I}\otimes\mathrm{X})|01\rangle\otimes\mathrm{CNOT}|10\rangle\otimes(\mathrm{I}\otimes\mathrm{I})|01\rangle\otimes(\mathrm{I}\otimes\mathrm{X})|11\rangle$

$= |00\rangle\otimes|11\rangle\otimes|01\rangle\otimes|10\rangle = |00110110\rangle$

Adım 13: $\mathrm{K^{Alice'}} = 0110$

Adım 14: $\mathrm{C'} = 0101\ ;\ \mathrm{K^{Alice'}} = 0110$

$\mathrm{M^4} = (0\oplus0)(1\oplus1)(1\oplus0)(0\oplus1) = 0011$

Adım 8'deki $\mathrm{M'} = 0011$ mesajı ve Adım 14'deki $\mathrm{M^4} = 0011$ mesajı aynı değere sahiptir. Alice, $\mathrm{M^4}$ mesajı ile Bob'un $\mathrm{M'}$ mesajına sahip olmuştur. Bob, $\mathrm{C} = 1000$ şifreli mesajının şifresini çözerek $\mathrm{M'} = 0011$ mesajını elde etmiştir. $\mathrm{M'} = 0011$ mesajının orijinal mesaj $\mathrm{M} = 1011$ ile aynı olması beklenmektedir. Alice, orijinal mesaj $\mathrm{M} = 1011$ ile $\mathrm{M^4} = 0011$ mesajını karşılaştırır. Alice, farklı bitlere ait olan kapıları yanlış kapı olarak işaretler ve Bob'a yanlış kapıları bildirir. Her ikisi de yanlış kapıları iptal eder.

Tarafların CNOT ve Birim/NOT Hata Kontrolü:

Bu hata yöntemi, iki taraftan birinin $CNOT$, diğerinin ise I veya X kapısını seçtiği durumları tespit etmek içindir. Alice $3n$ bitlik veri seti hazırlar ve bu veri setini Bob ile paylaşır. İlk n-bitlik veri seti kontrol bitidir ve diğer iki veri seti hedef bitlerdir. Bob ve Alice, veri setlerini kullanarak ikişer tane gizli anahtar üretir. Bob, bir mesaj oluşturur.

Daha sonra kendisine ait iki gizli anahtarı kullanarak mesajı ayrı ayrı şifreler ve iki adet şifreli mesaj oluşturur. Bob, şifrelenmiş mesajları Alice'e gönderir. Alice, kendisine ait iki gizli anahtarı kullanarak şifreli mesajların şifresini çözerek iki adet şifresi çözülmüş mesaj elde eder. Alice'in elde ettiği iki mesaj tek bir mesajdan türetilmiştir. Eğer Alice ve Bob, gizli anahtarları oluşturmak için aynı kapıları kullanmışlar ise bu iki mesajın aynı olması beklenir. Alice, elde ettiği iki mesajı kıyaslar. Alice, farklı bitlere ait olan kapıları yanlış kapı olarak işaretler. Alice, Bob'a yanlış kapıları bildirir ve her ikisi de yanlış kapıları iptal eder.

Alice ve Bob, aşağıdaki gibi kapılara sahiptir:

$$U_i^{Alice} = u_0, u_1, .., u_{n-1}\,; u_i \in \{\mathrm{I}, \mathrm{X}, \mathrm{CNOT}\}\,;\ \ i = 1 \ldots n-1$$
$$U_i^{Bob} = u_0^b, u_1^b, \ldots, u_{n-1}^b\,; u_i^b \in \{\mathrm{I}, \mathrm{X}, \mathrm{CNOT}\}\,;\ \ i = 1 \ldots n-1$$

CNOT-(Identity/NOT) Hata Kontrolü için algoritma aşağıdaki gibidir:

Adım 1: Alice, $3n$ bitlik klasik veriyi Bob ile paylaşır.

$$\mathrm{S}^1 = \mathrm{s}_0^1 \mathrm{s}_1^1 \ldots \mathrm{s}_{n-1}^1\,;\ \mathrm{s}_i^1 \in \{0,1\}; i = 0 \ldots \mathrm{n}-1 \tag{3.22}$$
$$\mathrm{S}^2 = \mathrm{s}_0^2 \mathrm{s}_1^2 \ldots \mathrm{s}_{n-1}^2\,;\ \mathrm{s}_i^2 \in \{0,1\}; i = 0 \ldots \mathrm{n}-1 \tag{3.23}$$
$$\mathrm{S}^3 = \mathrm{s}_0^3 \mathrm{s}_1^3 \ldots \mathrm{s}_{n-1}^3\,;\ \mathrm{s}_i^3 \in \{0,1\}; i = 0 \ldots \mathrm{n}-1 \tag{3.24}$$

Adım 2: Her iki kullanıcı, Denklem 3.22'deki bitleri kontrol kubitleri ve Denklem 3.23'deki bitleri hedef kubitleri olarak kabul ederek Denklem 3.25'teki ilk kuantum durumu oluşturur.

$$|\psi^1\rangle = |\mathrm{s}_0^1 \mathrm{s}_0^2 \mathrm{s}_1^1 \mathrm{s}_1^2 \ldots \mathrm{s}_{n-1}^1 \mathrm{s}_{n-1}^2\rangle\,; \left|\mathrm{s}_i^1 \mathrm{s}_i^2\right\rangle \in \{0,1\}; i = 0 \ldots \mathrm{n}-1 \tag{3.25}$$

Adım 3: Her iki kullanıcı, Denklem 3.22'deki bitlerin NOT uygulanmış hallerini kontrol kubitleri ve Denklem 3.24'deki bitleri hedef kubitleri olarak kabul ederek Denklem 3.26'daki ikinci kuantum durumu oluşturur.

$$|\psi^2\rangle = |NOT(\mathrm{s}_0^1)\mathrm{s}_0^3 NOT(\mathrm{s}_1^1)\mathrm{s}_1^3 \ldots NOT(\mathrm{s}_{n-1}^1)\mathrm{s}_{n-1}^3\rangle\,; \tag{3.26}$$

$\left|s_i^1 s_i^3\right\rangle \in \{0,1\}; i = 0 \ldots n-1$

Adım 4: Alice, Denklem 3.25'deki kuantum duruma ve Denklem 3.26'daki kuantum duruma kendi kapılarını uygular.

$$\begin{aligned}
&\left|\psi_1^{Alice}\right\rangle = U_i^{Alice}|\psi^1\rangle = \otimes_{i=0}^{n-1} u_i \left|s_i^1 s_i^2\right\rangle \\
&= u_0|s_0^1 s_0^2\rangle \otimes u_1|s_1^1 s_1^2\rangle \otimes \ldots \otimes u_{n-1}|s_{n-1}^1 s_{n-1}^2\rangle \qquad (3.27)\\
&= \left|s_0^1 s_0^{2'} s_1^1 s_1^{2'} \ldots s_{n-1}^1 s_{n-1}^{2'}\right\rangle \\
&\left|\psi_2^{Alice}\right\rangle = U_i^{Alice}|\psi^2\rangle = \otimes_{i=0}^{n-1} u_i \left|NOT(s_i^1) s_i^3\right\rangle \\
&= u_0|NOT(s_0^1) s_0^3\rangle \otimes u_1|NOT(s_1^1) s_1^3\rangle \otimes \ldots \otimes u_{n-1}|NOT(s_{n-1}^1) s_{n-1}^3\rangle \qquad (3.28)\\
&= \left|NOT(s_0^1) s_0^{3'} NOT(s_1^1) s_1^{3'} \ldots NOT(s_{n-1}^1) s_{n-1}^{3'}\right\rangle
\end{aligned}$$

Adım 5: Bob, Denklem 3.25'deki kuantum duruma ve Denklem 3.26'daki kuantum duruma kendi kapılarını uygular.

$$\begin{aligned}
&\left|\psi_1^{Bob}\right\rangle = U_i^{Bob}|\psi^1\rangle = \otimes_{i=0}^{n-1} u_i^b \left|s_i^1 s_i^2\right\rangle \\
&= u_0^b|s_0^1 s_0^2\rangle \otimes u_1^b|s_1^1 s_1^2\rangle \otimes \ldots \otimes u_{n-1}^b|s_{n-1}^1 s_{n-1}^2\rangle \qquad (3.29)\\
&= \left|s_0^1 s_0^{2'} s_1^1 s_1^{2'} \ldots s_{n-1}^1 s_{n-1}^{2'}\right\rangle \\
&\left|\psi_2^{Bob}\right\rangle = U_i^{Bob}|\psi^2\rangle = \otimes_{i=0}^{n-1} u_i^b \left|NOT(s_i^1) s_i^3\right\rangle \\
&= u_0^b|NOT(s_0^1) s_0^3\rangle \otimes u_1^b|NOT(s_1^1) s_1^3\rangle \otimes \ldots \otimes u_{n-1}^b|NOT(s_{n-1}^1) s_{n-1}^3\rangle \qquad (3.30)\\
&= \left|NOT(s_0^1) s_0^{3'} NOT(s_1^1) s_1^{3'} \ldots NOT(s_{n-1}^1) s_{n-1}^{3'}\right\rangle
\end{aligned}$$

Adım 6: Alice, Denklem 3.27'deki kuantum durumun hedef kubitlerini ölçer ve ölçüm sonucunda Denklem 3.31'deki gizli anahtar K^{Alice_1}'i elde eder.

$$K^{Alice_1} = k_0^{Alice_1} k_1^{Alice_1} \ldots k_{n-1}^{Alice_1};\ k_i^{Alice_1} \in \{0,1\}; i = 0..n-1 \qquad (3.31)$$

Adım 7: Alice, Denklem 3.28'deki kuantum durumun hedef kubitlerini ölçer ve ölçüm sonucunda Denklem 3.32'deki gizli anahtar K^{Alice_2}'yi elde eder.

$$K^{Alice_2} = k_0^{Alice_2} k_1^{Alice_2} \ldots k_{n-1}^{Alice_2};\ k_i^{Alice_2} \in \{0,1\}; i = 0..n-1 \qquad (3.32)$$

Adım 8: Alice, Denklem 3.29'deki kuantum durumun hedef kubitlerini ölçer ve ölçüm sonucunda Denklem 3.33'deki gizli anahtar K^{Bob_1}'i elde eder.

$$\mathrm{K}^{Bob_1} = k_0^{Bob_1} k_1^{Bob_1} \dots k_{n-1}^{Bob_1} \; ; \; k_i^{Bob_1} \in \{0,1\}; i = 0..\mathrm{n}-1 \tag{3.33}$$

Adım 9: Alice, Denklem 3.30'deki kuantum durumun hedef kubitlerini ölçer ve ölçüm sonucunda Denklem 3.34'deki gizli anahtar K^{Bob_2}'yi elde eder.

$$\mathrm{K}^{Bob_2} = k_0^{Bob_2} k_1^{Bob_2} \dots k_{n-1}^{Bob_2} \; ; \; k_i^{Bob_2} \in \{0,1\}; i = 0..\mathrm{n}-1 \tag{3.34}$$

Adım 10: Alice ve Bob, aynı kapıları seçerlerse her iki kullanıcı da aynı anahtarlara sahip olur. Kullanıcılardan biri $CNOT$ kapısını diğerinin I veya X kapısını seçerse, Bob'un anahtarlarından biri Alice'in anahtarıyla aynı değere sahipken diğeri farklı bir değere sahip olur. Yani Bob'un anahtarlarından biri geçerli iken diğeri geçersiz anahtar olur. Bob, bir mesaj oluşturur ve mesajı her iki anahtarla ayrı ayrı şifreleyerek iki adet şifreli mesaj üretir. Daha sonra bu şifreli mesajları Alice'e gönderir. Alice şifrelenmiş mesajları kendi anahtarlarını kullanarak çözer ve iki farklı mesaj elde eder. Mesajları karşılaştırarak yanlış kapıları tespit eder. Bob, Denklem 3.35'teki mesajı hazırlar.

$$\mathrm{M} = m_0 m_1 \dots m_{n-1} \; ; \; \mathrm{m}_i \in \{0,1\}; i = 0 \dots \mathrm{n}-1 \tag{3.35}$$

Adım 11: Bob, Denklem 3.35'deki mesaja ve Denklem 3.33'deki gizli anahtara XOR işlemini uygulayarak Denklem 3.36'deki şifreli mesajı elde eder.

$$\begin{aligned} \mathrm{C}^1 &= \left(k_0^{Bob_1} \oplus m_0\right)\left(k_1^{Bob_1} \oplus m_1\right) \dots \left(k_{n-1}^{Bob_1} \oplus m_{\mathrm{n}-1}\right) \\ \mathrm{C}^1 &= \mathrm{c}_0^1 \mathrm{c}_1^1 \dots \mathrm{c}_{n-1}^1 \; ; \; \mathrm{c}_i^1 \in \{0,1\}; \; i = 0 \dots \mathrm{n}-1 \end{aligned} \tag{3.36}$$

Adım 12: Bob, Denklem 3.35'deki mesaja ve Denklem 3.34'deki gizli anahtara XOR işlemini uygulayarak Denklem 3.37'deki şifreli mesajı elde eder.

$$\begin{aligned} \mathrm{C}^2 &= \left(k_0^{Bob_2} \oplus m_0\right)\left(k_1^{Bob_2} \oplus m_1\right) \dots \left(k_{n-1}^{Bob_2} \oplus m_{\mathrm{n}-1}\right) \\ \mathrm{C}^2 &= \mathrm{c}_0^2 \mathrm{c}_1^2 \dots \mathrm{c}_{n-1}^2 \; ; \; \mathrm{c}_i^2 \in \{0,1\}; \; i = 0 \dots \mathrm{n}-1 \end{aligned} \tag{3.37}$$

Adım 13: Bob, C^1 ve C^2 şifreli mesajlarını Alice gönderir. Alice, Denklem 3.36'daki şifreli mesaja ve Denklem 3.31'deki gizli anahtara XOR işlemini uygulayarak Denklem 3.38'deki şifresi çözülmüş mesajı elde eder.

$$M^1 = \left(k_0^{Alice_1} \oplus \mathrm{c}_0^1\right)\left(k_1^{Alice_1} \oplus \mathrm{c}_1^1\right) \dots \left(k_{n-1}^{Alice_1} \oplus \mathrm{c}_{n-1}^1\right)$$
$$\mathrm{M}^1 = \mathrm{m}_0^1 \mathrm{m}_1^1 \dots \mathrm{m}_{n-1}^1 \; ; \;\; \mathrm{m}_i^1 \in \{0,1\}; \; i = 0 \dots \mathrm{n} - 1 \tag{3.38}$$

Adım 14: Alice, Denklem 3.37'daki şifreli mesaja ve Denklem 3.32'deki gizli anahtara XOR işlemini uygulayarak Denklem 3.39'daki şifresi çözülmüş mesajı elde eder.

$$M^2 = \left(k_0^{Alice_2} \oplus \mathrm{c}_0^2\right)\left(k_1^{Alice_2} \oplus \mathrm{c}_1^2\right) \dots \left(k_{n-1}^{Alice_2} \oplus \mathrm{c}_{n-1}^2\right)$$
$$\mathrm{M}^2 = \mathrm{m}_0^2 \mathrm{m}_1^2 \dots \mathrm{m}_{n-1}^2 \; ; \;\; \mathrm{m}_i^2 \in \{0,1\}; \; i = 0 \dots \mathrm{n} - 1 \tag{3.39}$$

Alice, aynı mesajdan türetilmiş iki tane şifresi çözülmüş mesaja sahiptir. Bob, yanlış kapıları seçerse hatalı gizli anahtara sahip olur. Böylece mesajı yanlış şifreler. Alice ise yanlış şifrelenmiş mesajdan, orijinal mesajı elde edemez. Bu nedenle Alice'in mesajlarından biri, Bob'un yanlış kapı seçimi yüzünden orijinal mesajdan farklı içeriğe sahiptir. Diğeri ise orijinal mesajla aynı içeriğe sahip olur. Alice M^1 mesajını, M^2 mesajıyla karşılaştırır. Alice, farklı bitlere ait olan kapıları yanlış kapı olarak işaretler. Alice, Bob'a yanlış kapıları bildirir ve her ikisi de yanlış kapıları iptal eder.

$n = 4$ değeri için aşağıdaki gibi örneklendirilebilir:

Alice ve Bob'un kapıları $U_i^{Alice} = \{X, CNOT, I, X\}, U_i^{Bob} = \{CNOT, CNOT, I, X\}$ olsun.

Adım 1: $\mathrm{S}^1 = 1001 \; ; \; \mathrm{S}^2 = 0111 \; ; \; \mathrm{S}^3 = \; 1100$

Adım 2: $|\psi^1\rangle = |10010111\rangle$

Adım 3: $|\psi^2\rangle = |01111000\rangle$

Adım 4: $\left|\psi_1^{\mathrm{Alice}}\right\rangle = \mathrm{U}_\mathrm{i}^{\mathrm{Alice}}|10010111\rangle$

$= (\mathrm{I}\otimes\mathrm{X})|10\rangle\otimes\mathrm{CNOT}|01\rangle\otimes(\mathrm{I}\otimes\mathrm{I})|01\rangle\otimes(\mathrm{I}\otimes\mathrm{X})|11\rangle$

$= |11\rangle\otimes|01\rangle\otimes|01\rangle\otimes|10\rangle = |11010110\rangle$

$\left|\psi_2^{\mathrm{Alice}}\right\rangle = \mathrm{U}_\mathrm{i}^{\mathrm{Alice}}|01111000\rangle$

$= (\mathrm{I}\otimes\mathrm{X})|01\rangle\otimes\mathrm{CNOT}|11\rangle\otimes(\mathrm{I}\otimes\mathrm{I})|10\rangle\otimes(\mathrm{I}\otimes\mathrm{X})|00\rangle$

$= |00\rangle\otimes|10\rangle\otimes|10\rangle\otimes|01\rangle = |00101001\rangle$

Adım 5: $\left|\psi_1^{\mathrm{Bob}}\right\rangle = \mathrm{U}_{\mathrm{i}}^{\mathrm{Bob}}|10010111\rangle$

$= \mathrm{CNOT}|10\rangle\otimes\mathrm{CNOT}|01\rangle\otimes(\mathrm{I}\otimes\mathrm{I})|01\rangle\otimes(\mathrm{I}\otimes\mathrm{X})|11\rangle$

$= |11\rangle\otimes|01\rangle\otimes|01\rangle\otimes|10\rangle = |11010110\rangle$

$\left|\psi_2^{\mathrm{Bob}}\right\rangle = \mathrm{U}_{\mathrm{i}}^{\mathrm{Bob}}|01111000\rangle$

$= \mathrm{CNOT}|01\rangle\otimes\mathrm{CNOT}|11\rangle\otimes(\mathrm{I}\otimes\mathrm{I})|10\rangle\otimes(\mathrm{I}\otimes\mathrm{X})|00\rangle$

$= |01\rangle\otimes|10\rangle\otimes|10\rangle\otimes|01\rangle = |01101001\rangle$

Adım 6: $\left|\psi_1^{\mathrm{Alice}}\right\rangle = |11010110\rangle\ ;\ \mathrm{K}^{\mathrm{Alice}_1} = 1110$

Adım 7: $\left|\psi_2^{\mathrm{Alice}}\right\rangle = |00101001\rangle\ ;\ \mathrm{K}^{\mathrm{Alice}_2} = 0001$

Adım 8: $\left|\psi_1^{Bob}\right\rangle = |11010110\rangle\ ;\ \mathrm{K}^{Bob_1} = 1110$

Adım 9: $\left|\psi_2^{Bob}\right\rangle = |01101001\rangle\ ;\ \mathrm{K}^{Bob_2} = 1001$

Adım 10: $\mathrm{M} = 1100$

Adım 11: $\mathrm{K}^{Bob_1} = 1110\ ;\ \mathrm{M} = 1100$

$\mathrm{C}^1 = (1\oplus1)(1\oplus1)(1\oplus0)(0\oplus0) = 0010$

Adım 12: $\mathrm{K}^{Bob_2} = 1001\ ;\ \mathrm{M} = 1100$

$\mathrm{C}^2 = (1\oplus1)(0\oplus1)(0\oplus0)(1\oplus0) = 0101$

Adım 13: $\mathrm{K}^{Alice_1} = 1110\ ;\ \mathrm{C}^1 = 0010$

$\mathrm{M}^1 = (1\oplus0)(1\oplus0)(1\oplus1)(0\oplus0) = 1100$

Adım 14: $\mathrm{K}^{Alice_2} = 0001\ ;\ \mathrm{C}^2 = 0101$

$\mathrm{M}^2 = (0\oplus0)(0\oplus1)(0\oplus0)(1\oplus1) = 0100$

Alice $M^1 = 1100$ ve $M^2 = 0100$ mesajlarını karşılaştırarak farklı bitlere ait olan kapıları yanlış kapı olarak işaretler ve Bob'a yanlış kapıları bildirir. Her ikisi de yanlış kapıları iptal eder. Verilen örnekte, ilk kapı iptal edilir. Alice ve Bob aşağıdaki gibi aynı kapılara sahip olur:

$$U_i^{Alice} = \{CNOT, I, X\}\ ;\ U_i^{Bob} = \{CNOT, I, X\}$$

Farklı seçilen kapılar her iki hata kontrolü sayesinde sistemden çıkarılır. Bu sayede her iki tarafın da aynı kapılara sahip olması sağlanır. Bundan sonra her iki taraf da aynı gizli anahtarı oluşturacak bilgiye sahip olur.

3.1.3. Anahtar Üretimi

Bu bölümde anahtar üretimi incelenmektedir. Anahtarlar, yukarıda anlatıldığı gibi KTÖ tarafından öğretilen kuantum kapılar aracılığıyla üretilmektedir.

Alice ve Bob'un aşağıdaki gibi aynı kapılara sahip olması halinde:

$$U_i^{Alice} = u_0, u_1, .., u_{n-1}\,; u_i \in \{\mathrm{I}, \mathrm{X}, \mathrm{CNOT}\}\,;\ \ i = 1 \ldots n-1$$
$$U_i^{Bob} = u_0, u_1, .., u_{n-1}\,; u_i \in \{\mathrm{I}, \mathrm{X}, \mathrm{CNOT}\}\,;\ \ i = 1 \ldots n-1$$

Adım 1: Alice, 2n bitlik veri seti hazırlar.

$$\mathrm{S} = s_0 s_1 \ldots s_{2n-1}\,;\ \mathrm{s}_i \in \{0,1\}; i = 0 \ldots 2\mathrm{n}-1 \tag{3.40}$$

Alice, Denklem 3.40'taki 2n bitlik veri setini Bob'a gönderir.

Adım 2: Alice, Denklem 3.40'taki veri setini kullanarak Denklem 3.41'deki 2n kubitlik kuantum durumu oluşturur.

$$|\psi\rangle = |s_0 s_1 s_2 s_3 \ldots s_{2n-2} s_{2n-1}\rangle \tag{3.41}$$

Adım 3: Alice Denklem 3.41'deki kuantum duruma, kendi kapılarını Denklem 3.42'deki gibi uygular.

$$\begin{aligned} &|\psi'\rangle = U_i^{Alice}|\psi\rangle = \otimes_{i=0}^{n-1} u_i |s_{2i} s_{2i+1}\rangle \\ &= u_0|s_0 s_1\rangle \otimes u_1|s_2 s_3\rangle \otimes \ldots \otimes u_{n-1}|s_{2n-2} s_{2n-1}\rangle \\ &= |s_0 s_1' s_2 s_3' .. s_{2n-2} s_{2n-1}'\rangle \\ &|s_{2i} s_{2\mathrm{i}+1}\rangle, s_{2\mathrm{i}}: Kontrol\ Kubit\ \ s_{2\mathrm{i}+1}: Hedef\ Kubit\ ; i: 0 \ldots n-1 \end{aligned} \tag{3.42}$$

Adım 4: Alice, Denklem 3.42'deki kuantum durumun hedef kubitlerini ölçerek $K_{Alice} = "s_1' s_2' s_3'"$ gizli anahtarını elde eder.

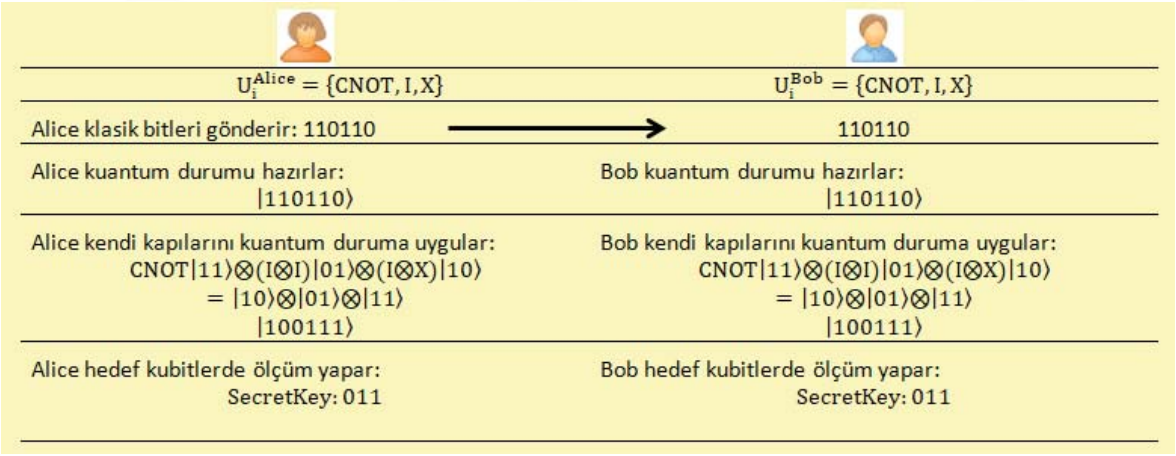
Adım 5: Bob, Denklem 3.40'taki veri setini kullanarak Denklem 3.43'deki 2n kubitlik kuantum durumu oluşturur.

$$|\psi\rangle = |s_0 s_1 s_2 s_3 \dots s_{2n-2} s_{2n-1}\rangle \tag{3.43}$$

Adım 6: Bob Denklem 3.43'deki kuantum duruma, kendi kapılarını Denklem 3.44'deki gibi uygular.

$$\begin{aligned} &|\psi'\rangle = U_i^{Bob}|\psi\rangle = \otimes_{i=0}^{n-1} u_i |s_{2i} s_{2i+1}\rangle \\ &= u_0|s_0 s_1\rangle \otimes u_1|s_2 s_3\rangle \otimes \dots \otimes u_{n-1}|s_{2n-2} s_{2n-1}\rangle \\ &= |s_0 s_1' s_2 s_3' .. s_{2n-2} s_{2n-1}'\rangle \\ &|s_{2i} s_{2i+1}\rangle, s_{2i}: Kontrol\ Kubit\ \ s_{2i+1}: Hedef\ Kubit\ ; i: 0 \dots n-1 \end{aligned} \tag{3.44}$$

Adım 7: Bob, Denklem 3.44'deki kuantum durumun hedef kubitlerini ölçerek $K_{Bob} = "s_1' s_2' s_3'"$ gizli anahtarı elde eder. Her iki katılımcı da gizli anahtarı yerel olarak oluşturur. Anahtar üretiminin örneği Şekil 8'de gösterilmiştir.



Şekil 8. Anahtarların yerel olarak üretilmesi örneği

3.2. Güvenli İletişim Yöntemi:

Bu bölümde iki tarafın güvenli bir şekilde nasıl iletişim kurduğu anlatılmaktadır. Artık her iki taraf da aynı anahtarı oluşturabildiğine göre, güvenli iletişim adımına geçilebilir. Alice ilk olarak 2n bitlik veri setini Denklem 3.45'teki gibi hazırlar.

$$S = s_0 s_1 \dots s_{2n-1}\ ;\ s_i\ \in \{0,1\}; i = 0 \dots 2n-1 \tag{3.45}$$

Alice, Denklem 3.45'teki veri setini Bob'a gönderir. Her iki katılımcı da Denklem 3.45'teki 2n bitlik veri setini kullanarak Denklem 3.46'daki 2n kubitlik kuantum durumu hazırlar.

$$|\psi\rangle = |s_0 s_1 s_2 s_3 \dots s_{2n-2} s_{2n-1}\rangle \tag{3.46}$$

Her iki katılımcı da Denklem 3.46'daki kuantum duruma, kendilerine ait kapıları Denklem 3.47'deki gibi uygular.

$$\begin{aligned} &|\psi'\rangle = U_i|\psi\rangle = \otimes_{i=0}^{n-1} u_i |s_{2i} s_{2i+1}\rangle \\ &= u_0|s_0 s_1\rangle \otimes u_1|s_2 s_3\rangle \otimes \dots \otimes u_{n-1}|s_{2n-2} s_{2n-1}\rangle \\ &= |s_0 s_1' s_2 s_3' .. s_{2n-2} s_{2n-1}'\rangle \\ &|s_{2i} s_{2i+1}\rangle, s_{2i}: Kontrol\ Kubit\ \ s_{2i+1}: Hedef\ Kubit\ ; i: 0 \dots n-1 \end{aligned} \tag{3.47}$$

Her iki katılımcı, Denklem 3.47'deki kuantum durumun hedef kubitlerinde ölçüm yapar. Ölçüm sonuçlarını Denklem 3.48'deki gibi gizli anahtar olarak saklar.

$$K = k_0 k_1 \dots k_{n-1}\ ;\ k_i\ \in \{0,1\}; i = 0 \dots n-1 \tag{3.48}$$

Her iki katılımcı, Denklem 3.48'de elde edilen anahtarın bitlerini toplayarak Denklem 3.49'daki gibi t kaydırma değerini elde eder.

$$t = k_0 + k_1 + \dots + k_{n-1} \tag{3.49}$$

Her iki katılımcı, Denklem 3.49'daki kaydırma değerini kullanarak kendilerine ait kapıları kaydırarak Denklem 3.50'deki gibi sıralı kapıları elde eder.

$$\begin{aligned} &U' = u_{(0+t)\%n}, u_{(1+t)\%n}, .., u_{(n-1+t)\%n}\ ; u_i\ \in \{I, X, CNOT\}\ ;\ \ i = 1 \dots n-1 \\ &U' = u_0', u_1', .., u_{n-1}'\ ; u_i'\ \in \{I, X, CNOT\}\ ;\ \ i = 1 \dots n-1 \end{aligned} \tag{3.50}$$

Böylece her şifreleme işleminde kullanılan gizli anahtarlar farklı şekilde üretilir. Ayrıca her güvenli iletişimde aynı bite uygulanan kapılar birbirinden farklı olur. Sonuç olarak iletişimi yetkisiz dinleyen bir katılımcının örnek veri seti oluşturması da engellenmiş olur. Aynı kapı, aynı bite tekrar tekrar uygulanırsa, yetkisiz dinleyiciler bir veri seti oluşturabilir ve gizli anahtar bilgisini elde etmeye çalışabilir. Yöntemde uygulanan kapılar her seferinde değiştirilerek güvenlik arttırılır.

Her iki katılımcı, Denklem 3.50'deki gibi sıralanmış kapıları Denklem 3.46'daki kuantum duruma uygular.

$$\begin{aligned} |\psi'\rangle &= U_i'|\psi\rangle = \otimes_{i=0}^{n-1} u_i'|s_{2i}s_{2i+1}\rangle \\ &= u_0'|s_0s_1\rangle \otimes u_1'|s_2s_3\rangle \otimes \dots \otimes u_{n-1}'|s_{2n-2}s_{2n-1}\rangle \\ &= |s_0s_1''s_2s_3'' \dots s_{2n-2}s_{2n-1}''\rangle \end{aligned} \tag{3.51}$$

Her iki katılımcı, Denklem 3.47'deki kuantum durumun hedef kubitlerinde ölçüm yapar. Ölçüm sonuçlarını Denklem 3.48'deki gibi gizli anahtar olarak saklar.

$$\mathrm{K}' = k_0'k_1' \dots k_{n-1}' \; ; \; k_i' \in \{0,1\}; i = 0 \dots \mathrm{n}-1 \tag{3.52}$$

Alice, Denklem 3.53'deki gibi n bitlik klasik veriden oluşan mesajını hazırlar.

$$\mathrm{M} = m_0m_1 \dots m_{n-1} \; ; \; \mathrm{m}_i \; \in \{0,1\}; i = 0 \dots \mathrm{n}-1 \tag{3.53}$$

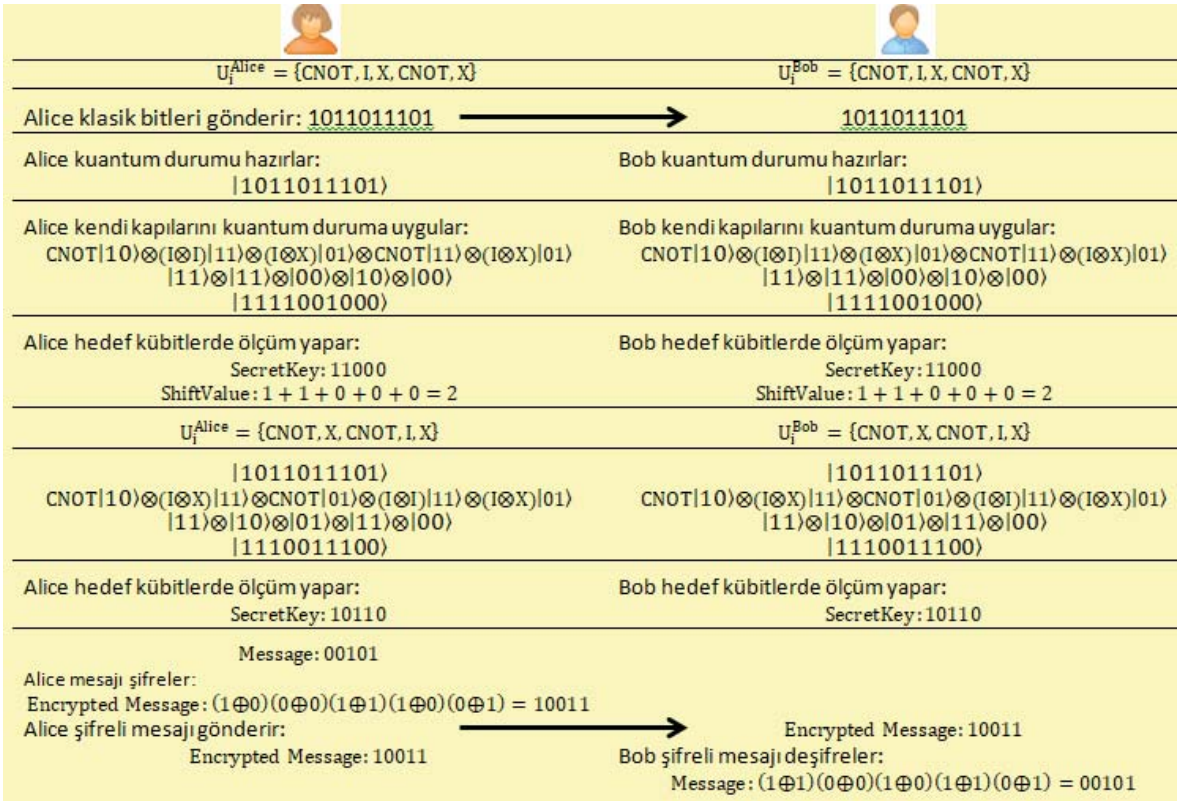
Alice, Denklem 3.53'deki mesaja ve Denklem 3.52'deki gizli anahtara XOR işlemini uygulayarak Denklem 3.54'deki şifreli mesajı elde eder.

$$\begin{aligned} \mathrm{C} &= (k_0' \oplus m_0)(k_1' \oplus m_1) \dots (k_{n-1}' \oplus m_{\mathrm{n}-1}) \\ \mathrm{C} &= c_0c_1 \dots c_{n-1} \; ; \; \mathrm{c}_i \; \in \{0,1\}; \; i = 0 \dots \mathrm{n}-1 \end{aligned} \tag{3.54}$$

Alice, C şifreli mesajını Bob'a gönderir. Bob, Denklem 3.54'deki şifreli mesaja ve Denklem 3.52'deki gizli anahtara XOR işlemini uygulayarak Denklem 3.55'deki şifresi çözülmüş mesajı elde eder. Böylece Alice, Bob'a mesajını güvenli bir şekilde göndermiştir. Güvenli iletişim yöntemi Şekil 9'da örneklendirilmiştir.

$$M = (k'_0 \oplus c_0)(k'_1 \oplus c_1) \dots (k'_{n-1} \oplus c_{n-1})$$

$$M = m_0 m_1 \dots m_{n-1} \; ; \; m_i \in \{0,1\}; i = 0 \dots n-1 \tag{3.55}$$



Şekil 9 Güvenli İletişim Yöntemi Örneği

DÖRDÜNCÜ BÖLÜM
ARAŞTIRMA BULGULARI

4.1. Kuantum Takviyeli Öğrenme ile Anahtar Üretimi Yönteminin Önceki Yöntemlerle Karşılaştırılması

KAD yöntemlerinin, her iletişim için gizli anahtarı güvenli bir şekilde paylaşması gerekir. Geliştirilen KTÖ yöntemi, daha önce geliştirilen KAD yöntemlerinden farklı olarak gizli anahtarın paylaşılmasını gerektirmez. Katılımcılar, gizli anahtarı yerel olarak üretirler. Gizli anahtar, herhangi bir iletişim aracı vasıtasıyla paylaşılmaz. KTÖ yöntemi, kuantum takviyeli öğrenme vasıtasıyla kuantum kapıların öğretilmesine odaklanır. Diğer KAD yöntemleri, KTÖ yönteminin öğrenme eylemi adımları ile benzerlik göstermektedir. KTÖ yönteminin öğrenme adımları ile diğer KAD yöntemlerinin karşılaştırılması aşağıda sunulmuştur.

KTÖ yönteminde Alice, kendi seçmiş olduğu kapıyı Bob'a öğretir. Bob, üç kapı içerisinden bir tanesini seçer. Algoritmanın ilk tekrarını göz önüne alırsak Bob'un, Alice ait kapı bilgisini öğrenme olasılığı %33'dür. Yeterli tekrar sağlandığında %100 olarak Alice ait kapı bilgisini öğrenmesi beklenir. Fakat simülasyon sonuçlarına göre öğrenme eyleminin başarısı yaklaşık %85'tir. Bunun nedeni süperpozisyon ilkesinden kaynaklanan hatalı öğrenmelerdir.

BB84 protokolünde Alice, iki polarizasyon tabanından birini seçerek polarize edilmiş fotonu Bob'a gönderir. Bob, iki polarizasyo tabanından Alice'in seçtiği tabanı seçer ise anahtar oluşturulur. Bu nedenle BB84 protokolünde, iletişimi dinleyen üçüncü bir taraf olmadığı zaman %50 olasılıkla anahtar oluşturulur. BB84 protokolü simüle edildiğinde %46,6 olasılıkla anahtar oluşturduğu görülmüştür (Çağlar vd., 2022).

KTÖ yönteminin tek bir tekrarı ile BB84 protokolü karşılaştırıldığında, BB84 protokolünün daha yüksek olasılıkla anahtar oluşturulduğu görülür. Fakat yeterli tekrar yapıldığı zaman KTÖ yöntemi daha başarılı olur. Simülasyon sonuçlarına göre KTÖ yöntemi %85, BB84 protokolü %46,6 başarı oranına sahiptir. Simülasyon sonuçları, KTÖ yönteminin daha başarılı olduğunu göstermiştir. Ayrıca BB84 protokolünde Alice ve Bob,

her iletişim için anahtar dağıtım işlemi yapmalıdır. KTÖ yönteminde ise öğrenme eylemi bir kere gerçekleştirilir. Alice ve Bob, aynı değere sahip gizli anahtarı %100 olasılıkla yerel olarak üretebilir. Gizli anahtar, daha önceki iletişimlerde kullanılan gizli anahtarlardan farklı olur. Böylece KTÖ yönteminin, BB84 protokolünden daha başarılı olduğu söylenebilir.

B92 protokolünde Alice, 0^0 ve 45^0 polarizsasyon durumlarını kabul eder. Bob ise 90^0 ve 135^0 polarizasyon durumlarını kabul eder. Alice'in göndermiş olduğu polarize fotona bağlı olarak Bob üç farklı olasılığa sahiptir. Bunlardan birincisi Alice ile aynı polarizasyon tabanını kulandığı durumdur. Bu durumda gönderilen foton anahtar biti olarak kabul edilmez. Farklı polarizasyon tabanını kullandığı zaman ise karşısına iki olasılık çıkar ve bunlardan bir tanesi anahtar biti olarak kabul edilir. Yani B92 portokolünde, üç olasılıktan bir tanesi ile anahtar oluşturulur. Dolayısıyla B92 protokolünde, iletişimi dinleyen üçüncü bir taraf olmadığı zaman %33 olasılıkla anahtar oluşturulur. B92 protokolü simüle edildiğinde %29 olasılıkla anahtar oluşturduğu görülmüştür (Çağlar vd., 2022).

KTÖ yönteminin tek bir tekrarı ile B92 protokolü karşılaştırıldığında, iki yönteminde aynı olasılıkla anahtar oluşturulduğu görülür. Simülasyon sonuçlarına göre KTÖ yöntemi %85, B92 protokolü %29 başarı oranına sahiptir. Simülasyon sonuçları, KTÖ yönteminin daha başarılı olduğunu göstermiştir. Ayrıca B92 protokolünde Alice ve Bob, her iletişim için anahtar dağıtım işlemi yapmalıdır. KTÖ yönteminde ise öğrenme eylemi bir kere gerçekleştirilir. Alice ve Bob, aynı değere sahip gizli anahtarı %100 olasılıkla yerel olarak üretebilir. Gizli anahtar, daha önceki iletişimlerde kullanılan gizli anahtarlardan farklı olur. Böylece KTÖ yönteminin, B92 protokolünden daha başarılı olduğu söylenebilir.

Çağlar vd. (2022), yaptıkları çalışmada BB84 ve B92 protokolünün her ikisininde Eve'nin varlığını %22 olasılıkla tespit ettiğini belirtmişlerdir. KTÖ yönteminde ise Eve'nin varlığı, ödül değerinin %100 olasılıkla 1 değerine sahip olması gereken aynı kapının seçildiği durumlarda, ödül değerinin 0 değerine sahip olmasıyla tespit edilir. Eve'nin müdahalesinin sonucunda ödül ya 1 ya da 0 değerini alır. Ödül, 1 değerini aldığında Eve tespit edilemezken 0 değerini aldığında Eve tespit edilir. Böylece KTÖ yönteminin, Eve'yi

%50 olasılıkla tespit ettiği söylenebilir. Eve'yi tespit etme açısından %50 olasılığa sahip KTÖ yönteminin, %22 olasılığa sahip BB84 ve B92 protokolünden daha başarılı olduğu görülmektedir.

Dolanık tabanlı KAD yöntemleri, temel olarak dolanık durum paylaşıldıktan sonra yerel olarak yapılan ölçümler ile anahtar oluşturur. Geliştirilen KTÖ yönteminin, yerel olarak anahtarı üretmesi nedeniyle dolanık tabanlı KAD yöntemleri ile benzerlik gösterdiği söylenebilir.

Kuantum takviyeli öğrenme çalışmaları, bir grid üzerindeki hareketler, bir oyundaki en iyi hamle ya da robotik uygulamaları gibi konulara odaklanır. Bu çalışmalarda gerçekleştirilen bir eylem, kendinden önce gerçekleştirilen eyleme bağlıdır. Geliştirilen KTÖ yönteminde her bir kapının öğretilmesi birbirinden bağımsız bir eylemdir. Geliştirilen KTÖ yönteminin, birbirinden bağımsız öğrenme eylemi gerçekleştirmesi nedeniyle diğer çalışmalardan farklı olduğu söylenebilir.

Klasik yapay sinir ağlarının kullanıldığı anahtar dağıtım yöntemleri, karşılıklı öğrenme yoluyla gizli anahtar oluşturur. Alice ve Bob, aynı giriş değerine ait çıktıları birbirleriyle paylaşarak öğrenme eylemini çift taraflı gerçekleştirir. Geliştirilen KTÖ yönteminde ise, Alice sahip olduğu veriyi Bob'a ödül/ceza sistemiyle öğretir. Klasik olarak güvenli bir iletişim kanalı sağlanamayacağı için yöntemin klasik yapay sinir ağları ile gerçekleştirilmesi mümkün değildir. KTÖ yönteminin, kuantum mekaniğinin üstün özelliklerini kullanması nedeniyle klasik yöntemlere göre daha başarılı olduğu söylenebilir.

4.2. Kuantum Takviyeli Öğrenme ile Anahtar Üretimi Simülasyonu

Bu bölümde Kuantum Takviyeli Öğrenme ile Anahtar Üretimi yöntemi için Pyton programlama dilinin IBM Qiskit kütüphanesinde geliştirilen simülasyona ait kod parçaları sözde kod olarak sunulmuştur.

Adım 1: Alice, *rastgelesec(2)* komutunu kulllanarak 2n bitlik klasik veri seti hazırlar. Komut, 0 ve 1 değerlerinin içerisinden 2n tane rastgele seçim yapar. Yapmış olduğu seçimleri *d_set* isimli diziye ekler.

```
1   BAŞLA
2       n değerini al
3       FOR i=0 TO 2*n-1 STEP +1
4           d_set[i] = rastgelesec(2)
5       ENDFOR
6   BİTİR
```

Alice, kendine ait kapıları oluşturmak için 0, 1 ve 2 rakamları arasından n tane farklı seçim yapar. Burada 0 Identity (I), 1 NOT (X) ve 2 CNOT kapılarını temsil etmektedir.

```
1   BAŞLA
2       n değerini al
3       FOR i=0 TO n-1 STEP +1
4           alice_key[i] = rastgelesec(3)
5       ENDFOR
6   BİTİR
```

Adım 2: Alice, rotasyon kapısında kullanmak için rastgele 2n tane farklı açı belirler.

```
1   BAŞLA
2       n değerini al
3       FOR i=0 TO 2*n-1 STEP +1
4           angle[i] = rastgelesec(360)
5       ENDFOR
6   BİTİR
```

Alice, 2n bitlik klasik veri setini kullanarak 2n kubitlik kuantum durumu oluşturur. Daha sonra her bir kubit için farklı açı olmak üzere rotasyon kapısını uygular. Son olarak *ab_state* kuantum durumunu Bob'a gönderir.

```
1   BAŞLA
2       n değerini al
3       ab_state kuantum durumunu her bir kubit 0 değeri olacak şekilde oluştur
4       FOR i=0 TO 2*n-1 STEP +1
5           IF d_set[i]==1 THEN
6               ab_state[i] kuantum durumuna X kapısını uygula
7           ENDIF
8           ab_state[i] kuantum durumunu angle[i] açısıyla y ekseninde döndür
9       ENDFOR
10  BİTİR
```

Adım 3: Bob, kendine ait kapıları oluşturmak için 0, 1 ve 2 rakamları arasından n tane farklı seçim yapar. Burada 0 Identity (I), 1 NOT (X) ve 2 CNOT kapılarını temsil etmektedir.

```
1   BAŞLA
2       n değerini al
3       FOR i=0 TO n-1 STEP +1
4           bob_key[i] = ratgelesec(3)
5       ENDFOR
6   BİTİR
```

Bob, kendi aday anahtarlaını *ab_state* kuantum durumuna uygular. Eğer *bob_key[i],* 0 değerine sahip ise herhangi bir kapı uygulanmaz. Çünkü 0, Identity (I) kapısını temsil etmektedir. Eğer *bob_key[i],* 1 değerine sahip ise NOT (X) kapısı ve 2 değerine sahip ise CNOT kapısı uygulanır. 0,2,4… indisli kubitler kontrol kubitidir. 1,3,5… indisli kubitler hedef kubittir ve kapılar bu kubitlere uygulanır.

```
1   BAŞLA
2       n değerini al
3       FOR i=0 TO n-1 STEP +1
4           IF bob_key[i]==1 THEN
5               ab_state[2*i+1] kuantum durumuna X kapısını uygula
6           ENDIF
7           IF bob_key[i]==2 THEN
8               ab_state[2*i] (Kontrol kubit) ve ab_state[2*i+1] (Hedef Kubit)
9               kuantum durumuna CNOT kapısını uygula
10          ENDIF
11
12      ENDFOR
13  BİTİR
```

Adım 4: Alice, kuantum duruma kendi kapılarını uygular. Eğer *alice_key[i],* 0 değerine sahip ise herhangi bir kapı uygulanmaz. Çünkü 0, Identity (I) kapısını temsil etmektedir. Eğer *alice_key[i],* 1 değerine sahip ise NOT (X) kapısı ve 2 değerine sahip ise CNOT kapısı uygulanır.

```
BAŞLA
    n değerini al
    FOR i=0 TO n-1 STEP +1
        IF alice_key[i]==1 THEN
            ab_state[2*i+1] kuantum durumuna X kapısını uygula
        ENDIF
        IF alice_key[i]==2 THEN
            ab_state[2*i] (Kontrol kubit) ve ab_state[2*i+1] (Hedef Kubit)
            kuantum durumuna CNOT kapısını uygula
        ENDIF
    ENDFOR
BİTİR
```

Adım 5: Alice, Adım 2'de kullandığı açıların negatifini kullanarak kuantum duruma rotasyon kapısı uygular.

```
BAŞLA
    n değerini al
    FOR i=0 TO 2*n-1 STEP +1
        ab_state[i] kuantum durumunu -1*angle[i] açısıyla y ekseninde döndür
    ENDFOR
BİTİR
```

Adım 6: Alice kuantum durumunu ölçtükten sonra ölçüm sonucunu kuantum durumunu oluşturmak için kullandığı veri setindeki ilgili bitler ile karşılaştırır. Ölçüm sonucuna göre ödül listesi belirlenir.

```
BAŞLA
    n değerini al
    2n kubitlik ab_state kuantum durumun hedef kubitlerinde ölçüm yap
    Ölçüm sonuçlarını n bitlik ab_statebit dizisine ata
    FOR i=0 TO n-1 STEP +1
        IF ab_statebit[i]==d_set[2*i+1] THEN
            kontrol_list[i]=1
        ELSE
            kontrol_list[i]=0
        ENDIF
    ENDFOR
    kontrol_list dizisini duyur
BİTİR
```

Alice, Eve'nin tespiti için ödül değeri 0 olan kapıların %50 sini duyurur. Eve, aynı kapı seçildiği halde ödül değeri 0 olan durumla karşılaşırsa Eve'nin varlığını ilan eder ve iletişim iptal edilir. Eğer Eve yoksa duyurulan bu kapılar için Alice ve Bob baştan yeni

tercihler yapar. Tüm kapılar başarılı bir şekilde öğretilene kadar bu işlemler tekrar eder. Yapılan tekrarlarda Alice duyurulmayan kapılar için yeni bir seçim yapmaz. Bob ise her tekrarda kontrol listesinde 0 olarak belirtilen ve duyurulmayan kapılar için bir önceki seçiminden farklı bir kapı seçer.

BEŞİNCİ BÖLÜM
SONUÇ VE ÖNERİLER

5.1. Güvenlik Analizi

Bu bölümde iletişimi başlatan gönderen taraf Alice, alıcı taraf Bob ve iletişimi yetkisiz olarak dinleyerek gizli bilgileri elde etmeye çalışan taraf ise Eve olarak adlandırılmıştır. Önerilen KTÖ ve güvenli iletişim yönteminin güvenliği genel olarak aşağıdaki şekildedir.

Simetrik kriptografide, güvenli bir iletişim için gizli anahtarın üçüncü bir katılımcı tarafından bilinmemesi gerekmektedir. Önerilen çalışmada anahtar paylaşılmamaktadır. Anahtarın yerel olarak üretilmesini sağlayacak kuantum kapılar, geliştirilen KTÖ yöntemi ile öğretilmektedir. Bu kuantum kapılar, açık bir kanal vasıtasıyla duyurulan ya da gönderilen klasik bitlere uygulanarak anahtar oluşturulur. Eve, kuantum kapılar paylaşılmadığı için hangi bite hangi kuantum kapının uygulanacağı bilgisine sahip değildir. Bu nedenle paylaşılan klasik veriyi kullanarak anahtarı elde etmesi mümkün değildir. Eve'nin temel gayesi bu kuantum kapıları öğrenmektir. Bu nedenle odaklanılması gereken nokta öğrenme eylemini gerçekleştiren KTÖ yönteminin güvenliğidir.

Öğrenme eyleminde farklı genliğe sahip süperpozisyon durumu kullanılır (bkz. Denklem 3.4). Alice, her bir kubit için farklı açı belirledikten sonra, öğrenme eylemi için kullanacağı kuantum duruma y ekseninde rotasyon kapısı uygular. Böylece kuantum durum farklı genliklere sahip süperpozsiyon durumuna gelir. Eve, kullanılan açıların bilgisine sahip olmadığı için süperpozisyon halindeki kuantum durumdan faydalı bir veri elde edemez. Kuantum durumu ölçmesi halinde rastgele bir veri elde etmiş olur. Mesela kuantum durum Hadamard kapısı kullanılarak süperpozisyon haline getirilseydi Eve, Hadamard kapısı uygulayarak orijinal kuantum durumu elde etmiş olurdu. Fakat önerilen yöntem için Alice'in dışında bir katılımcının orijinal kuantum durumu elde etmesi mümkün değildir. Çünkü kullanılan açıların bilgisine sadece Alice sahiptir.

Eve'nin kuantum durumu dolanık hale getirdiği kabul edilsin. Dolanıklık sayesinde Eve, Alice'in ölçüm sonuçlarına ve öğrenme çıktılarına sahip olabilir. Ancak bu bilgileri

kullanarak hangi kapıların uygulandığını tespit edemez. Eve'nin elde etmiş olduğu bu veri, öğrenme çıktısı 1 ise Alice'in kuantum durumu oluşturmak için kullandığı klasik veri olur. Eğer öğrenme çıktısı 0 ise, elde ettiği veri Alice'in kuantum durumu oluşturmak için kullandığı klasik verinin değili olur. Kuantum kapıların uygulandıktan sonraki kuantum duruma ait bir ölçüm sonucuna sahip olmadığı için Eve, kuantum kapılar hakkında bilgi elde edemez. Sadece Bob'un başarılı bir şekilde öğrenip öğrenmediğini tespit edebilir.

Eve, Alice'e Bob, Bob'a Alice gibi davranmak isteyebilir. Bunu önlemek için Alice, ödül değerinde 0 olarak işaretlenen kubitlere ait kuantum kapıların %50'sini duyurur. Alice'in duyurduğu bu kuantum kapıların Bob'un seçtiği kuantum kapılardan farklı olması beklenir. Bob kendi kapılarını Alice'in duyurduğu kapılarla karşılaştırır. Bob, aynı indislere sahip kubitler için aynı kuantum kapıların kullanıldığını tespit ederse Eve'nin varlığını ilan eder. Eve tespit edildiği için öğrenme eylemi sonlandırılır. Alice ve Bob'un X kapısına sahip olduğu kabul edilerek aşağıdaki gibi örneklendirilmiştir:

Adım 1: Alice 0 bitine sahiptir. $|0\rangle$, kuantum durumunu hazırlar.

Adım 2: Alice, $\frac{\pi}{3}$ açısına sahip rotasyon kapısını $|0\rangle$ kuantum durumuna uygular ve $\frac{\sqrt{3}}{2}|0\rangle + \frac{1}{2}|1\rangle$ elde eder. Bob'a $\frac{\sqrt{3}}{2}|0\rangle + \frac{1}{2}|1\rangle$ kuantum durumunu gönderir.

Adım 3: Bob, X kapısını $\frac{\sqrt{3}}{2}|0\rangle + \frac{1}{2}|1\rangle$'ya uygular ve $\frac{1}{2}|0\rangle + \frac{\sqrt{3}}{2}|1\rangle$ elde eder. Bob, $\frac{1}{2}|0\rangle + \frac{\sqrt{3}}{2}|1\rangle$ kuantum durumunu Alice'e gönderir

Adım 4: Alice, X kapısını $\frac{1}{2}|0\rangle + \frac{\sqrt{3}}{2}|1\rangle$ 'ya uygular ve $\frac{\sqrt{3}}{2}|0\rangle + \frac{1}{2}|1\rangle$ elde eder.

Adım 5: Alice, $-\frac{\pi}{3}$ açısına sahip rotasyon kapısını $\frac{\sqrt{3}}{2}|0\rangle + \frac{1}{2}|1\rangle$ kuantum durumuna uygular ve $|0\rangle$ elde eder.

Görüldüğü üzere eğer her iki taraf da aynı kuantum kapıya sahipse Alice öğrenme eylemi sonunda başlangıç değerini elde eder. Bu durumda Alice'in ödül değerini 1 olarak

işaretlemesi gerekir. Ödül değerinin 0 olarak işaretlenmesinin tek nedeni kuantum durumunun Eve tarafından değiştirilmiş olmasıdır.

Hata denetimlerinin güvenliği incelenecek olursa, her iki hata denetiminde de veri seti paylaşılır. Hangi veriye hangi kapının uygulanacağı bilinmediğinden dolayı bu veri setinden yararlı bir bilgi çıkarmak mümkün değildir. Veri setlerinden anahtar oluşturulduktan sonra, mesaj bu anahtarla şifrelenerek karşı tarafa gönderilir. Mesajın içeriğinin paylaşılmaması nedeniyle, bu şifreli bilgiden kullanılan anahtarı elde etmek mümkün değildir. Ayrıca anahtar sadece bir kere kullanılır. Aynı anahtar, ikinci bir mesaja uygulanarak gönderilmez. Aynı anahtar tekrar kullanılmadığı için Eve, örneklem uzayı oluşturup anahtarı tahmin etme yoluna gidemez. Anahtarın tahmin edilememesi kuantum kapıların güvende olmasını sağlar.

Anahtarı oluşturan kuantum kapıların öğretilmesi zorlu bir süreç olsada bir kereye mahsus gerçekleştirilir. Alice ve Bob, aynı kuantum kapılara sahip olduktan sonra anahtarları yerel olarak üretecekleri için güvenlik ihlali olmaz. Anahtarın paylaşılmadığı için iletişim güvenlidir. Böylece her iletişim için farklı bir anahtar kullanılabilir. Eve'nin, 512 bitlik bir anahtarla şifrelenmiş mesajı elde etmek için 2^{512} olası anahtarı denemesi gerekir.

5.2. Kuantum Takviyeli Öğrenme ile Anahtar Üretimi Simülasyon Sonuçları

Önerilen çalışma Python programlama dilinin IBM Qiskit kütüphanesi kullanılarak simüle edilmiştir. Simülasyon için kullanılan bilgisayar i7-11800H işlemci ve 16 GB RAM donanım özelliklerine sahiptir. Bu donanım ile simülasyon, üst sınır olarak 195 adet kuantum kapı için öğrenme eylemini gerçekleştirebilmektedir. Simülasyon sonuçları Tablo 6'da gösterilmektedir. Simülasyon sonuçlarını incelerken bu çalışmanın n adet bağımsız öğrenme eylemi gerçekleştirdiğini unutmamak gerekir. Günümüzde bir oyundaki veya robotik uygulamalardaki en iyi hamlenin belirlenmesinde takviyeli öğrenme yaygın olarak tercih edilmektedir. Takviyeli öğrenme, bir noktadan diğerine en uygun yolu bulmaya çalışır. Bir sonraki seçim önceki seçime bağlıdır. Ancak bizim çalışmamızda seçimler bağımsızdır.

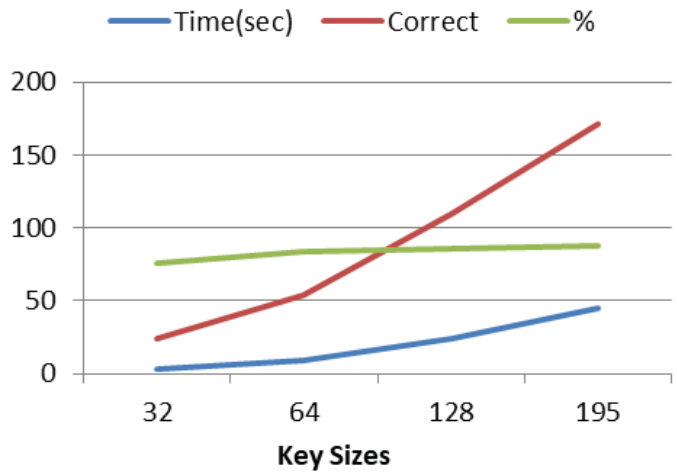
Tablo 6

Simülasyon sonuçları. Simülasyon her anahtar boyutu için 10 kez çalıştırılarak ortalaması alınmıştır (Çağlar ve Yılmaz, 2023).

Key Sizes (bits)**	Correct (bits)	Incorect (bits)	Time (Sec)	%
195	171.5	23.5	44.9	87.95
128	109.4	18.6	24.5	85.47
64	53.5	10.5	9.3	83.59
32	24.4	7.6	3	76.25

** Bir adet kapı ile bir adet anahtar biti oluşturulduğundan dolayı Anahtarın boyutu ile Öğrenilen kapı sayısı aynıdır.

Önerilen çalışma, öğrenme eylemini 195 kapı için %87,95, 128 kapı için %85,47, 64 kapı için %83,59, 32 kapı için %76,25 doğrulukla gerçekleştirmektedir. Her bir kapı ile bir adet anahtar biti oluşturulmaktadır. Anahtar boyutu yani öğrenilen kapı sayısı arttıkça yöntemin performansının da arttığı görülmektedir. Anahtar boyutu arttığı zaman, simülasyonun çalışma süresinin arttığı gözlenmiştir. Şekil 10'dan görülebileceği gibi yöntemin performansının ve çalışma süresinin anahtar boyutuyla doğru orantılı olarak arttığı görülmektedir.



Şekil 10 Simülasyon sonuçlarının grafik gösterimi. Simülasyon her anahtar boyutu için 10 kez çalıştırılarak ortalaması alınmıştır (Çağlar ve Yılmaz, 2023).

5.3. Sonuçlar

Bu tez çalışması, takviyeli öğrenme ve anahtar oluşturma için kuantum mekaniğinin ilkelerini kullanır. Mesajın şifrelenmesi ve şifresinin çözülmesi için klasik XOR işlemi kullanılır. I, X, CNOT kapıları klasik bilgisayarlara kolaylıkla uygulanabildiği için hata kontrolleri de tamamen klasik olarak yapılabilmektedir. Kuantum Takviyeli öğrenmenın uygulanabilmesi için bir kuantum kanalı gerektirir. Kuantum ağları üzerine birçok çalışma mevcuttur. Kuantum ağı yaygın olarak kullanıldığında geliştirilen yöntem rahatlıkla uygulanabilir. Günümüz imkanlarında ise yöntemin uygulanabilmesi için kuantum ağ simülasyonları kullanılabilir.

Bu tez çalışmasında, geliştirilen yöntemin literatürdeki diğer yöntemlerden en önemli farkları aşağıdaki şekilde özetlenebilir. 1- Bu yöntemde gizli anahtarı oluşturmak için kullanılacak kapılar kuantum takviyeli öğrenme ile öğretilmektedir. 2- Oluşturulan gizli anahtar hiçbir şekilde katılımcılar arasında paylaşılmamaktadır. 3- Bu çalışmada KAD kullanımına ihtiyaç duyulmadığından maliyet bakımından diğerlerine göre daha az maliyetlidir.

Bu tez çalışmasında geliştirilen yöntem, sadece öğrenme eylemini gerçekleştirirken kuantum kanal gerektirmektedir. Yani gizli anahtarı, yerel olarak oluşturmakta ve anahtar paylaşımına gerek duymamaktadır. Yöntem, sanayi veya güvenli iletişimin ihtiyaç duyulduğu her alanda iki bilgisayarın ya da cihazın birbirleri ile şifreli bir şekilde iletişim kurulmasının istendiği tüm durumlarda yaygınca kullanılabilir.

Bu tez çalışmasında önerilen yöntemin geliştirilmesi adına gelecekte aşağıdaki çalışmalar gerçekleştirilebilir:

- Kullanılan kuantum kanalın veri kaybı ihmal edilmiştir. Bu nedenle kuantum ağ üzerine oluşabilecek veri kaybını en aza indirecek ya da gerekli hata düzeltmeleri yapılarak doğru verinin elde edilmesini sağlayacak çalışmalar,
- Simülasyon için farklı dillerin ve kütüphanelerin kullanılıp birbiriyle kıyaslandığı çalışmalar,
- Donanımsal olarak gerçekleştirilebilen kuantum ağlar üzerinde uygulanarak sonuçların tartışıldığı çalışmalar yapılabilir.

KAYNAKÇA

Aczel, A.D. (2018). *Dolanıklık: Fiziğin En Büyük Gizemi*. Kutay Kence (çev.). Kırmızı Kedi Yayınevi: İstanbul.

Afacan, E. (2016). *Kriptografiye Giriş Şifreleme Teorisi,* Epos Yayınları: Ankara.

Arvandi, M., Wu, S., Sadeghian, A., Melek, W.W. ve Woungang, I. (2006). "Symmetric Cipher Design Using Recurrent Neural Networks". *The 2006 IEEE International Joint Conference on Neural Network Proceedings,* 16-21 Temmuz 2006, Vancouver, BC, Canada. 2039 – 2046. https://doi.org/10.1109/IJCNN.2006.246972.

Bencheikh, K., Symul, Th., Jankovic, A. ve Levenson J. A. (2001). "Quantum Key Distribution with Continuous Variables". *Journal of Modern Optics*, 48 (13), 1903-1920, https://doi.org/10.1080/09500340108240896

Bennett, C.H. (1992). "Quantum Cryptography Using Any Two Nonorthogonal States". *Physical Review Letters*, 68, 3121 – 3124. https://doi.org/10.1103/PhysRevLett.68.3121.

Bennett, C.H. ve Brassard, G. (1984). "Quantum Cryptography: Public Key Distribution and Coin Tossing". *International Conference on Computers, systems & Signal Processing*, 9-12 Aralık 1984, Bangalore, India. 175 – 179.

Bennett, C.H., Brassard, G. ve Mermin, N.D. (1992). "Quantum cryptography without Bell's theorem". *Physical Review Letters*, 68, 557-559. https://doi.org/10.1103/PhysRevLett.68.557.

Çağlar, E. ve Yılmaz, İ. (2023). "Secure Communication Based On Key Generation With Quantum Reinforcement Learning". *International Journal of Information Security Science*, 12 (2), 22-41. https://doi.org/10.55859/ijiss.1264169.

Çağlar, E., Yılmaz, İ. ve Şahin, E. (2022). Kuantum Anahtar Dağıtım Protokollerinin Simüle Edilerek Karşılaştırılması: BB84 ve B92, *15. Uluslararası Bilgisayar ve Öğretim Teknolojileri Sempozyumu*, 7-9 Eylül 2022, Çanakkale Onsekiz Mart Üniversitesi, Çanakkale. 268-278

Dong, D., Chen, C., Chen, Z. ve Zhang, C. (2006). "Control of Five-qubit System Based on Quantum Reinforcement Learning". *2006 International Conference on Computational Intelligence and Security*, 3-6 Kasım 2006, Guangzhou, China. 164-167. https://doi.org/10.1109/ICCIAS.2006.294113.

Dong, D., Chen, C., Li, H. ve Tarn, T.J. (2008). "Quantum Reinforcement Learning". *IEEE Transactions On Systems, Man, And Cybernetics, Part B (Cybernetics),* 38(5), 1207-1220. http://dx.doi.org/10.1109/TSMCB.2008.925743.

Dong, D., Chen, C., Chu, J. ve Tarn, T.J. (2012). "Robust Quantum-Inspired Reinforcement Learning for Robot Navigation" . *IEEE/ASME Transactions on Mechatronics*, 17(1), 86-97, https://doi.org/10.1109/TMECH.2010.2090896.

Ekert, A. K. (1991). "Quantum Cryptography based on Bell's theorem". *Physical Review Letters*, 67, 661 – 663. https://doi.org/10.1103/PhysRevLett.67.661.

Feynman, R.P. (1982). "Simulating Physics with Computers". *International Journal of Theoretical Physics.* 21, 467 – 488. https://doi.org/10.1007/BF02650179.

Gao, F., Guo, F., Wen, Q., ve Zhu, F. (2006). "Quantum key distribution without alternative measurements and rotations". *Physics Letters A*, 349 (1), 53-58, https://doi.org/10.1016/j.physleta.2005.09.012

Gisin, N., Ribordy, G., Tittel, W. ve Zbinden, H. (2002). "Quantum Cryptography". *Reviews of Modern Physics,* 74, 145–195. https://doi.org/10.1103/RevModPhys.74.145.

Godhavari, T., Alamelu N.R. ve Soundararajan, R. (2005). "Cryptography Using Neural Network". *2005 Annual IEEE India Conference - Indicon*, 11-13 Aralık 2005, Chennai, India. 258 – 261. https://doi.org/10.1109/INDCON.2005.1590168.

Gruska, J. (1999). *Quantum Computing*, McGraw-Hill Publishing Company: Maidenhead, Berkshire, England.

Hajji, H. ve Baz, M. (2021). "Qutrit-based semi-quantum key distribution protocol". *Quantum Information Processing,* 20, 4, https://doi.org/10.1007/s11128-020-02927-8

Heidari, S., Gheibi, R., Houshmand, M. ve Nagata, K.(2017). "A Robust Blind Quantum Copyright Protection Method For Colored Images Based On Owner's Signature". *International Journal of Theoretical Physics,* 56 (8), 2562–2578, https://doi.org/10.1007/s10773-017-3412-9

Hu, Y., Tang, F., Chen, J. ve Wang, W. (2021). "Quantum-enhanced reinforcement learning for control: a preliminary study". *Control Theory and Technology,* 19, 455–464 https://doi.org/10.1007/s11768-021-00063-x

Imre, S. ve Balazs, F. (2005). *Quantum Computing and Communications An Engineering Approach*, John Wiley&Sons Ltd.: Southern Gate, Chichester, West Sussex, England.

İpekoğlu, Y., Turgut, S., Yakaboylu, E. ve Uyanık, K. (2009). IARS Kuantum Bilgi Kuramının Temel Kavramları, ODTÜ Fizik Bölümü, Ders Notu

Kadir, A., Azzaz, M.S. ve Kaibou, R. (2023). "Chaos-based Key Generator using Artificial Neural Networks Models". *2023 International Conference on Advances in Electronics, Control and Communication Systems (ICAECCS)*, 6-7 Mart 2023, BLIDA, Algeria. 1 – 5. https://doi.org/10.1109/ICAECCS56710.2023.10105105.

Kanter, I., Kinzel, W. ve Kanter, E. (2002). "Secure exchange of information by synchronization of neural networks". *Europhysics Letters*, 57 (1), 141-147, https://dx.doi.org/10.1209/epl/i2002-00552-9

Kaye, P., Laflamme, R. ve Mosca, M. (2007). *An Introduction to Quantum Computing*, Oxford University Press: New York.

Kumar, M., Dohare, U., Kumar, S. ve Kumar, N. (2023). "Blockchain Based Optimized Energy Trading for E-Mobility Using Quantum Reinforcement Learning," *IEEE Transactions on Vehicular Technology,* 72 (4), 5167-5180, https://doi.org/10.1109/TVT.2022.3225524.

Kwak, Y., Yun, W.J., Jung, S., Kim, J.K. ve Kim, J. (2021) "Introduction to Quantum Reinforcement Learning: Theory and PennyLane-based Implementation". *2021 International Conference on Information and Communication Technology Convergence (ICTC)*, 20-22 Ekim 2021, Jeju Island, Korea , Republic of. 416-420. https://doi.org/10.1109/ICTC52510.2021.9620885.

Li, C.M., Yu, K.F., Kao, S.H. ve Hwang, T. (2016) "Authenticated semi-quantum key distributions without classical channel". *Quantum Inf Process,* 15, 2881–2893, https://doi.org/10.1007/s11128-016-1307-y

Neumann, N.M.P., de Heer, P.B.U.L. ve Phillipson, F. (2023). "Quantum reinforcement learning". *Quantum Inf Process,* 22, 125, https://doi.org/10.1007/s11128-023-03867-9

Nielsen, M.A. ve Chuang I.L. (2010). *Quantum Computation and Quantum Information*, Cambridge University Press: New York.

Niraula, D., Jamaluddin, J., Matuszak, M.M., Haken, R.K.T. ve Naqa, I. (2021). "Quantum deep reinforcement learning for clinical decision support in oncology: application to adaptive radiotherapy". *Scientific Reports,* 11, 23545, https://doi.org/10.1038/s41598-021-02910-y

Niwa, S., Shiota, S. ve Kiya, H. (2023). "A Privacy-Preserving Method Using Secret Key for Convolutional Neural Network-Based Speech Classification". *2023 31st European Signal Processing Conference (EUSIPCO)*, 4-8 Eylül 2023, Helsinki, Finland, 76-80, https://doi.org/10.23919/EUSIPCO58844.2023.10289898.

Park, S. ve Kim, J. (2023). "Quantum Reinforcement Learning for Large-Scale Multi-Agent Decision-Making in Autonomous Aerial Networks". *2023 VTS Asia Pacific Wireless Communications Symposium (APWCS),* 23-25 Ağustos 2023, Tainan city, Taiwan, 1-4, https://doi.org/10.1109/APWCS60142.2023.10233966.

Perumangatt, C., Rahim, A. A., Salla, G.R., Prabhakar, S., Samanta, G.K., Paul, G. ve Singh, R. P. (2015). "Three-particle hyper-entanglement: teleportation and quantum key distribution". *Quantum Inf Process* 14, 3813–3826, https://doi.org/10.1007/s11128-015-1056-3

Rivest, R., Shamir, A. ve Adleman, L. (1978). "A Method for Obtaining Digital Signatures and Public Key Cryptosystems". *Commucations of the ACM*, 21 (2), 120-126. https://doi.org/10.1145/359340.359342.

Shor, P.W. (1994). "Algorithms for Quantum computation: Discrete Logarithms and factoring", *35th Symposium on Foundations of Computer Science*, 20-22 Kasım 1994, Santa Fe, NM, USA. 124 – 134.

Şahin E. ve Yılmaz İ. (2018a). "A novel quantum steganography algorithm based on LSBq formulti-wavelength quantum images". *Quantum Information Processing,* 17, 319 https://doi.org/10.1007/s11128-018-2092-6

Şahin E. ve Yılmaz İ. (2018b) "Security of NEQR Quantum Image by Using Quantum Fourier Transform with Blind Trent". *International Journal of Information Security Science*, 7 (1), 20-25

Şahin, E. (2019). Kuantum Temelli Görüntü İşleme. Doktora Tezi. Çanakkale Onsekiz Mart Üniversitesi, Lisansüstü Eğitim Enstitüsü, Çanakkale.

Uğuz, S. (2019). *Makine Öğrenmesi Teorik Yönleri ve Python Uygulamaları ile Bir Yapay Zeka Ekolü*, Nobel Akademik Yayıncılık Eğitim Danışmanlık: Ankara.

Ural, M.N. (2021). *Kuantum Hesaplayıcılar ve Kuantum Hesaplamaya Giriş*, Kodlab Yayın Dağıtım: İstanbul.

Wang, C., Huang, D., Huang, P., Lin, D., Peng, J. ve Zeng, G. (2015). "25 mhz clock continuous-variable quantum key distribution system over 50 km fiber channel". *Scientific Reports* 5, 14607, https://doi.org/10.1038/srep14607

Yu, K.F., Yang, C.W., Liao, C.H. ve Hwang T. (2014) "Authenticated semi-quantum key distribution protocol using Bell states". *Quantum Inf Process* 13, 1457–1465, https://doi.org/10.1007/s11128-014-0740-z

Zhu, W., Yan, T., Sun, W., Wu, Y., Dong, J. ve He, Y. (2023). "Hyperchaotic Image Encryption Algorithm Based on Deep Neural Network Key Generation and Dynamic DNA Coding". *2023 4th International Conference on Information Science, Parallel and Distributed Systems (ISPDS)*, 14-16 Temmuz 2023, Guangzhou, China. 95 - 101. https://doi.org/10.1109/ISPDS58840.2023.10235534.

EKLER