T.C.

ÇANAKKALE ONSEKİZ MART ÜNİVERSİTESİ

LİSANSÜSTÜ EĞİTİM ENSTİTÜSÜ

BİLGİSAYAR MÜHENDİSLİĞİ ANABİLİM DALI

KUANTUM AĞ SİMÜLASYONLARININ DAĞITIK YÜRÜTÜLMESİ

YÜKSEK LİSANS TEZİ

OSMAN SEMİ CEYLAN

Tez Danışmanı

PROF. DR. İHSAN YILMAZ

ÇANAKKALE – 2024

T.C.
ÇANAKKALE ONSEKİZ MART ÜNİVERSİTESİ
LİSANSÜSTÜ EĞİTİM ENSTİTÜSÜ

BİLGİSAYAR MÜHENDİSLİĞİ ANABİLİM DALI

KUANTUM AĞ SİMÜLASYONLARININ DAĞITIK YÜRÜTÜLMESİ

YÜKSEK LİSANS TEZİ

OSMAN SEMİ CEYLAN

Tez Danışmanı
PROF. DR. İHSAN YILMAZ

Bu çalışma, TÜBİTAK kurumu tarafından desteklenmiştir.
Proje No: 120E087

ÇANAKKALE – 2024

T.C.
ÇANAKKALE ONSEKİZ MART ÜNİVERSİTESİ
LİSANSÜSTÜ EĞİTİM ENSTİTÜSÜ

Osman Semi CEYLAN tarafından Prof. Dr. İhsan YILMAZ yönetiminde hazırlanan ve **22/01/2024** tarihinde aşağıdaki jüri karşısında sunulan "**Kuantum Ağ Simülasyonlarının Dağıtık Yürütülmesi**" başlıklı çalışma, Çanakkale Onsekiz Mart Üniversitesi Lisansüstü Eğitim Enstitüsü **Bilgisayar Mühendisliği Anabilim Dalı**'nda **YÜKSEK LİSANS TEZİ** olarak oy birliği ile kabul edilmiştir.

Jüri Üyeleri	**İmza**
Prof. Dr. İhsan YILMAZ (Danışman)	……
Doç. Dr. Levent ÇETİNKAYA	……
Dr. Öğr. Üyesi Bora ASLAN	…….

Tez No : ……..
Tez Savunma Tarihi : 22/01/2024

……
İSİM SOYİSMİ
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.

Osman Semi CEYLAN
22/01/2024

TEŞEKKÜR

Bu tezin gerçekleştirilmesinde, çalışmam boyunca benden bir an olsun yardımlarını esirgemeyen saygı değer danışman hocam Prof. Dr. İhsan YILMAZ, çalışma süresince tüm zorlukları benimle göğüsleyen ve hayatımın her evresinde bana destek olan değerli aileme ve sonsuz teşekkürlerimi sunarım.

Osman Semi CEYLAN

Çanakkale, Ocak 2024

ÖZET

KUANTUM AĞ SİMÜLASYONLARININ DAĞITIK YÜRÜTÜLMESİ

Osman Semi CEYLAN
Çanakkale Onsekiz Mart Üniversitesi
Lisansüstü Eğitim Enstitüsü
Bilgisayar Mühendisliği Anabilim Dalı Yüksek Lisans Tezi
Danışman: Prof. Dr. İhsan YILMAZ

22/01/2024, 51

Kuantum ağ, kuantum bilgilerin düğümler arasında aktarımını kolaylaştırmak için kuantum mekaniği ilkelerini kullanan bir iletişim altyapısıdır. Deneysel kuantum ağları bu prensipleri kullanan fiziksel sistemlerin ve cihazların uygulanmasını içerir. Ancak verimli bir şekilde ölçeklendirilebilen kuantum ağlarının inşası maliyetli olduğundan simülasyonlara ihtiyaç duyulmaktadır. Simülasyonlar, yalnızca kaynak yoğun deneysel konfigürasyonlara bağlı kalmadan, kuantum ağlarının dinamiklerini incelemek, farklı koşullar altında verimliliklerini tahmin etmek ve uygulanabilir kuantum iletişim teknolojilerinin ilerlemesini yönlendirmek için kontrollü bir ortam sunar. Fakat kuantum simülasyonlarda iç içe geçmiş kuantum durumlarının dijital şekilde ifade edilmesi gerektiğinden dolayı özellikle veri uzayının bağımlılığı gibi klasik hesaplama yöntemleri için zorluklar oluşturmaktadır. Bu tez çalışmasında bu probleme çözüm olarak orta ve büyük ölçekli kuantum ağların simülasyonunda, gereken işlem yükünün klasik ağa bağlı bilgisayarların arasında paylaştırarak daha etkin biçimde dağıtık simülasyonunun mümkün olabileceği gösterilmektedir. Yapılması planlanan deneysel kuantum ağların gerçekleştirilmeden önce simülasyonlarının dağıtık olarak yapılması zamandan ve maliyetten tasarruf edilebileceğini göstermektedir.

Anahtar Kelimeler: Kuantum Ağlar, Kuantum Simülasyon, Dağıtık Simülasyon Modeli

ABSTRACT

DISTRIBUTED EXECUTION OF QUANTUM NETWORK SIMULATIONS

Osman Semi CEYLAN
Çanakkale Onsekiz Mart University
School of Graduate Studies
Master of Science Thesis in Computer Engineering
Advisor: Prof. Dr. İhsan YILMAZ
22/01/2024, 51

A quantum network is a communications infrastructure that uses the principles of quantum mechanics to facilitate the transfer of quantum information between nodes. Experimental quantum networks involve the implementation of physical systems and devices that use these principles. However, since the construction of efficiently scalable quantum networks is costly, simulations are needed. Simulations provide a controlled environment to study the dynamics of quantum networks, predict their efficiency under different conditions, and guide the advancement of applicable quantum communication technologies, without relying solely on resource-intensive experimental configurations. However, in quantum simulations, since the intertwined quantum states must be expressed digitally, they pose difficulties for classical calculation methods, especially the dependency of the data space. In this thesis study, it is shown that, as a solution to this problem, more effective distributed simulation is possible in the simulation of medium and large-scale quantum networks by sharing the required processing load among computers connected to the classical network. Distributed simulations of the planned experimental quantum networks before their implementation show that time and cost can be saved.

Keywords: Quantum Networks, Quantum Simulation, Distributed Execution Model

İÇİNDEKİLER

Sayfa No

SİMGELER VE KISALTMALAR

$\mathfrak{H}$	Hilbert Uzayı
$\widehat{H}$	Hamilton Operatörü
$\|\psi\rangle$	Kuantum Durum
σ	Pauli Operatörü
CNOT	Kontrollü Değil Operatörü
SWAP	Değiş Tokuş Operatörü
CCNOT	Kontrollü Kontrollü Değil Operatörü
$\oplus$	İkili Toplama İşlevi
$\otimes$	Tensör Çarpım İşlevi
$\widehat{M}$	Ölçüm Operatörü
$\hat{X}$	Konum Operatörü
PVM	Pozitif Değerli Ölçüm
QKD	Kuantum Anahtar Dağıtımı
BB84	Bennett – Brassard 1984 Protokolü
E91	Ekert 1991 Protokolü
BBM92	Bennett – Brassard – Mermin 1992 Protokolü
MSZ96	Mu – Seberry – Zheng 1996 Protokolü
DARPA	Savunma İleri Araştırma Projeleri Ajansı
SECOQC	Kuantum Kriptografi ile Güvenli İletişim
UDP	Kullanıcı Veri-bloğu İletişim Kuralları

TABLOLAR DİZİNİ

ŞEKİLLER DİZİNİ

BİRİNCİ BÖLÜM
GİRİŞ

Geçtiğimiz elli yıl boyunca, yarı iletken teknolojilerinin ilerlemesi dikkate değer bir ivme ile gerçekleşmiştir. Bunun bir sonucu olarak, yarı iletken teknolojiler, çeşitli bilimsel disiplinlere sağladıkları araçlar sayesinde şimdiye kadar çoğu zorlukların üstesinden gelmiştir. Parçacık fiziği, gelişen bu araçların kullanımı sayesinde parçacıkların anlaşılmasında önemli ölçüde ilerleme kaydetmiştir. Kuantum teknolojileri araştırma alanı bu konularda çalışmaların incelenmesi üzere ortaya çıktı. Kuantum teknolojiler, modern endüstriyel sistemlerde karşılaşılan zorluklara yönelik daha üstün ve gelişmiş çözümler geliştirmek için kuantum mekaniğinin ilkelerinden yararlanır. Bu üstünlükler çeşitli teorik ve deneysel çalışmalarda gözlenmekle birlikte, yaygın olarak "kuantum üstünlüğü" olarak anılmaktadır. Bu kuantum üstünlükleri aşağıdaki şekilde özetleyebiliriz.

- Süperpozisyon (Superposition)
- Dolaşıklık (Entanglement)
- Kuantum Işınlama (Teleportation)
- Kopyalanamama Teorisi (No-clonning Theorem)
- Terslenebilirlik (Reversibility)
- Dolaşıklık Aktarımı (Entanglement Swapping)

Kuantum teknolojiler kuantum mekaniği ilkeleri doğrultusunda etkileşen atomlar, kuarklar, fotonlar, elektronlar gibi durumlar ile ilgilenmektedir. Fakat bunların birbirinden ayıran çeşitli özniteliklerinden dolayı araştırmacılar kuantum üstünlükleri farklı çalışma alanlarında incelenmektedir. Günümüz kuantum teknolojisindeki çalışma alanlarına kuantum bilişim, kuantum hesaplama, kuantum algılama ve metroloji, kuantum ağlar, kuantum makine öğrenmesi, kuantum görüntü işleme, kuantum cihazlar gibi örnekler verilebilir.

Bu tezin kapsamında olan kuantum ağlar, bilginin güvenli ve verimli bir şekilde iletilmesini sağlamak için kuantum mekaniğinin ilkelerinden yararlanan bir tür iletişim altyapısıdır. Kuantum ağ, topolojik açıdan geleneksel bilgisayar ağlarına çok benzerdir.

Kuantum ağlar, geleneksel kanallar ve düğümlerin aksine kuantum düğümler ve kanalları kullanılarak oluşturulur. Bununla birlikte, bu topolojik yapılar üzerinde kontrol sağlamak amacıyla klasik benzerleriyle birlikte kullanılırlar. Bu nedenle bunlara akademide hibrit kuantum ağlar (Wallquist vd., 2009) olarak da bilinmektedir. Kuantum ağlarının temel amacı, geleneksel ağlara kıyasla gelişmiş iletişim güvenliği sunmak için kuantum fiziği ilkelerinden yararlanmaktır. BB84 (Bennett ve Brassard, 1984), E91 (Ekert, 1991) ve BBM92 (Bennett vd., 1992) gibi güvenli anahtar üretme teknikleri Kuantum Anahtar Dağıtım (QKD) protokollerinin birer uygulaması olarak geliştirilmiştir. Bu protokoller, kuantum kanalı kullanan taraflar arasındaki geleneksel iletişim kanalında kullanılabilecek gizli bir anahtar üretir. Günümüzde mevcut tüm deneysel kuantum ağlar öncelikle QKD protokolleri çalıştıracak biçimde tasarlanmıştır.

Kuantum ağlar, klasik ağlara benzer bir yapıya sahiptir, ancak kuantum düğümler, fotonları polarizasyon filtresinin ötesinde manipüle etme yeteneğine sahiptir ve bu onların fotonlar üzerinde kontrole sahip olmalarını gerektirir. Üstelik kuantum kanallar, mevcut fiber teknolojisine göre farklı bir tasarım yaklaşımını zorunlu kılmaktadır ve aynı zamanda çok maliyetlidirler. Bu nedenle kuantum ağlar inşa edilmeden önce fizibilite simülasyonları yapılmaktadır.

Kuantum ağ simülasyon yazılımları paralel olarak çalışabilme yeteneğine sahip olsa da orta veya büyük ölçekli kuantum ağlarını etkili bir şekilde simüle etme yeteneğinden yoksundur. Ancak deneysel kuantum ağlarında topolojinin karmaşıklığı, orta ve büyük kuantum ağlarında maliyetin katlanarak artmasına neden olur. Bu bağlamda bu tez çalışmasının amacı, simülasyonu dağıtık bir şekilde gerçekleştirerek bu soruna bir çözüm sunmaktır. Bunu gerçekleştirmek için Quantum Dynamic Network Simulator (Ceylan ve Yılmaz, 2021) yazılımına eklenti geliştirilmiştir. Dağıtılmış simülasyonun başarım ölçütlerini değerlendirmek için çeşitli kuantum anahtar dağıtım protokolleri ve çeşitli kuantum kanal ortamları içeren senaryolar test edilmiştir. Elde edilen sonuçlar göre daha önce simülasyonları zor olan kuantum ağ simülasyonlarının dağıtık olarak yapılması hem zamandan hem de maliyetten tasarruf edilebileceği göstermektedir.

Bu tez çalışması 5 bölümden oluşmaktadır. Bu tez çalışmasının ilk bölümünde kuantum teknolojilerin fiziksel temelleri, kuantum mekaniği ve kuantum bilişim alanına ait önemli kavramlar anlatılmaktadır. İkinci bölümde ise günümüze kadar inşa edilmiş önemli deneysel kuantum ağlar ve geliştirilmiş önemli kuantum ağ simülatörleri incelenmektedir. Üçüncü bölümde dağıtık simülasyon modeli ve bu modelin kuantum ağ simülatörüne nasıl eklenti olarak geliştirildiği gösterilmektedir. Dördüncü bölümde dağıtık simülasyon ile merkezi simülasyon modellerini karşılaştırmak üzere tasarlanan ağ senaryoları ve gömülü cihazlar tanıtılmaktadır. Dördüncü bölümde yapılan testlerin sonuçları tablolar üzerinde gösterilmektedir. Son bölümde kuantum ağların simülasyonlarının önemine ve bu nedenle elde edilen sonuçların bilime nasıl bir katkıda bulunabileceği tartışılmaktadır.

1.1. Kuantum Bilgi

Kuantum bilgi, bilgiyi kodlamak, işlemek ve değiştirmek için kuantum mekaniğinden türetilen kavramların kullanılmasına dayanmaktadır. Klasik bilgisayarlar, bilgiyi temsil etmenin bir aracı olarak bitleri kullanır ve her bir bit, 0 veya 1 durumunda var olabilir. Kuantum bilgi işleme, aynı anda hem 0 hem de 1'in süperpozisyonunda bulunabilen, kübitler olarak da bilinen kuantum bitlerini kullanır. Yerel bir uzayda kübitlerin süperpozisyon durumu sayesinde günümüz bilgisayarlarının kapasitelerinin üzerinde bilgi miktarının kodlanması ve işlenmesi sağlanabilmektedir. Bu ilkeleri esas alan kuantum bilgisayarlar, özellikle belirli problem kategorilerinde, klasik bilgisayarlara kıyasla çok daha yüksek verimlilikle belirli hesaplamaları yapabilme yeteneğine sahiptir.

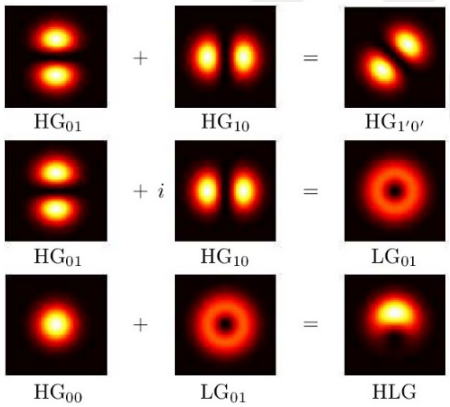
1.1.1. Kübitler

Kübitler kuantum bilginin temel biridir. Bir parçacığa eşlik eden dalga paketinin karmaşık Hilbert vektör uzayında ($\mathfrak{H}$) iki seviyeli matematiksel denkliğini ifade etmektedir. Her ne kadar farklı parçacıkları farklı fiziksel özelliklere sahip olsa da hesaplama yapmaya hazır duruma getirilen parçacıklar için kübit terimi kullanılır. Dirac notasyonu biçiminde bir sütun vektörü olarak gösterilirler ve parçacığın durum vektörü olarak ifade edilir. Bir kübitin durum vektörü özvektörlerinden biri karmaşık düzlem olan ve 1 birim yarıçaplı küresel koordinat sisteminde ifade edilebilmektedir. Bu gösterim Bloch küresi olarak bilinmektedir.

1.1.2. Süperpozisyon

Nesnelerin her zaman tek ve iyi tanımlanmış bir durumda var olduğunu varsayan klasik fiziğin aksine, kuantum parçacıklarında durum böyle değildir. Kuantum süperpozisyonu, kuantum sistemlerinin aynı anda birçok durumda var olma kapasitesini açıklayan, kuantum fiziğinde önemli bir kavramdır.

Elektronlar ve fotonlar gibi parçacıklar aynı anda birçok durumda veya konumda var olma yeteneğine sahiptir. Birden fazla durumun aynı anda bir arada bulunmasına süperpozisyon olarak adlandırılmıştır. Konsept özellikle Schrödinger'in kedi düşünce deneyi ile örneklendirilmiştir; burada bir kutu içinde hapsedilmiş bir kedinin, bir kişi kutuyu açıp bir gözlem yapana kadar aynı anda hem canlı hem de ölü bir durumda var olduğu kabul edilir.



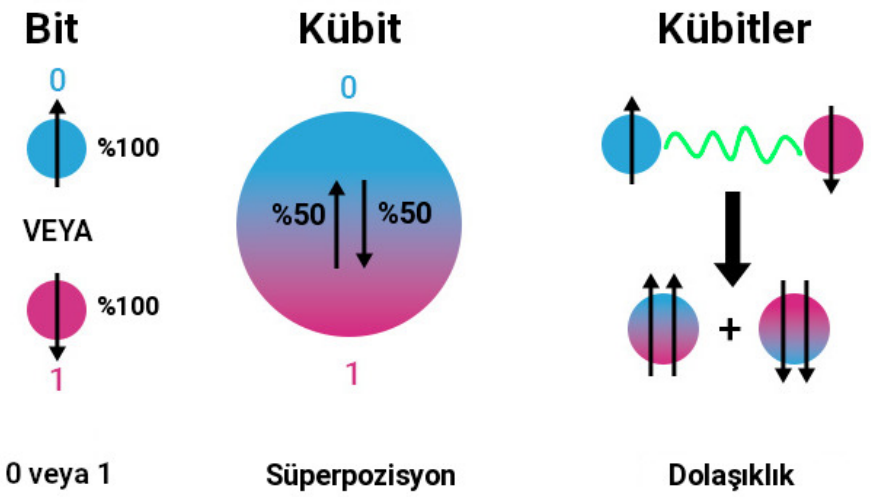
Şekil 1. Tek fotonun uzayda Hermite-Gaussian (HG) ve Laguerre-Gaussian (LG) modlarını göstermektedir (Ljunggren, 2006: 14).

Süperpozisyon ilkesi, Schrödinger'in kedisinin makroskobik alanının ötesine uzanır ve parçacıkların çok sayıda enerji seviyesi veya spin yönelimi gibi çeşitli durumların süperpozisyonunda var olabildiği kuantum seviyesinde uygulanabilir. En önemlisi, bu süperpozisyon durumu, bir ölçüm veya gözlem gerçekleşene kadar değişmeden kalır. Ölçüm durumunda sistem bir "çöküşe" uğrar ve potansiyel durumlardan birini üstlenir. Şekil 1'de bir fotonun temel modların toplamları eşitliğin solundaki süperpozisyon modlarını oluşturduğu tek foton görüntüleme kullanılarak kanıtlanmıştır.

1.1.3. Dolaşıklık

Kuantum dolaşıklığı, elektronlar veya fotonlar gibi parçacık çiftleri veya grupları arasında var olabilen benzersiz ve klasik olmayan bir korelasyondur. Parçacıklar dolaşık hale geldiğinde, bir parçacığın kuantum durumu, aralarındaki mesafeye bakılmaksızın, diğerinin durumuyla doğrudan ilişkili hale gelir. Kuantum dolaşıklığın temel özellikleri şunları içerir:

1. **Korelasyon Durumları:** Parçacıklar dolaşık yapıldığında, parçacıklar büyük mesafelerle ayrılmış olsa bile bir parçacığın özellikleri (dönme, polarizasyon veya açısal momentum gibi) diğerinin özellikleriyle ilişkili hale gelir.
2. **Anlık Korelasyon:** Dolaşmış bir parçacığın durumundaki değişiklikler, aralarındaki mesafeye bakılmaksızın diğerinin durumuna anında yansır. Işıktan hızlı bu iletişim, kuantum dolaşıklığın bir özelliğidir.
3. **Kuantum Ölçümü:** Dolaşmış bir parçacığın ölçülmesi eylemi, onun kuantum durumunu ve dolayısıyla diğer dolaşık parçacığın durumunu "çöktürür". Bu olay, parçacıklar birbirlerinden çok uzakta olsa bile anında meydana gelir.



Şekil 2. Bir klasik bit, bir parçacığın süperpozisyonu ve iki parçacığın dolaşıklık durumları gösterilmektedir. Kuantum parçacıklar biçimsel olup spin yukarı ve aşağı ikili sistem durumlarının korelasyonunu açıklamaktadır.

Şekil 2'de iki kuantum parçacık arasındaki spin korelasyonu biçimsel olarak gösterilmektedir. Şekilden görüleceği üzere dolaşıklığın sağlanması için en azından bir parçacığın süperpozisyon durumunda olmalıdır. Dolaşıklığın kuantum bilgi durumu detaylı olarak incelenmiştir (Wootters, 1998).

Dolaşıklık, kuantum mekaniğinin temellerinde çok önemli bir rol oynar ve kuantum bilgi işleme ve kuantum iletişimi gibi yeni gelişen teknolojilerde pratik uygulamalara sahiptir. Kuantum bilgisayarlar, belirli hesaplamaları klasik bilgisayarlara göre daha verimli bir şekilde gerçekleştirmek için dolaşık kübitleri kullanabilir. Ek olarak, kriptografik anahtarların güvenliğini sağlamak için benzersiz kuantum özelliklerinden yararlanan kuantum anahtar dağıtımı gibi güvenli iletişim protokolleri için kuantum dolaşıklık ayrıntılı olarak çalışılmaktadır.

1.1.4. Kopyalanamama Teorisi

Kuantum klonlamama teoremi, kuantum mekaniğinde, keyfi olarak bilinmeyen bir kuantum durumunun mükemmel bir şekilde kopyalanamayacağını veya klonlanamayacağını belirten temel bir prensiptir. Bu, bilgilerin kopyalanmasının rutin ve basit bir süreç olduğu klasik bilgilerin tersidir.

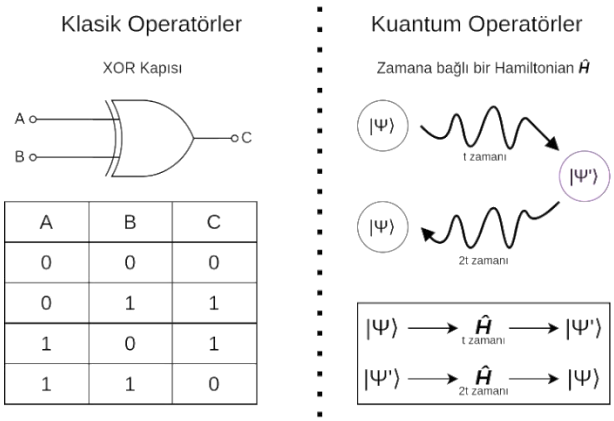
Resmi olarak kuantum klonlamanın olmadığı teoremi ilk olarak fizikçiler tarafından kanıtlandı (Wootters ve Zurek, 1982). Bu teorem rasgele bilinmeyen kuantum durumu $|\psi\rangle$ için iki özdeş kopya $|\psi\rangle\otimes|\psi\rangle$ üretebilecek bir işlem veya cihaz oluşturmak imkansızdır. Başka bir deyişle, olası tüm kuantum durumları için çalışan evrensel bir kuantum klonlama makinesi olmadığını kanıtlamaktadır.

Klonlamama teoremi, bir kuantum iletişim biçimi olan kuantum anahtar dağıtım protokollerinin güvenliğinde önemli bir kavramdır. Kuantum durumlarını klonlayamamak, bir dinleyicinin bir kuantum anahtarını ele geçirmeye çalışması durumunda, ölçümlerinin

kaçınılmaz olarak kuantum durumlarını bozacağı ve meşru kullanıcıların bu bozukluğu tespit ederek iletişimin güvenliğini sağlayabileceği anlamına gelir.

1.1.5. Terslenebilirlik

Kuantum mekaniği bağlamında terslenebilirlik, kuantum sistemlerini yöneten temel yasaların zaman simetrik olduğu, yani geçmiş ile gelecek arasında ayrım yapmadıkları fikrine atıfta bulunur. Başka bir deyişle, kuantum durumlarının evrimini tanımlayan denklemler genellikle tersine çevrilebilir ve eğer bir sistemin belirli bir zamandaki kuantum durumu biliniyorsa, prensip olarak onun geçmişini ve geleceğini belirlemek için kuantum mekaniği yasaları kullanılabilir olmaktadır. Bir kuantum sisteminin zaman içindeki evrimi Schrödinger denklemi tarafından yönetilir ve bu denklem birimseldir, yani evrim tersinir bir süreçtir. Kuantum mekaniğindeki zaman evrimi operatörü birimsel olduğundan olasılıkların zaman içinde korunmasını sağlar. Kuantum terslenebilir operatörler (Williams, 2011: 25-29) evrensel kuantum kapıları olarak da bilinmektedir.



A	B	C
0	0	0
0	1	1
1	0	1
1	1	0

Şekil 3. Klasik sistemlerde çalışan bir operatör ile kuantum parçacıklarda kullanılabilen operatörlerde terslenebilirlik karşılaştırılması. Solda özel veya operatörü ve doğruluk tablosu ile sağda kuantum zamana bağlı operatörün süreci gösterilmiştir.

Bu nedenle terslenebilirlik açısından kuantum teknolojilerin üstün olduğu söylenebilir. Şekil 3'te klasik operatör olan özel veya ile kuantum zamana bağlı bir $\hat{H}$ operatörü karşılaştırılmaktadır. Bu şekilden görüleceği üzere verilen klasik operatör **C**

çıktısının sonucundan tekrar **A** ve **B** girdilerinin kesin olarak ne olduğu hesaplanamamaktadır. Fakat kuantum parçacıklarına *t* zamanda uygulanan bir $\hat{H}$ operatörü tekrardan uygulandığında sistem *2t* zamanında başlangıç durumuna geri dönecektir.

Kuantum mekaniğinin temel yasalarının tersine çevrilebilir olmasına rağmen, kuantum mekaniğindeki ölçüm sürecinin geri döndürülemez bir yönü ortaya çıkardığını belirtmek önemlidir. Bir ölçüm yapıldığında kuantum durumu, ölçülen gözlemlenebilirin olası öz-durumlarından birine "çöker". Bu çöküş deterministik değildir ve belirli olasılıklarla farklı sonuçlar ortaya çıkabilir.

1.2. Kuantum Operatörler

Kuantum mekaniğinde operatörler veya kapılar, fiziksel gözlemlenebilirleri veya kuantum durumları üzerindeki dönüşümleri temsil eden matematiksel varlıklardır. Kuantum sistemlerinin davranışını ve evrimini tanımlamada merkezi bir rol oynarlar. Operatörler konum, momentum, açısal momentum, enerji ve daha fazlası gibi fiziksel nicelikleri temsil etmek için kullanılır. Kuantum hesaplama alanında enerji operatörü olan Hamiltoniyen operatörü kullanılmaktadır. Bu operatör bir sistemin toplam enerjisini temsil eder. Bir kuantum sisteminin zaman gelişimi, Hamilton operatörünü içeren Schrödinger denklemi tarafından yönetilir. $\hat{H}$ sembolü ile ifade edilir.

Bir kuantum sisteminin durumu tipik olarak bir dalga fonksiyonu veya bir durum vektörü ile temsil edilir. Operatörler, yeni durumlar üretmek veya sistem hakkında bilgi çıkarmak için bu durumlara göre hareket eder. Bir operatörün kuantum durumu üzerindeki eylemi, temsil ettiği fiziksel niceliğe bağlı olarak çarpma, türev alma veya entegrasyon gibi işlemleri içerebilir.

Kuantum mekaniğindeki operatörler genellikle doğrusal Hermisyen matrisleriyle temsil edilir ve özdeğerleri ölçülebilir niceliklere karşılık gelir. Operatörlerin öz-durumları, karşılık gelen gözlemlenebilirin ölçümünün kesin bir değer vereceği olası durumlardır.

1.2.1. Pauli Kapıları

Evrensel kuantum operatörlerinde (Barenco vd., 1995) 3 adet Pauli spin kapıları bulunmaktadır. Bunlar $\sigma_X, \sigma_Y, \sigma_Z$ olarak gösterilmektedir. Adını fizikçi Wolfgang Pauli'den alıyor ve tek kübitin durumunu değiştirmede kullanılan en temel kapılardır. Kuantum hesaplama ve kuantum enformatikte sıkça kullanılır.

Basitçe *X* kapısı veya *NOT* olarak adlandırılan σ_X kapısı, kuantum hesaplama ve kuantum bilgi işlemedeki temel kuantum mantık kapılarından biridir. *X* kapısı aşağıdaki matrisle temsil edilir:

$$\sigma_X = X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \tag{1.1}$$

Bir kübite uygulandığında *X* kapısı bir bit çevirme işlemi gerçekleştirir. Matematiksel olarak, eğer $|0\rangle$ ve $|1\rangle$ sırasıyla bir kübitin mantıksal 0 ve 1 durumlarını temsil eden temel özvektörler ise, o zaman *X* kapısının işlevi aşağıdaki gibidir:

$$X|0\rangle = |1\rangle \text{ ve } X|1\rangle = |0\rangle \tag{1.2}$$

Başka bir deyişle, *X* kapısı, $|0\rangle$ ve $|1\rangle$ durumlarının olasılık genliklerini etkili bir şekilde değiştirerek değiştirir. Geometrik olarak *X* kapısını, kübit durum vektörünün Bloch küresi etrafında π radyan kadar dönmesidir.

Y kapısı bir bit dönüşümü gerçekleştirir (*X* kapısına benzer şekilde) ve bir faz dönüşümü başlatır. Geometrik olarak *Y* kapısı, kübit durum vektörünün Bloch küresi etrafında *Y* ekseni yönünde π radyan (180 derece) kadar dönmesine karşılık gelir.

Matematiksel olarak, eğer $|0\rangle$ ve $|1\rangle$ sırasıyla bir kübitin mantıksal 0 ve 1 durumlarını temsil eden temel durumlarsa, Y kapısının işlevi aşağıdaki gibidir:

$$\sigma_Y = Y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}$$
$$Y|0\rangle = i|1\rangle \text{ ve } Y|1\rangle = -i|0\rangle \quad (1.3)$$

Bir kübite uygulandığında Z kapısı bir faz çevirme işlemi gerçekleştirir. Matematiksel olarak, eğer $|0\rangle$ ve $|1\rangle$ sırasıyla bir kübitin mantıksal 0 ve 1 durumlarını temsil eden temel durumlarsa, Z kapısının işlevi aşağıdaki gibidir:

$$\sigma_Z = Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$
$$Z|0\rangle = |0\rangle \text{ ve } Z|1\rangle = -|1\rangle \quad (1.4)$$

Geometrik olarak Z kapısı, kübit durum vektörünün Bloch küresi etrafında Z ekseni yönünde π radyan (180 derece) kadar dönmesine karşılık gelir. Pauli Z kapısı genellikle kuantum devrelerinde kübitlere faz değişiklikleri uygulamak için kullanılır ve çeşitli kuantum algoritmaları için temel bir yapı taşıdır.

1.2.2. Faz Kapıları

Faz kapıları, kuantum hesaplamada bir kübitin kuantum durumunun fazını değiştirmek için kullanılan bir kuantum kapısı sınıfıdır. Bu kapılar, genliğini etkilemeden kuantum durumuna bir faz kayması getirir. Faz kapıları kuantum algoritmalarının temelini oluşturur ve genellikle kuantum bilgi işleme için gereken belirli işlemleri gerçekleştirmek için kullanılır.

En yaygın faz kapısı türü R_φ kapısıdır; burada φ, kübit durumunun döndürüldüğü faz açısını temsil eder. Bir R_φ kapısının matris gösterimi şöyledir:

$$R_\varphi = \begin{bmatrix} 1 & 0 \\ 0 & e^{i\varphi} \end{bmatrix} \tag{1.5}$$

Kuantum durumu $|1\rangle$ olan bir kübite uygulandığında, R_φ kapısı duruma $e^{i\varphi}$ miktarında faz faktörünü ekler. Kübit $|0\rangle$ durumundaysa herhangi bir değişiklik olmaz. Süperpozisyondaki bir kübit üzerinde R_φ kapısının etkisi, faz faktörünün ilgili katsayılara uygulanmasını içerir.

Faz kapısının diğer bir yaygın örneği, $\varphi = \pi/2$ olduğu durumda R_φ kapısının özel bir durumu olan *S* kapısıdır:

$$S = \begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix} \tag{1.6}$$

Faz kapıları, Kuantum Faz Tahmini ve Kuantum Fourier Dönüşümü (Nielsen ve Chuang, 2010:216-242) gibi kuantum algoritmalarında çok önemlidir; burada kuantum durumlarının fazı üzerinde hassas kontrol, hesaplama avantajı için gereklidir. Bunlar, çeşitli kuantum algoritmaları için kuantum devreleri oluşturmak için kullanılan daha geniş kuantum kapıları setinin bir parçasıdır.

1.2.3. Hadamard Kapısı

Genellikle *H* olarak gösterilen Hadamard kapısı, kuantum hesaplama ve kuantum bilgi işlemede kullanılan temel bir kuantum kapısıdır. Süperpozisyon durumlarının üretilmesinde çok önemli bir rol oynar. Hadamard kapısı tek bir kübit üzerinde çalışır ve aşağıdaki matrisle temsil edilir:

$$H = \frac{1}{\sqrt{2}}\begin{bmatrix}1 & 1\\ 1 & -1\end{bmatrix} \tag{1.7}$$

Hadamard kapısının temel durumlar üzerindeki etkisi aşağıdaki gibidir:

$$\begin{aligned} &H|0\rangle\,(|0\rangle + |1\rangle)/\sqrt{2}\\ &H|1\rangle\,(|0\rangle - |1\rangle)/\sqrt{2}\end{aligned} \tag{1.8}$$

Geometrik olarak Hadamard kapısı, ekvator düzleminde yer alan Bloch küre ekseni etrafındaki bir dönüşe karşılık gelir. Hadamard kapısı, kuantum algoritmalarında kuantum paralelliği ve girişimin temelini oluşturan süperpozisyon durumlarını oluşturmak için özellikle kullanışlıdır. Çok yönlü bir kapıdır ve birçok kuantum devresinde önemli bir bileşendir.

1.2.4. Kontrollü Kapılar

Kontrollü kapı, bir veya daha fazla kontrol kübitinin durumuna bağlı olarak hedef kübit üzerinde birimsel bir işlem uygulayan bir tür kuantum kapıdır. Kapının işlevi, kontrol kübitlerinin durumuna bağlıdır ve kuantum devrelerinde koşullu işlemlere izin verir. Ayrıca kontrollü kapılar ölçüm sonucunun kullanıldığı zamanlarda klasik kontrollü olabilmektedir.

Kontrollü kapının en yaygın türü, Kontrollü-NOT (*CNOT*) kapısıdır; burada kontrol kübiti $|1\rangle$ durumundaysa hedef kübite *X* kapısı uygulanır. *CNOT* kapısının matris gösterimi ve bir kuantum duruma etkisi aşağıdaki biçimdedir:

$$CNOT = \begin{bmatrix}1 & 0 & 0 & 0\\ 0 & 1 & 0 & 0\\ 0 & 0 & 0 & 1\\ 0 & 0 & 1 & 0\end{bmatrix} \tag{1.9}$$

$$CNOT|0\rangle \otimes |a\rangle = |0\rangle \otimes |a\rangle$$
$$CNOT|1\rangle \otimes |a\rangle = |1\rangle \otimes X|a\rangle \quad (1.10)$$

Burada, $|a\rangle$ hedef kübittir ve $|0\rangle$ ile $|1\rangle$ kontrol kübitleridir. Daha genel olarak, herhangi bir tek kübitli kapı için kontrollü bir geçit oluşturulabilir. Örneğin, *U* tek kübitlik birimsel bir dönüşüm olduğu kontrollü bir *CU* kapısı, kontrol kübiti $|1\rangle$ ise *U* işlemini hedef kübite uygular. Kontrollü kapılar, kuantum devrelerindeki temel yapı taşlarıdır. Dolaşıklığın üretilmesini sağlar, koşullu kuantum operasyonlarını uygular ve kuantum hata düzeltme kodları da dahil olmak üzere çeşitli kuantum algoritmalarının temelini oluşturur.

1.2.5. Swap Kapısı

Genellikle *SWAP* olarak gösterilen kuantum takas kapısı, kuantum hesaplamada iki kübitin durumlarını değiştiren iki kübitlik bir kapıdır. Matematiksel olarak, *SWAP* kapısının $|ab\rangle$ durumlarındaki bir çift kübit üzerindeki etkisi aşağıdaki gibidir:

$$SWAP|a\rangle \otimes |b\rangle = |b\rangle \otimes |a\rangle \quad (1.11)$$

Burada $|a\rangle$ ve $|b\rangle$ iki kübitin durumlarını temsil ediyor ve *SWAP* kapısı bunların durumlarını değiştiriyor. Örneğin, eğer kübitler $|01\rangle$ durumundaysa, *SWAP* kapısı onu $|01\rangle$ dönüştürür. *SWAP* kapısının matris gösterimi şöyledir:

$$SWAP = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{bmatrix} \quad (1.12)$$

SWAP kapısı temel bir kuantum kapısıdır ve çeşitli kuantum algoritmalarında ve kuantum devre yapılarında yaygın olarak kullanılır. Kübit permütasyonunun veya değişiminin gerekli olduğu kuantum bilgi işleme görevlerinde özellikle önemlidir. Fakat *SWAP* kapısı, dolaşıklık üreten veya kuantum paralelliği gerçekleştiren bir kuantum kapısı değildir; bunun yerine, iki kübitin durumlarını doğrudan değiş tokuş eden bir kapıdır. Kuantum algoritmalarında ve kuantum iletişim protokollerinde *SWAP* kapısı, kübit durumlarını yeniden düzenlemek ve belirli hesaplama veya iletişim hedeflerine ulaşmak için stratejik olarak kullanılabilir.

1.2.6. Toffoli Kapısı

Kontrollü-kontrollü-NOT (CCNOT) kapısı olarak da bilinen Toffoli kapısı, bir hedef kübit üzerinde iki kontrol kübitinin durumlarına göre bir *NOT* kapısı gerçekleştiren üç kübitlik bir kuantum kapısıdır. Matematiksel olarak, Toffoli kapısının üç kübitlik bir durum $|abc\rangle$ üzerindeki etkisi aşağıdaki gibidir:

$$CCX|abc\rangle = \left|ab\big(c \oplus (a \wedge c)\big)\right\rangle \tag{1.13}$$

Toffoli kapısı, kuantum hesaplamada evrensel bir kapıdır; bu, herhangi bir klasik veya kuantum hesaplamanın, Toffoli kapılarının bir kombinasyonu kullanılarak ifade edilebileceği anlamına gelir. Kuantum algoritmalarında ve kuantum devre yapılarında, özellikle tersinir hesaplama ve kuantum hata düzeltme bağlamında yaygın olarak kullanılır. Toffoli kapısı ayrıca tersinir hesaplama için de kullanılabilen bir kapıdır.

1.2.7. Kuantum Ölçüm Operatörü

Kuantum mekaniğinde ölçüm süreci, bir kuantum sisteminin sonucunu belirleyen temel bir husustur. Pozitif Değerli Ölçüm olarak bilinmektedir ve genellikle $\widehat{\boldsymbol{M}}$ ile gösterilir.

Ölçüm operatörü, bir kuantum sistemi üzerinde ölçüm yapılmasıyla ilişkili matematiksel işlemi temsil eder.

Bir ölçüm operatörünün genel formu, operatörün özdeğerleri ile temsil edilen bir dizi ölçüm sonucunu ve özvektörler tarafından temsil edilen karşılık gelen bir dizi ölçüm durumunu içerir. Özdeğerleri λ_i ve özvektörleri $|\psi_i\rangle$ olan bir kuantum durumun ölçüm operatörü $\widehat{\boldsymbol{M}}$ aşağıdaki biçimde yazılabilir:

$$\widehat{M} = \sum_i \lambda_i |\psi_i\rangle\langle\psi_i| \tag{1.14}$$

Bir kuantum durumunu $|\psi\rangle$ ölçerken ölçüm sonucunu λ_i elde etme olasılığı aşağıdaki biçimde Born kuralıyla hesaplanabilir:

$$P(\lambda_i) = \langle\psi|\widehat{M}^\dagger \widehat{M}|\psi\rangle \tag{1.15}$$

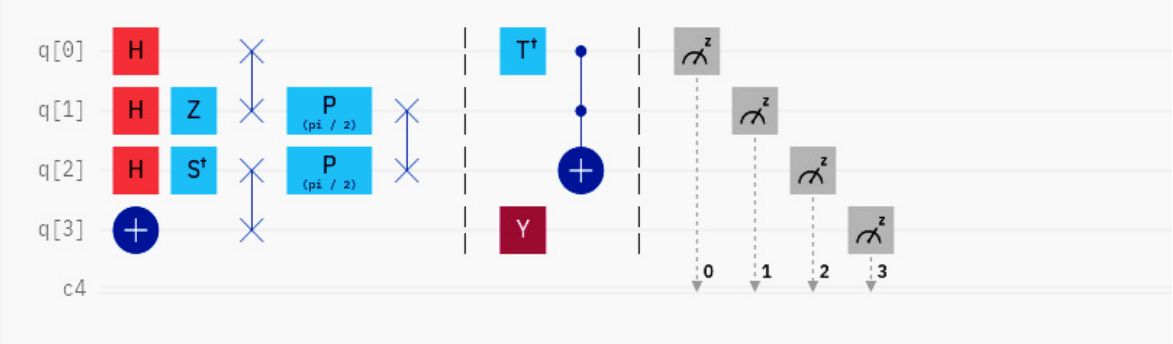
Ölçüm operatörü $\widehat{\boldsymbol{M}}$ genellikle fiziksel bir gözlemlenebilir veya ölçmek istenen bir özellik ile ilişkilendirilir. Eğer bir parçacığın $\dot{x}$ ekseni boyunca konumu ölçülüyorsa, ölçüm operatörü $\widehat{\boldsymbol{X}}$ konum operatörüne karşılık gelmektedir.

Kuantum ölçümlerinin olasılıksal doğası, kuantum sistemlerindeki doğal belirsizliği yansıtır. Bir kuantum sistemi iyi tanımlanmış bir başlangıç durumunda hazırlansa bile ölçümün sonucu kesin olarak tahmin edilemez. Bunun yerine kuantum mekaniği farklı sonuçlar için olasılıklar sağlar ve gerçek sonuç yalnızca ölçüm üzerine bilinir. Bu olasılıksal davranış, kuantum mekaniğinin temel bir yönüdür ve bir sistemin durumunun tipik olarak deterministik ve öngörülebilir olduğu klasik fizikten bir sapmadır. Kuantum ölçümünün olasılıksal doğası deneysel olarak doğrulanmıştır ve kuantum mekaniğini klasik fizikten ayıran önemli bir özelliktir.

1.3. Kuantum Algoritmalar

Kuantum algoritmalar, belirli hesaplama problemlerini klasik algoritmalardan daha verimli bir şekilde çözmek için kuantum mekaniği ilkelerinden yararlanan, bir kuantum bilgisayarında uygulanmak üzere tasarlanmış bir algoritmadır. Kuantum algoritmalar, belirli hesaplamaları paralel olarak gerçekleştirmek ve aynı anda birden fazla olasılığı keşfetmek için süperpozisyon ve dolaşma gibi benzersiz kuantum olaylarından yararlanır. Kuantum algoritmaların karakteristik özellikleri aşağıdaki biçimde listelenebilir:

1. Kuantum devre üzerinde programlanması
2. Kübitlerin temel durumda hazırlanması
3. Verilerin kübitlere işlenmesi
4. Algoritma için gerekli kapıların yerleştirilmesi
5. Kübitlerin en sonda ölçümü ve işlenmesi



Şekil 4. 4 adet kübit ve bit bulunduran bir kuantum devre örneğini göstermektedir.

Kuantum devresi kuantum hesaplamada kuantum bilgisini temsil etmek ve işlemek için kullanılan bir hesaplama modelidir. Kuantum devreler, klasik hesaplamadaki klasik devrelere benzer ancak kuantum mekaniğinin ilkelerini içerir. Kuantum devre modelinde n adet kübit her zaman temel durum olan $|0\rangle^{\otimes n}$ olarak başlamaktadır.

Şekil 4'te üzerinde tasarlanan bir kuantum devre örneği gösterilmektedir. Şekilden görülebileceği üzere kuantum devre 4 kübit ve ölçüm sonuçlarını kaydetmek için 4 adet bit bulundurmaktadır. Kübitler "**q**" ile gösterilen, bitler ise "**c**" ile gösterilen yatay çizgilerdir. Devrenin akış yönü soldan sağa doğrudur. Kare ve dikdörtgen biçimler üzerinde bulunduğu kübitlere ilgili kapının uygulandığını göstermektedir. Devrenin en sonunda ise kübitler ölçüm operatörü ile ölçülmektedir.

Bu biçimde kuantum devre modeline uyarlanmış kuantum algoritmalar hem deneysel hem de simülasyon olarak uygulanabilirler. Böylelikle birçok görevi gerçekleştirmek üzere çokça kuantum algoritma geliştirilmiştir. Fakat bu bölümde bu tezin kapsamında yer alan kuantum ağlar için önemli olan algoritmalar incelenmektedir.

1.3.1. Dolaşıklık Aktarımı

Dolaşıklık aktarımı (Su vd., 2016), iki çift parçacığın dolaşıklığının birleştirildiği veya "değiştirildiği" ve birbiriyle hiçbir zaman doğrudan etkileşime girmemiş iki parçacığın dolaşıklaş olmasına yol açan bir kuantum olgusudur. Bu süreç, dolaşık kuantum durumlarının doğasında bulunan yerel olmayan korelasyonların bir sonucudur. Dolaşıklık değişiminin temel konsepti, A, B, C ve D etiketli dört parçacığı içeren aşağıdaki senaryo aracılığıyla açıklanabilir:

İlk dolaşma: A ve B parçacıkları başlangıçta dolaşıktır ve dolaşık bir çift oluşturur. Benzer şekilde, C ve D parçacıkları da dolaşıktır ve başka bir dolaşık çift oluşturur. Bu aşamada A, B ile, C ise D ile dolaşmış durumdadır.

$$|\psi_{AB}\rangle = 1/\sqrt{2}\ (|00\rangle + |11\rangle) \tag{1.16}$$

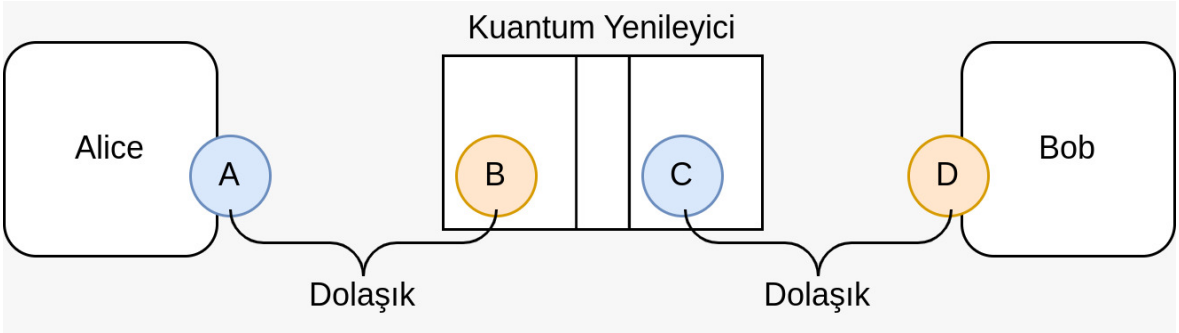
$$|\psi_{CD}\rangle = 1/\sqrt{2}\ (|00\rangle + |11\rangle) \tag{1.17}$$

Aracı parçacıkların ölçümü: Aracı parçacıklar olarak adlandırılan B ve C parçacıkları üzerinde bir Bell ölçümü gerçekleştirilir. Ölçüm sonuçları aşağıda verilen Bell durumlarından birisi olacaktır.

$$
\begin{aligned}
|\Phi^+\rangle &= 1/\sqrt{2}\ (|00\rangle + |11\rangle) \\
|\Phi^-\rangle &= 1/\sqrt{2}\ (|00\rangle - |11\rangle) \\
|\Psi^+\rangle &= 1/\sqrt{2}\ (|01\rangle + |10\rangle) \\
|\Psi^-\rangle &= 1/\sqrt{2}\ (|01\rangle - |10\rangle)
\end{aligned}
\tag{1.18}
$$

Ortaya çıkan dolaşma: Aracı parçacıklar üzerinde yapılan ölçümden sonra, A ve D parçacıkları dolaşık hale gelerek yeni bir dolaşık çift oluşturur. Dolaşma, başlangıçtaki çiftlerden (A-B ve C-D) yeni bir çifte (A-D) aktarılır. Yeni dolaşık durum bu algoritmanın 2. adımında ölçülen durum olacaktır.

$$|\psi_{AD}\rangle \in \{\Phi^+, \Phi^-, \Psi^+, \Psi^-\} \tag{1.19}$$



Şekil 5. Alice ile Bob arasında kurulan bir kuantum kanalın üzerinde dolaşıklık aktarımı yapan bir kuantum yenileyici gösterilmektedir.

Dolaşıklık değişiminin kuantum iletişiminde ve kuantum ağlarında pratik uygulamaları vardır. Uzun mesafelerde kuantum iletişimi için dolaşıklık aralığını genişletmek için kullanılabilir. Şekil 5'te dolaşıklık aktarımını kullanan bir kuantum

yenileyici örneği gösterilmektedir. Alice ile Bob arasında kurulan bir kuantum kanalın arasında bulunan kuantum yenileyici dolaşıklık aktarımı kullanmaktadır. Bu sayede dolaşıklık değişimi, kuantum iletişim kanallarında büyük mesafelerde dolaşma kaybının getirdiği sınırlamaların üstesinden gelmeyi amaçlayan bazı kuantum tekrarlayıcı protokollerinde önemli bir unsurdur.

1.3.2. Kuantum Işınlama

Kuantum ışınlanma (Bouwmeester, 1997), bir kübitin kuantum durumunun, iki dolaşmış parçacık ve klasik iletişim yardımıyla bir konumdan diğerine aktarılmasına olanak tanıyan bir kuantum iletişim protokolüdür. Adına rağmen kuantum ışınlanma, parçacıkların fiziksel taşınmasını değil, kuantum bilgisinin uzak konumlar arasında aktarılmasını içerir. Kuantum ışınlama süreci Alice ile Bob taraflarının bulunduğu senaryoda aşağıdaki sıralı adımlarla gerçekleşir:

Dolaşıklık hazırlanması: Alice ile Bob aralarında aşağıdaki biçimde matematiksel olarak ifade edilen dolaşıklık üretir.

$$|\Phi^+\rangle_{AB} = 1/\sqrt{2}\ (|00\rangle + |11\rangle) \tag{1.20}$$

Işınlanacak kuantum durum hazırlanır: Alice bilinmeyen bir durumda olan **C** kübiti ile kendi dolaşık kübit eşi arasında sırasıyla *CNOT* ve *H* kapıları uygular.

Bell ölçümü: Alice bilinmeyen durumda olan **C** kübiti ve dolaşık kübiti arasında Bell ölçümü yapar. Bell ölçümünde kullanılan ölçüm operatörü $\widehat{M}_{m1m2} = |m1m2\rangle\langle m1m2|$ olmak üzere bu adımın sonunda aşağıdaki denklem elde edilir.

$$|\psi\rangle_C \otimes |\Phi^+\rangle_{AB} \xrightarrow{Bell\ \text{ölçümü}} \sum_{m_1,m_2} M_{m1m2}\ |\psi\rangle_C \otimes |m1m2\rangle_{AB} \tag{1.21}$$

Koşullu kapılar: Alice daha sonra ölçüm sonuçlarını Bob'a iletir. Ölçüm sonucu *m1, m2* sonucuna göre Bob elindeki kübitine kapı uygular. Bu kapılar sırasıyla $X^{m2}Z^{m1}$ kapılarıdır. Koşullu kapıların ardımdan kuantum sistem aşağıdaki duruma evrilir ve Bob'un elindeki kübit **B**, Alice'in ışınlamak istediği **C** kübitinin durumuna denk olur.

$$\sum_{m1m2} M_{m1m2} X^{m2} Z^{m1} |\psi\rangle_c \otimes |m1m2\rangle_{AB} \tag{1.22}$$

1.3.3. Kuantum Süper Yoğun Kodlama

Kuantum süper yoğun kodlama (Wang vd., 2005), geleneksel olarak Alice (gönderen) ve Bob (alıcı) olarak adlandırılan iki tarafın, dolaşık kuantum parçacıklarını kullanarak klasik bilgileri daha verimli bir şekilde iletmesine olanak tanıyan bir kuantum iletişim protokolüdür. Süper yoğun kodlama, yalnızca bir kübit göndererek iki klasik bilgi bitini iletmek için kuantum dolaşma ve kuantum mekaniği ilkelerinden yararlanır. Alice ve Bob arasındaki bir süper yoğun kodlama algoritması aşağıdaki sıralı adımlar ile gerçekleşir:

Dolaşıklık hazırlanması: Alice ile Bob aralarında aşağıdaki biçimde matematiksel olarak ifade edilen dolaşıklık üretir.

$$|\Phi^+\rangle_{AB} = 1/\sqrt{2}\ (|00\rangle + |11\rangle) \tag{1.23}$$

Mesajın kodlanması: Alice göndermek istediği iki bitlik mesajı olan *m1, m2* bitlere göre kendi kübit eşine kapı uygular.

- Eğer $m_1 = 0$ ve $m_2 = 0$ ise Alice kendi kübitine hiçbir işlem yapmaz.
- Eğer $m_1 = 0$ ve $m_2 = 1$ ise Alice kendi kübitine *X* kapısı uygular.

- Eğer $m_1 = 1$ ve $m_2 = 0$ ise Alice kendi kübitine *Z* kapısı uygular.
- Eğer $m_1 = 1$ ve $m_2 = 1$ ise Alice kendi kübitine *ZX* kapısı uygular.

Elde edilen durum ise: $|\Phi^+\rangle_{AB} \xrightarrow{kodlama} |\Psi_{AB}\rangle$ olmaktadır. Alice daha sonra bu kübitini kuantum kanal yardımıyla Bob'a gönderir.

Çözümleme: Bob'un elinde bu aşamada dolaşık kübitlerin ikisi de elindedir. Bob iki kübit arasında Bell ölçümü yaparak Alice'in göndermek istediği *m1, m2* çiftini elde eder.

Süper yoğun kodlamanın verimliliği, Alice'in dolaşıklığı kullanarak yalnızca bir kübit ileterek iki klasik bilgi biti gönderebilmesinde yatmaktadır. Bu algoritma, kuantum iletişimi bağlamında kuantum dolaşmanın sezgisel olmayan ve güçlü özelliklerini sergiliyor.

1.4. Kuantum Anahtar Dağıtımı Protokolü

Kuantum Anahtar Dağıtımı (QKD), iki tarafın kriptografik anahtarları güvenli bir şekilde değiş tokuş etmesini sağlamak için kuantum mekaniğini kullanan bir şifreleme protokolüdür. QKD'nin altında yatan temel prensip, kuantum süperpozisyon ilkesi ve rastgele bilinmeyen bir kuantum durumunun tam olarak kopyalanamayacağını belirten klonlamama teoremidir. Bu özellik, QKD'nin kuantum anahtarını ele geçirmeye çalışan bir dinleyicinin varlığını tespit etmesine olanak tanır.

BB84 gibi QKD protokolleri, teorik olarak koşulsuz güvenlik sağlayacak şekilde iki taraf arasında paylaşılan bir gizli anahtar oluşturmak için kuantum mekaniği ilkelerinden yararlanır. QKD'nin güvenliği, kuantum mekaniğinin ilkelerine ve bir kuantum durumunun ölçülmesiyle ortaya çıkan rahatsızlık nedeniyle herhangi bir dinleme girişimini tespit etme yeteneğine dayanmaktadır. Ancak pratik uygulamalarda çeşitli teknolojik zorlukların ve olası yan kanal saldırılarının dikkate alınması gerekir.

1.4.1. BB84 Protokolü

BB84 (Bennett ve Brassard, 1984) protokolü, geleneksel olarak Alice (gönderen) ve Bob (alıcı) olarak adlandırılan iki tarafın güvenli bir paylaşılan anahtar oluşturmasına olanak tanıyan bir kuantum anahtar dağıtım (QKD) protokolüdür. Anahtar dağıtımının güvenliği kuantum mekaniğinin ilkelerine, özellikle de kuantum durumlarının özelliklerine dayanmaktadır. Hem klasik hem de kuantum kanalı dinleyebilen saldırgan aktör Eve'in bulunduğu BB84 protokolünün adımları şunlardır:

Anahtar üretimi: Alice iki ortonormal olmayan durumdan birisi olan kübitlerden bir Q seti hazırlar ve sonra kuantum kanal ile Bob'a gönderir. Ortonormal olmayan kuantum durumlar $|\psi_0\rangle$ ve $|\psi_1\rangle$ denklikleri aşağıdaki denklemlerden biri olsun:

$$\begin{aligned} &|\psi_0\rangle = |0\rangle, |\psi_1\rangle = |1\rangle \\ &|\psi_0\rangle = |+\rangle, |\psi_1\rangle = |-\rangle \end{aligned} \tag{1.24}$$

Alice sonra kübitlerini kodlamak için bir baz seti $B \in \{|\psi_0\rangle, |\psi_1\rangle\}$ seçer.

Tablo 1

BB84 anahtar üretimi adımında tarafların elindeki veriler

Alice	Eve	Bob
Q, B	Q	Q

Bob'un ölçümü: Bu adımda Bob, gönderici olan Alice'ten Q kübit setini almaktadır. Bob sonra setteki her bir kübit için bir baz $\acute{B}$ seti hazırlar. Bob kübitleri sırasıyla o kübit için seçtiği rastgele baz ile ölçüm yaparak ölçüm sonuçları olarak M_B setini elde eder.

Tablo 2

BB84 Bob'un ölçümü adımında tarafların elindeki veriler

Alice	Eve	Bob
Q, B	Q	Q
-	-	$\acute{B}, M_B$

Bazların duyurulması: Alice ve Bob klasik kanalı kullanarak her kübit için seçtikleri bazları duyururlar.

Tablo 3

BB84 bazların duyurulması adımında tarafların elindeki veriler

Alice	Eve	Bob
Q, B	Q	Q
-	-	$\acute{B}, M_B$
$\acute{B}$	$B, \acute{B}$	B

Anahtarın oluşturulması: Alice ve Bob seçtikleri B ve $\acute{B}$ bazlarında aynı olan elemanlarından bir altküme S_B setini oluştururlar. Bob bu seti kullanarak beklenen ölçüm sonuçları M_S ile daha önce elde ettiği M_B sonuçlarını karşılaştırır. Eğer karşılaştırma belirli bir eşik değerini aşamaz ise kanalda bir saldırgan olduğu ortaya çıkar. Eğer saldırgan yok ise aralarındaki iletişimin gizli şifresi eşleşen bazlardan oluşmaktadır.

Tablo 4

BB84 anahtarın oluşturulması adımında tarafların elindeki veriler

Alice	Eve	Bob
Q, B	Q	Q
-	-	$\acute{B}, M_B$
$\acute{B}$	$B, \acute{B}$	B
S_B	S_B	S_B, M_S

Saldırgan aktör Eve kuantumun kopyalanamaz mekaniklerinden dolayı ölçüm yaptığı Alice'in Q kübitleri Bob'a ulaşmadan farklı kuantum durumlara çökmektedir. Bu nedenle saldırganın var olduğu bir senaryoda M_B ile M_S ölçüm sonuçları setlerinin eşleşme oranı eşik değerini aşamaz. BB84 protokolü için yapılan güvenlik analizi (Renner, 2008:75-95) sonucunda anahtar uzunluğu 1000 ve üzeri kübit olduğu durumda geleneksel saldırı yöntemleri ile bu protokolün kırılamaz olduğu teorik olarak kanıtlanmıştır.

1.4.2. E91 Protokolü

Ekert-91 protokolü olarak da bilinen E91 (Ekert, 1991) protokolü, fizikçi Artur Ekert tarafından 1991 yılında önerilen bir kuantum anahtar dağıtım (QKD) protokolüdür. Diğer QKD protokolleri gibi, E91 de geleneksel olarak Alice (gönderen) olarak adlandırılan ve iki tarafı etkinleştirmek için tasarlanmıştır. Bob (alıcı), kuantum mekaniğinin ilkelerini kullanarak paylaşılan bir gizli anahtar oluşturacak. E91 protokolü, güvenli anahtar dağıtımını sağlamak için dolaşık parçacık çiftlerine dayanması açısından BB84 gibi diğer bazı QKD protokollerinden farklıdır.

E91 protokolünün güvenliği kuantum dolaşma ilkelerine dayanmaktadır. Dolaşmış parçacıkların kullanılması, gizlice dinleme girişimlerini tespit etmek için bir yol sağlar; çünkü bir parçacık üzerinde yapılan herhangi bir ölçüm, dolaşmış ortağını etkileyerek potansiyel olarak bir dinleyicinin varlığını açığa çıkaracaktır. E91, güvenli iletişim için kuantum dolaşmanın gücünü gösteren ilk protokollerden biridir.

1.4.3. BBM92 Protokolü

Bennett-Brassard-Mermin 1992 protokolü (Bennett vd., 1992) olarak da bilinen BBM92 protokolü, 1992 yılında Charles Bennett tarafından önerilen bir kuantum anahtar dağıtım protokolüdür.

BBM92 protokolünün güvenliği, Alice tarafından kullanılan kuantum durumlarının ortogonal olmamasına dayanır. Dik olmayan durumların kullanılması, bir dinleyicinin (Eve) tespit edilebilir hatalara yol açmadan doğru ölçüm esasını ve sonuçlarını belirlemesini zorlaştıran bir kuantum ölçüm belirsizliği ortaya çıkarır.

1.4.4. MSZ96 Protokolü

Kısaca MSZ96 olarak bilinen Mu-Seberry-Zheng 1996 protokolü, kuantum anahtar dağıtımı için sıkı bir teorik çerçeve sağlayarak genel saldırılara karşı koşulsuz güvenlik sağlamaya yönelik ilk algoritmalardandır (Mu vd., 1996).

MSZ96 protokolü, kuantum anahtar dağıtımı için temel bir yapı taşı olarak "kuantum zayıf yazı-tura atma" kavramını tanıtması açısından dikkate değerdir. Protokol, sinyal vermeme ilkesini kullanıyor ve güvenli iletişim için süperpozisyon ve dolaşma gibi kuantum özelliklerinden yararlanıyor.

1.4.5. Diferansiyel Faz Kaymalı QKD Protokolü

Diferansiyel Faz Kaymalı Kuantum Anahtar Dağıtımı (Inoue vd., 2002) veya kısaca DPS-QKD, geleneksel olarak Alice (gönderen) ve Bob (alıcı) olarak adlandırılan iki taraf arasında güvenli bir şifreleme anahtarı oluşturmak için tasarlanmış özel bir tür kuantum anahtar dağıtımı protokolüdür. DPS-QKD'nin temel amacı, anahtar dağıtım sürecinin güvenliğini sağlamak için kuantum özelliklerinden yararlanmaktır. DPS-QKD protokolünün güvenliği kuantum mekaniğinin ilkelerine, özellikle de kuantum durumlarının özelliklerine ve ölçüm sürecine dayanır. Diferansiyel faz ölçümlerinin seçimi, dinleyicinin tespit edilebilir hatalara yol açmadan bilgi edinmesini daha da zorlaştırarak güvenliği artırır. Bu protokolün güvenlik analizi incelenmiştir (Scarani vd., 2009). Diğer QKD protokollerine göre pratikte uygulanması diğerlerine oranla daha kolay olduğu saptanmıştır.

1.4.6 Tuzak Durum Protokolü

Tuzak durumu protokolü (Wang, 2005) veya kısaca DSP, özellikle foton sayısını bölme saldırılarını (Stucki vd., 2005) içeren belirli saldırı türlerine yönelik güvenlik açıklarını azaltarak kuantum iletişim sistemlerinin güvenliğini artırmak için kuantum anahtar dağıtımında kullanılan bir tekniktir. Bu protokol, kuantum kanalı üzerindeki potansiyel gizlice dinleme girişimlerinin etkisini tespit etmek ve en aza indirmek için tasarlanmıştır.

Tuzak durumu protokolü, Alice ve Bob'un kanal üzerinden gönderilen kuantum durumlarının istatistiklerini tahmin etmesine izin vererek ek bir güvenlik katmanı sağlar. Bu bilgi daha sonra potansiyel gizlice dinleme girişimlerini, özellikle de bir kulak misafirinin tespit edilmeden kuantum durumları arasında ayrım yapmaya çalıştığı foton sayısını bölme saldırılarını içerenleri tespit etmek için kullanılır. Tuzak durumlarını birleştirerek, QKD sistemi güvenlik parametrelerini uyarlanabilir bir şekilde ayarlayabilir, bu da onu belirli saldırı türlerine karşı daha dayanıklı hale getirir ve oluşturulan anahtarın güvenliğine daha yüksek düzeyde güven sağlar.

İKİNCİ BÖLÜM
ÖNCEKİ ÇALIŞMALAR

Kuantum iletişim alanında amaç, önemli mesafelerde bulunan kuantum işlemciler arasında kübitlerin iletilmesidir. Bu yöntemi kullanarak yerel kuantum ağlarını birbirine bağlayarak bir kuantum internet oluşturmak mümkündür. Kuantum internet (Kimble, 2008), kuantum dolaşmış kübitler üretme yeteneğini kullanarak çeşitli uygulamalara olanak tanır ve uzak kuantum bilgisayarlar arasında bilgi aktarımına olanak tanır. Kuantum internete yönelik uygulamaların çoğunluğu yalnızca küçük ölçekli kuantum işlemcileri gerektirir. Kuantum kriptografisindeki kuantum anahtar dağıtımı gibi kuantum internet protokollerinin çoğunda, bu işlemcilerin aynı anda yalnızca bir kübiti manipüle etme ve ölçme yeteneğine sahip olması tatmin edicidir. Kuantum internet uygulamaları, genellikle tek bir kübitten oluşan minimum kuantum bilgisayarları gerektirir; çünkü kuantum dolaşma yalnızca iki kübitle zaten gerçekleştirilebilir. Dolaşmış bir kuantum sisteminin geleneksel bir bilgisayarda simüle edilmesi, aynı anda hem aynı düzeyde güvenlik hem de hız elde edemez.

2.1. Kuantum Ağların Öğeleri

Bir kuantum ağı topolojisi klasik bilgisayar ağları topolojilerine benzemektedir. Bir kuantum ağı için gereken öğeler aşağıdaki biçimde listelenebilir:

- Düğümler
- Kuantum kanallar
- Kuantum tekrarlayıcılar

2.1.1. Düğümler

Kuantum ağ düğümleri hem bilgi alma hem de iletme yeteneğine sahiptir. QKD, foton detektörlerle birlikte telekomünikasyon lazerleri ve parametrik aşağı dönüştürme kullanılarak elde edilebilir.

Bununla birlikte, birçok protokolde daha gelişmiş düğümlere sahip olmak tercih edilir. Bu sistemler gelişmiş işleme yetenekleri sunar ve aynı zamanda kuantum tekrarlayıcılar olarak da işlev görebilir. Bu sistemlerin en büyük faydalarından biri, temel kuantum durumunda herhangi bir bozulmaya neden olmadan kuantum bilgisini saklama ve iletme yetenekleridir. Depolanan kuantum durumu, elektronun manyetik alandaki göreceli dönüşü veya enerji durumu olabilir. Ayrıca kuantum mantık kapılarını çalıştırma yeteneğine de sahiptirler.

Bu düğümlere ulaşmaya yönelik bir yaklaşım, elmastaki renk merkezlerinin, yani nitrojen boşluk merkezinin kullanılmasıdır. Bu sistem, birkaç kübitten oluşan kompakt bir kuantum işlemciden oluşuyor. NV merkezleri ortam sıcaklıklarında kullanılabilir. Bu sistem halihazırda kuantum algoritmalarının ve kuantum hata düzeltmesinin (Cramer vd., 2016) küçük ölçekte uygulanmasını sergilemiştir. Ek olarak, iki kuantum işlemciyi dolaştırma ve deterministik kuantum ışınlamayı gerçekleştirme yeteneğini de gösterdi (Hensen vd., 2015).

2.1.2. Kuantum Kanallar

Kuantum ağlarını büyük mesafelerde çalıştırmaya yönelik baskın yaklaşım, optik ağların ve fotonlara dayalı kübitlerin kullanılmasını içerir. Bunun nedeni, optik ağların uyumsuzluk yaşama olasılığının daha düşük olmasıdır. Optik ağlar, önceden var olan optik fiberi kullanma yeteneğinden yararlanır. Alternatif olarak, boş alan ağları, kuantum bilgisini atmosfer yoluyla veya boşlukta taşımak için kullanılabilir (Gisin vd., 2002).

2.1.3. Kuantum Tekrarlayıcılar

Gerçek bir kuantum tekrarlayıcı, kuantum dolaşmanın bir uçtan diğerine tam olarak üretilmesini sağlayarak, kuantum ışınlanmayı kullanarak kübitlerin iletilmesine olanak tanır. Dolaşma kuantum anahtar dağıtım protokollerinde test edilebilir. Sonuç olarak, kuantum tekrarlayıcıya olan güven düzeylerine bakılmaksızın, şifreleme anahtarlarının oluşturulması sırasında verici ve alıcının güvenliği sağlanır. Kübitlerin bir uçtan diğerine iletilmesi, kuantum internetin diğer uygulamaları için gerekli bir gerekliliktir. Sonuç olarak, bir

kuantum tekrarlayıcının uygulanması zorunlu hale gelir. Kuantum tekrarlayıcılar, dolaşık bir kübitin tüm mesafe boyunca fiziksel olarak iletilmesine gerek kalmadan uzak düğümler arasında dolaşıklığın kurulmasını sağlar.

2.2. Deneysel Kuantum Ağlar

Özellikle kuantum anahtar dağıtımı amacıyla çeşitli deneysel ağlar inşa edilmiştir. Bu ağlar, birden fazla kullanıcıyı birbirine bağlayarak küçük mesafelerde veya güvenilir tekrarlayıcılar kullanarak daha uzun mesafelerde çalışacak şekilde tasarlanmıştır. Şu anda bu ağlar, kübitlerin bir uçtan diğerine tam olarak aktarılmasını desteklemiyor ve en uzak düğümleri arasında dolaşıklığın gelişmesine de olanak vermiyor.

2.2.1. DARPA Kuantum Ağı

2002'den 2007'ye kadar faaliyet gösteren DARPA (İleri Savunma Araştırma Projeleri Ajansı) Kuantum Ağı dünyada BB84 protokolünü uygulayan ilk ağ oldu (Elliot, 2018). Boston ve Cambridge, Massachusetts'te bulunan 10 optik düğümden oluşuyordu. Sistem, 23 Ekim 2003'te BBN tesislerinde başarıyla devreye alındı. Haziran 2004'te, Cambridge ve Boston şehirlerinde yeraltı optik kabloları aracılığıyla konuşlandırıldı ve 3 yıldan fazla bir süre boyunca istikrarlı bir şekilde faaliyet gösterdi. Kullanıcının metni etiketler içine alınmıştır. Ekip ayrıca dünyanın ilk süper iletken nano telli tek foton dedektörünü geliştirdi ve kullanıma sundu. BBN Technologies, projeyi Harvard Üniversitesi ve Boston Üniversitesi Fotonik Merkezi'nden araştırmacılarla yakın iş birliği içinde çalışarak inşa etti ve yönetti.

DARPA Kuantum Ağı, geleneksel İnternet teknolojisiyle tamamen birlikte çalışabiliyordu ve IPsec'i veya diğer kimlik doğrulama biçimlerini kolaylaştırmak veya istenen herhangi bir şey için sanal özel ağların kurulması için QKD aracılığıyla elde edilen anahtar materyalin sağlanmasına olanak tanıyordu.

2.2.2. SECOQC Vienna Kuantum Ağı

2003'ten 2008'e kadar uzanan SECOQC projesi (Peev vd., 2009), kuantum kriptografisine dayalı güvenli iletişim alanını geliştirmek için birçok Avrupa üniversitesi arasında bir deneysel kuantum ağı kurdu. SECOQC projesi, noktadan noktaya kuantum bağlantılarının cihazları bağladığı, uzun mesafeli iletişimin ise tekrarlayıcılar tarafından kolaylaştırıldığı güvenilir bir tekrarlayıcı mimarisi kullanıyor.

2.2.3. Tokyo Kuantum Ağı

2010 yılında Japonya ve Avrupa Birliği'nden çeşitli kuruluşlar Tokyo Kuantum Anahtar Dağıtımı ağını kurdu ve denemeler gerçekleştirdi (Sasaki vd., 2011). Tokyo ağı, önceden var olan QKD teknolojileri kullanılarak oluşturulmuştur ve SECOQC'ye benzer bir ağ tasarımı uygulamaktadır. Tek seferlik şifrelemesi, güvenli ses ve video konferans gibi yaygın olarak kullanılan son kullanıcı uygulamalarını mümkün kılacak veri hızlarında ilk kez başarıyla uygulandı. Önceki büyük ölçekli QKD ağlarında, yüksek hızlı veri iletimi için AES gibi geleneksel şifreleme teknikleri yaygın olarak kullanılıyordu. Kuantumdan türetilmiş anahtarlar ya düşük hızlı veriler için ya da geleneksel şifreleme algoritmalarının periyodik olarak yeniden kurulması için kullanıldı.

2.2.4. Pekin-Şangay Kuantum Ağı

Çin'in Pekin ve Şanghay kentini birbirine bağlayan 2000 kilometrelik kuantum anahtar dağıtım ağının açılışı Eylül 2017'de gerçekleşti. Bu ana hattın amacı Pekin, Şangay, Shandong eyaletindeki Jinan'daki kuantum ağlarını birbirine bağlayan merkezi bir bağlantı görevi görmektir (China's 2,000-km Quantum Link Is Almost Complete, 2016). Hat tekrarlayıcı olarak 32 güvenilir düğüm kullanıyor. 2021'de araştırmacılar, güvenilir bir aktarma yapısı kullanarak 700'den fazla optik fiberi iki yerden uydu bağlantılarıyla başarıyla entegre etti. Bu, düğümler arasında yaklaşık 4.600 km'lik toplam mesafeyle sonuçlandı ve bu da onu dünyadaki en büyük kuantum iletişim ağı haline getirdi (Chen vd., 2021).

2.2.5. IQNET Kuantum Ağı

Aralık 2020'de IQNET, fiber optik teknolojisini kullanarak zaman kutusu kübitlerini 44 kilometre mesafeye başarılı bir şekilde ışınlama başarısını ayrıntılarıyla anlatan bir yayın yayınladı (Valivarthi vd., 2020). Böyle bir internet, güvenli iletişim, veri depolama, hassas algılama ve hesaplama alanlarında önemli yenilikler sunmaktadır.

2.3. Kuantum Ağ Simülatörleri

Kuantum ağ simülatörleri, kuantum iletişim ve ağ sistemlerinin davranışını modellemek ve simüle etmek için tasarlanmış yazılım araçlarıdır. Bu simülatörler araştırmacıların, bilim adamlarının ve mühendislerin kuantum bilgi aktarımının dinamiklerini, kuantum dolaşıklığının ve kuantum protokollerini kontrollü, sanal bir ortamda incelemelerine olanak tanır. Kuantum ağ simülatörleri, kuantum iletişim teknolojilerinin geliştirilmesinde, test edilmesinde ve anlaşılmasında çok önemli bir rol oynamaktadır. Kuantum ağ simülatörlerinin bazı ortak özellikleri ve yönleri şunlardır:

1. **Kuantum durumu simülasyonu:** Simülatörler, kübitler ve dolaşmış çiftler de dahil olmak üzere kuantum durumlarının oluşturulmasını, manipülasyonunu ve iletilmesini modeller. Bu durumların evrimini yöneten kuantum mekaniğini simüle ediyorlar.
2. **Kuantum kapıları ve operasyonları:** Kuantum kapıları ve operasyonları, kuantum bilgilerinin bir ağ içinde nasıl işlendiğini incelemek için simüle edilir. Bu, Hadamard kapıları ve CNOT kapıları gibi ortak kuantum kapılarının modellenmesini içerir.
3. **Gürültü modellemesi:** Simülatörler, kuantum iletişim sistemlerinin performansını etkileyebilecek çeşitli gürültü kaynaklarına yönelik modelleri içerir. Bu, araştırmacıların gürültünün etkilerini incelemesine ve hata düzeltme tekniklerini keşfetmesine olanak tanır.
4. **Kuantum anahtar dağıtımı simülasyonu:** Kuantum ağ simülatörleri genellikle güvenli iletişim için çok önemli olan QKD protokollerini simüle etmeye yönelik

modüller içerir. Bu, kuantum anahtar bitlerinin iletiminin simüle edilmesini, ölçümleri ve gizli dinleme girişimlerinin tespitini içerir.

5. **Dolaşıklık değiştirme ve Bell ölçümü:** Simülatörler, kuantum ağ protokollerinin temel bileşenleri olan dolaşıklık değiştirme ve Bell durumu ölçümlerinin modellenmesine olanak sağlar.
6. **Kuantum ağ topolojisi simülasyonu:** Simülatörler, araştırmacıların, düğümlerin düzenlenmesi, dolaşma bağlantılarının kurulması ve kuantum bilgilerinin yönlendirilmesi de dahil olmak üzere kuantum ağlarının topolojisini modellemesine olanak tanır.
7. **Ölçeklenebilirlik analizi:** Araştırmacılar kuantum ağlarının ölçeklenebilirliğini incelemek için simülatörleri kullanabilirler. Bu, ağın boyutu arttıkça kuantum iletişim protokollerinin performansının nasıl değiştiğini değerlendirmeyi içerir. Kuantum ağlar simülasyonlarında kuantum ağın ölçeklenme problemi bu tezin birincil kapsamındadır.
8. **Kaynak optimizasyonu:** Simülatörler, verimli ve güvenilir kuantum iletişimi sağlamak için kübitler ve dolaşmış çiftler gibi kuantum kaynaklarının kullanımını optimize etmeye yardımcı olur.
9. **Güvenlik analizi:** Kuantum iletişim protokollerinin güvenlik analizi için simülatörler kullanılır ve kuantum anahtar dağıtımının potansiyel saldırılara karşı sağlamlığı değerlendirilir.
10. **Kuantum hata düzeltme simülasyonu:** Simülatörler, araştırmacıların kuantum iletişim sistemlerinin güvenilirliğini artırmak için çeşitli kuantum hata düzeltme tekniklerini denemelerine olanak tanır.
11. **Görselleştirme ve analiz araçları:** Kuantum ağ simülatörleri genellikle araştırmacıların simülasyon sonuçlarını anlamalarına ve analiz etmelerine yardımcı olmak için görselleştirme araçlarıyla birlikte gelir. Bu, kuantum durumlarının, dolaşma bağlantılarının ve daha fazlasının grafiksel temsillerini içerebilir.

2.3.1. SimulaQron

SimulaQron (Dahlberg vd., 2018), kuantum internetin geliştirilmesi için özel olarak tasarlanmış bir simülatördür. Sistem, bir kuantum ağının düğümlerinde bulunan ve simüle edilmiş kuantum bağlantılarıyla birbirine bağlanan birçok kuantum işlemcisini taklit eder. SimulaQron öncelikle bir ağın uygulama katmanını taklit etmeye hizmet eder. Yönlendirme gibi görevleri uygulama sorumluluğu, gerektiğinde kendi çözümünü kullanabilecek kullanıcıya devredilir. SimulaQron ayrıca simülasyonları dağıtılmış bir sistemde yürütme yeteneği sağlar. Böylelikle simülasyonların çok sayıda bilgisayarda çalışacak şekilde yapılandırılabilme kapasitesine sahiptir. SimulaQron'da biraz eksik yönlerden biri, kübitlerin gelişi açısından ilgili tarafları verimli bir şekilde koordine edecek basit bir yöntemin bulunmamasıdır. SimulaQron aynı zamanda kübit aktarımı, Einstein-Podolsky-Rosen (EPR) dolaşıklıkların kurulması, klasik bilgilerin iletilmesi gibi yeteneklere sahip ana bilgisayarları da içeriyor.

2.3.2. NetSquid

NetSquid (Coopman vd., 2020), olaylara dayalı olarak çalışan güçlü bir kuantum ağ simülatörüdür. Yazılım, kuantum kapıları ve belleğin yanı sıra gürültünün etkilerini, kuantum kanalındaki kaybı ve zamana bağlı kuantum durumlarının bozulmasını da içeren kuantum cihazlarının fiziksel özelliklerini kopyalama yeteneğine sahiptir. NetSquid, kuantum ağ protokollerinin ağın fiziksel ve bağlantı katmanlarının etkilerine karşı dayanıklılığını değerlendirmek için bir kıyaslama aracı olarak hizmet eder. Sistem, ağ inşası için modüler bir metodoloji kullanıyor ve kullanıcıların simülasyonlarını çeşitli şekillerde kişiselleştirmelerine olanak tanıyor. NetSquid, kuantum sistemlerinin zamansal dinamiklerini bütünleştirme kapasitesinde öne çıkıyor. Bu özelliklere eşlik eden ek karmaşıklığın üstesinden gelmek kullanıcının sorumluluğundadır. NetSquid'i tam olarak kullanabilmek için kullanıcının kuantum ağının donanım mimarisine ilişkin sağlam bir anlayışa sahip olması gerekir.

2.3.3. SQUANCH

SQUANCH (Barlett, 2018), SimulaQron ile karşılaştırılabilir işlevsellik sunarken aynı zamanda fiziksel katman parametrelerini ve hata modellerini özelleştirme esnekliği de sağlar. Bu, simülasyon verimliliğini artırmak için paralelleştirilebilecek dağıtılmış kuantum bilgi işlemeye yönelik simülasyonların oluşturulmasına olanak tanır. Amacı, kuantum iletimi ve ağ protokolleriyle ilgili kavramları değerlendirmek için kuantum ağlarını açıkça simüle etmektir. SQUANCH platformu, birkaç kübitin simülasyonuna olanak tanır ve kullanıcılara kendi hata modellerini dahil etme yeteneği sağlar. Böylece kuantum ağ simülatörünün gerçekçiliği artar. SQUANCH, kuantum ve klasik ağların kapsamlı bir ağ içerisinde ayrılmasını sağlarken aynı zamanda uzunluğa bağlı gürültünün kanala girmesini kolaylaştırır.

2.3.4. QuISP

QuISP ("QuISP - Quantum Internet Simulation Package", 2017), olay odaklı bir yaklaşım kullanarak kuantum tekrarlayıcı ağlarını modelleyen bir simülasyon yazılımıdır. QuISP, her ağın 100'e kadar düğüme sahip olduğu, maksimum 100 ağdan oluşan eksiksiz bir kuantum ağı kopyalamayı amaçlamaktadır. Ek olarak her düğüm 100 kübit ile donatılmıştır. Ana vurgu, fiziksel katmanın gerçekçi bir temsilini korurken, protokollerin tasarlanması ve karmaşık ve çeşitli ağların kendiliğinden davranışlarının geniş ölçekte analiz edilmesidir. QuISP'nin yaptığı gibi büyük ölçekli bir ağı simüle etmek, karşılıklı dolaşmış kübitlerin durum vektörünün üstel büyümesi nedeniyle pratik değildir. Çok sayıda kübitin durum bilgisini saklamak mümkün olmaz. QuISP kübitlere uygulanan hataları kaydederek basitleştirilmiş bir kübit veri yapısı kullanıyor.

2.3.5. SeQUeNCe

SeQUeNCe (Wu vd., 2021), QuISP ve NetSquid'in tümü ayrık olaylı kuantum ağ simülatörleridir. Kullanıcılar ağ topolojisini, düğümlerin donanım özelliklerini ve kübitlerin depolanmasıyla ilgili işlemleri özelleştirme olanağına sahiptir. SeQUeNCe, fiziksel

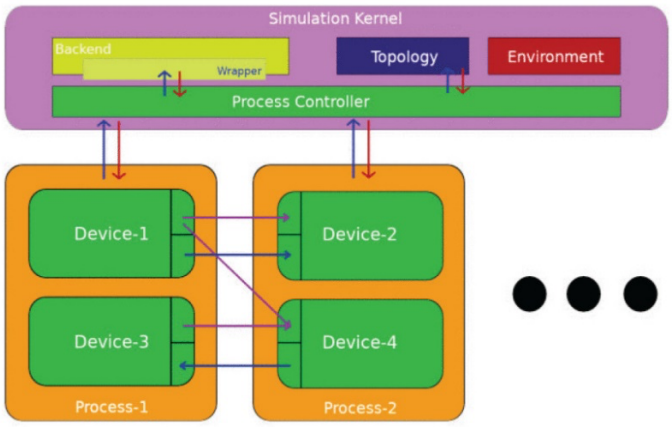
modelleri içerir ve modüller arası bağlantı yoluyla esnek simülasyonu kolaylaştıran modülerleştirilmiş bir tasarıma sahiptir. SeQUeNCe ve NetSquid mevcut kuantum ağ simülasyon yazılımları arasında en benzer olanlardır.

2.3.6. QuNetSim

QuNetSim (DiAdamo vd., 2021) gibi gerçek zamanlı bir ağ simülatörüdür. Fiziksel donanım cihazlarıyla kusursuz bağlantı sağlayarak "döngü halinde donanım" yaklaşımını içeren bir simülasyonu kolaylaştırmaktadır. Bu özelliğinden dolayı kuantum simülasyonunu mikrodenetleyici talimatları aracılığıyla kontrol etmemizi sağlar. Bu işlevselliği elde etmek amacıyla kuantum simülasyon cihazlarının somut donanımlarla değiştirilmesine olanak tanır. QuNetSim, dağıtılmış kuantum sistemlerini simüle etmek için harici bir kitaplık olarak dahil edilebilir.

2.3.7. QDNS

Bu tez kapsamında dağıtık yürütme modeli eklentisi geliştirilen QDNS yazılımı donanımı mümkün olduğunca etkin kullanma, simülasyonun dinamik kısmını yönetebilme ve kullanıcı dostu olma özellikleri ile ön plana çıkar. Bu nedenle çok katmanlı bir mimari tercih edildiği gözlemlenmiştir. Bu mimaride, her katman kendi süreci veya iş parçacığı ile gelir ve katman iletişimine erişim için kuyruklar ve kanallar bulunur.



Şekil 6. QDNS yazılımsal katmanlı mimarisi gösterilmektedir (Ceylan ve Yılmaz, 2021: 2).

QDNS yazılımı kuantum kaynakların simülasyonunda gerçekliği yakalamak için kuantum kaynakların simülasyonu için Cirq (Cirq Developers, 2021) ve Qiskit (Aleksandriwicz vd., 2019) kullanmaktadır. Ayrıca yüksek performans sağlayan Stim (Gidney, 2021) simülatörünü de bulundurmaktadır.

QDS diğer olay tetikleyici simülasyon gerçekleştiren yazılımlara göre daha dinamik yapılar sunmaktadır. Kuantum ağın simülasyon zamanında topolojik değişikliklere, çeşitli gürültü desenlerinin değişikliklerine veya düğümlerin fiziksel koşullarının değişimlere olanak sağlanmaktadır. Bunu Şekil 6 ile gösterilen çok çekirdekli mimaride dinamik emir komuta zincirlerinin olması sağlamaktadır.

Yazılım katmanlı mimarisinin dinamik değişikliklere olanak sağlaması kuantum ağ simülasyonlarının dağıtık yürütülmesine de olanak sağlamaktadır. Fakat QDNS yazılımı hazır olarak böyle bir yapı içermemektedir. Bu tez kapsamında kuantum ağların dağıtık simülasyonunu geçekleştirmek için QDNS'in dinamik yapısını kullanarak ek bir modül geliştirdik.

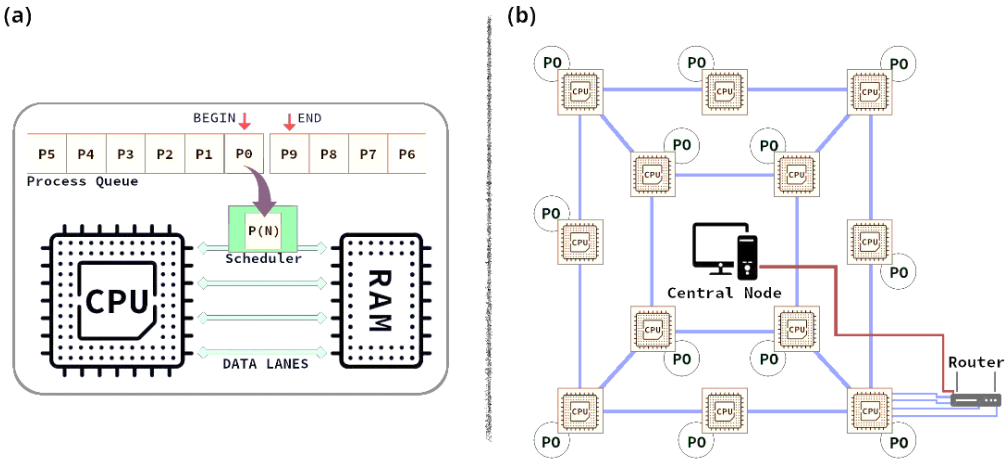
Dağıtık simülasyon modelini aynı zamanda SimulaQron simülatörü de gerçekleştirmektedir. Fakat SimulaQron yazılımı üzerinde bulunan dağıtık simülasyon modeli her ne kadar kuantum düğümleri aynı ağa bağlı farklı bilgisayarlar arasında simüle edebilmesine karşın simüle edilen tüm kuantum kaynaklar tek bir bilgisayarda toplanmaktadır. Bu nedenle SimulaQron gerçek anlamda dağıtık simülasyonu yapamamaktadır.

ÜÇÜNCÜ BÖLÜM
MATERYAL VE YÖNTEM

Bu tez kapsamında klasik bilgisayarlarda gerçekleşen bir iş yükünün aynı ağa bağlı farklı bilgisayara dağıtılarak daha performanslı çalışmasını sağlayan dağıtık simülasyon modeli incelenmiştir. Sonra bu model kuantum ağ simülasyon yazılımına eklenti olarak geliştirilerek ölçeklenebilir bir simülasyonun olabileceği gösterilmiştir.

3.1. Dağıtık Simülasyon

Dağıtılmış simülasyon, bir simülasyon modelinin birden fazla bilgi işlem kaynağına veya düğüme dağıtıldığı bir simülasyon paradigmasını ifade eder. Simülasyon, tek bir monolitik simülasyon motoru üzerinde çalışmak yerine, her biri genel sistemin bir bölümünü simüle etmekten sorumlu olan birbirine bağlı bilgisayarlardan oluşan bir ağ üzerinde yürütülür. Bu dağıtılmış simülasyonlar, büyük ölçekli, karmaşık sistemler veya önemli hesaplama kaynakları gerektiren simülasyonlar için özellikle avantajlı olabilir.



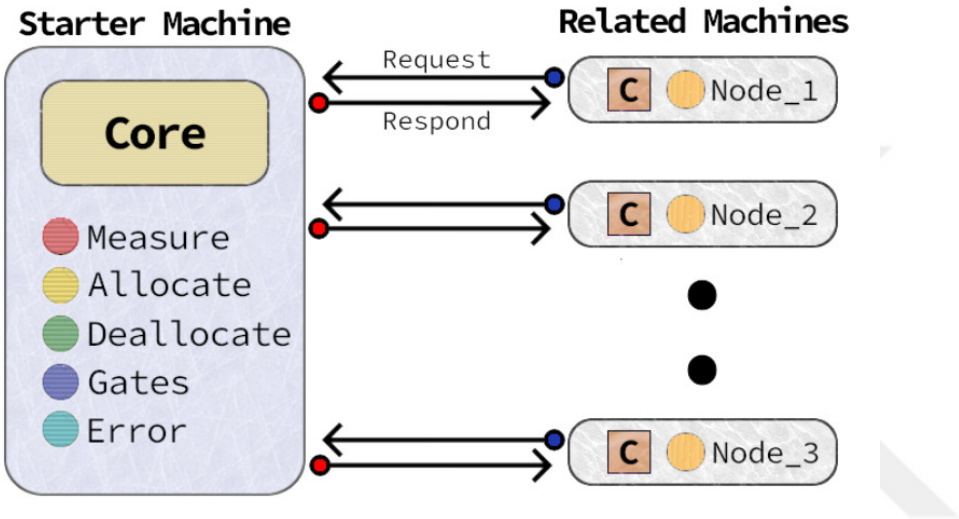
Şekil 7. Bir iş yükü için merkezi simülasyon ile dağıtık simülasyon arasındaki biçimsel fark gösterilmektedir. **(a)** Merkezi simülasyon modelinde bir işlemin merkezi işlemci biriminin (CPU) önceki işleri bitirene kadar bekleme kuyruğunda bekler. **(b)** Dağıtık simülasyonda bir ağa bağlı birden fazla CPU bir iş yükünün farklı işlemlerini tamamlamaktadır.

Dağıtılmış simülasyon modeli Şekil 7'de gösterilmektedir. Şeklin solunda bir merkezi simülasyon modelinde bir işlemci birçok işlemi çalıştırmak zorunda olduğu biçimsel olarak gösterilmektedir. Şeklin sağında ise aynı yükü farklı bir ağa bağlı birden fazla CPU kullanıldığı dağıtık simülasyon modeli gösterilmektedir. Bu model aslında çok çekirdekli yürütme modeline benzemektedir. Fakat çok çekirdekli modelde CPU çekirdeği sayısında fiziksel sınırlar bulunduğundan dolayı büyük ölçekli simülasyon yüklerinin olduğu senaryolarda dağıtık simülasyon modeli tercih edilmektedir. Dağıtılmış simülasyon modellerinin temel özellikleri aşağıdaki biçimde listelenebilir:

1. **Paralel yürütme:** Dağıtılmış bir simülasyonda, simülasyon modelinin farklı bölümleri farklı düğümlerde aynı anda yürütülebilir. Bu, paralel işlemeye olanak tanır ve genel simülasyon süresini önemli ölçüde azaltabilir.
2. **Birbirine bağlı düğümler:** Dağıtılmış bir simülasyondaki düğümler bir ağ aracılığıyla birbirine bağlanır. Bu düğümler arasındaki iletişim, simülasyon verilerinin alışverişi ve senkronizasyonun sürdürülmesi için gereklidir.
3. **Simülasyon bölümleme:** Simülasyon modeli, farklı düğümlere dağıtılabilen daha küçük, yönetilebilir bölümlere ayrılmıştır. Her düğüm, modelin kendisine atanmış kısmını simüle etmekten sorumludur.
4. **Senkronizasyon:** Tutarlılık sağlamak için senkronizasyon mekanizmaları kullanılır. Düğümlerin, dağıtılmış sistemin tamamında tutarlı bir simülasyonu sürdürmek için zamanın belirli noktalarında bilgi alışverişinde bulunması gerekir.
5. **İletişim protokolleri:** İletişim protokolleri, dağıtılmış düğümler arasında bilgi alışverişini sağlamak içindir. Bu protokoller, simülasyonun bütünlüğünü korumak için verilerin nasıl iletildiğini, alındığını ve yorumlandığını tanımlar.
6. **Yük Dengeleme:** Yük dengeleme, iş yükünün düğümler arasında eşit dağıtılmasını sağlamak için dağıtılmış simülasyonlarda önemli bir husustur. Bu, darboğazların önlenmesine yardımcı olur ve simülasyonun genel performansını optimize eder.
7. **Ölçeklenebilirlik:** Dağıtılmış simülasyon mimarileri ölçeklenebilirdir; bu da onları çok sayıda varlığı, karmaşık etkileşimleri içeren simülasyonlar için uygun kılar.

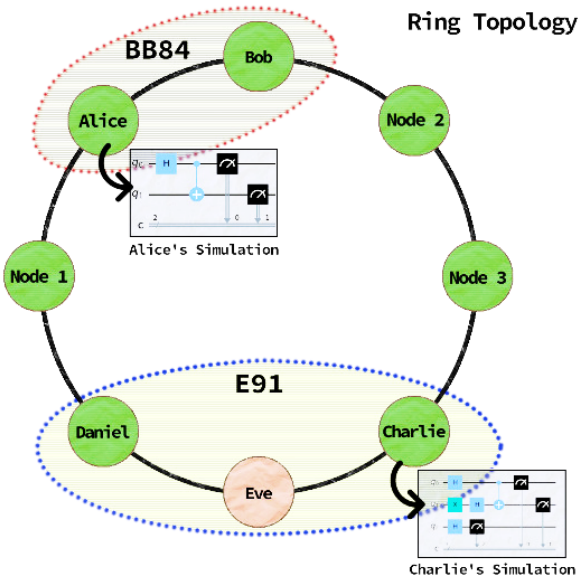
3.2. Dağıtık Simülasyonun Entegrasyonu

Dağıtık simülasyon modellerinde aynı anda aynı veriyi kullanan işlemlerin olması istenilen bir durum değildir. Kuantum ağ simülasyonlarındaki kuantum kaynaklar ise veri bağımlılığı bulunmaktadır. Bu nedenle dağıtık simülasyon modeli bu tip bir uygulama çalışma zamanında veri bağımlılığı olabilecek kaynaklar tespit edilmelidir.



Şekil 8. Bir dağıtık simülasyon esnasında bir kuantum protokol başladığı alakalı tarafların sorumlulukları gösterilmektedir.

Kuantum ağların simülasyonunu etkili bir şekilde dağıtık gerçekleştirebilmek için simülasyonun çalışma zamanında veri bağımlılığı olan kaynaklar tespit edilir. Şekil 8'de dağıtık olarak gerçekleşen bir kuantum protokolün simülasyonu esnasında kuantum kaynaklar protokolü başlatan düğüm tarafından tahsis edilmektedir. Protokolün içinde yer alan diğer düğümler kullanması mecbur olduğu kaynaklara istekler ile erişebilir. Her ne kadar kuantum kaynaklarda bağımlılık olsa da bu sadece protokolü başlatan düğümler arasında bağımlı kalır. Böylelikle gerçekleşen bir kuantum ağ simülasyonu esnasında aynı anda birden fazla yerel kuantum kaynakların tahsisi yapılarak merkezi simülasyon modelinde bulunan olası darboğazın performansa etkileri en aza indirgenir.



Şekil 9. Halka topolojisine ait bir kuantum ağının dağıtık model ile simülasyonunda protokol çalıştırma esnasında düğümlerin sorumluluklarına ait bir örnek gösterilmektedir.

Olası böyle bir senaryo Şekil 9'da bir halka topolojisinde olan bir kuantum ağın simülasyonu gösterilmektedir. Şekilde verilen senaryoda Alice, Bob, Charlie, Daniel, Eve, Node-1, Node-2 ve Node-3 isimli 8 düğümlü bir kuantum ağ bulunmaktadır. Alice ile Bob aralarında BB84, Daniel ve Charlie aralarında E91 protokolü çalıştırmak üzeredir. Kırmızı renk ile ifade edilen Eve ise ağda bulunan saldırgan bir düğümdür. Aynı anda 2 protokolün çalıştığı bu senaryoda Alice ve Charlie düğümlerinin simülasyonunu üstlenen bilgisayarlar 2 farklı kuantum kaynak oluşturmaktadır. Eğer bu simülasyon merkezi simülasyon modelinde çalışsaydı bu 2 protokol aynı anda çalışamayabilirdi. Bu şekilde 2 adet protokol örnek olarak verilmektedir ancak orta veya büyük ölçekli deneysel bir kuantum ağı aynı anda 100000'in üzerinde aynı anda kuantum işlemler yapabilmektedir. Bu ölçekteki bir ağın makul seviyede bir simülasyonu ancak dağıtık simülasyon modeli ile gerçekleşebilir.

3.3. Yazılımsal Entegrasyon

Dağıtık simülasyon modeli kuantum ağ simülatörüne entegrasyon yöntemi belirlendikten sonra bu iş için en uygun olarak belirlenen QDNS yazlımı seçilmiştir. Daha sonra QDNS'e dağıtık simülasyon modeli eklenti olarak geliştirilmiştir.

Python ile geliştirilmiş olan QDNS için bu eklentide UDP tabanlı bir veri iletişimi tercih edilmiştir. Bu eklenti QDNS'in çatı katmanında yer almaktadır. Böylelikle her cihaz üzerinde alıcısı kendisi olmayan ve işlenmek üzere gelen istekleri ve giden yanıtları ağ üzerinden ilgili düğümü simüle eden cihaza göndermektedir.

```
import QDNS
from QDNS.plugins import distribute_sim

network_conf = {
  "Center": "192.168.1.101",
  "Alice": "192.168.1.102",
  "Bob": "192.168.1.103",
  "Charlie": "192.168.1.104"
}
port = 20594
#Set this false for others.
center_node = True
```

Şekil 10. Geliştirilen dağıtık simülasyon eklentisinin içe aktarılması ve ağın ayarlanmasını sağlayan örnek Python kodu gösterilmektedir.

Geliştirilen eklentinin çalışabilmesi için tüm cihazların aynı anda ağda olması gerekmektedir. Sonra tüm cihazlar Şekil 10'da verilen Python kodu kullanılarak içe aktarılır ve bir ağ ayarı yapılandırılır.

```
  import QDNS
  from QDNS.plugins import distribute_sim

  state = distribute_sim.check_network(
network_conf, port, timeout=20)
  print(state)
```

Çıktı:

```
{ 'Alice': 'Ready', 'Bob': 'Ready', '
Charlie': 'Ready' }
```

Şekil 11. Dağıtık simülasyon eklentisinin bağlı cihazları tanımlaması sağlayan örnek Python kodu gösterilmektedir.

Dağıtık simülasyon için ayarlanan cihazların birbirlerini ağ üzerinden gördüklerini ve simülasyon için hazır durumunu kontrol edilmesi Şekil 11 ile verilen kod parçası ile yapılabilir. Bu şekilden görüleceği üzere çıktıda düğümler hazır durumundadır.

```
def main():
  alice = QDNS.Node('Alice')
  bob = QDNS.Node('Bob')
  charlie = QDNS.Node('Charlie')
  net = QDNS.Network(alice, bob,
      charlie))
  net.add_channels(alice, bob)
  net.add_channels(bob, charlie)
```

Şekil 12. QDNS yazılımı üzerinde 3 düğüme sahip basit bir kuantum ağ hazırlanmasını sağlayan örnek Python kodu gösterilmektedir.

Tez kapsamında geliştirilen eklentinin test edilebilmesi için öncelikle QDNS üzerinde simüle edilmek üzere kuantum ağlar oluşturulmalıdır. Şekil 12'de Alice, Bob ve Charlie etiketine sahip 3 düğümlü bir ağ oluşturmak için gereken kod gösterilmektedir.

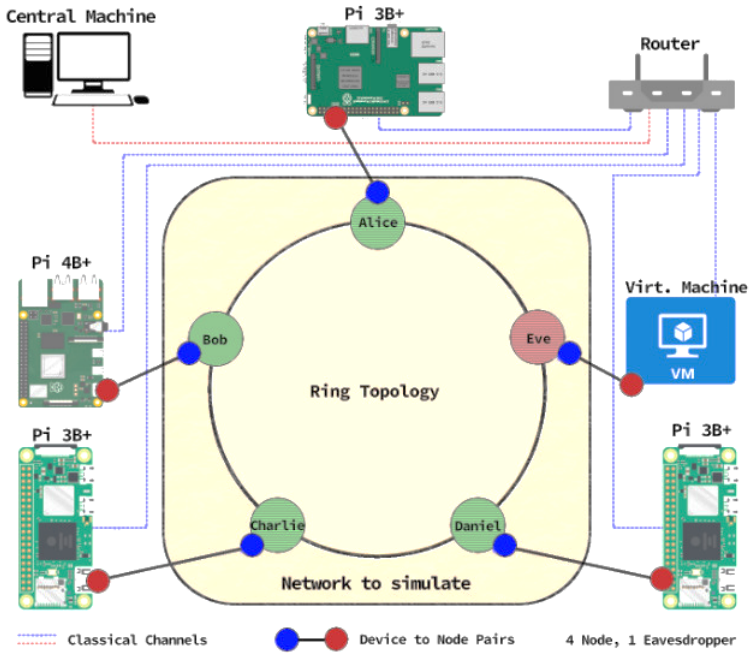
```
def main():
  ...
  backend = QDNS.STIM_BACKEND
  qubit_conf = {2: 10000}
  conf = QDNS.BackendConfiguration(
      backend, 1, qubit_conf)

  # For normal simulator
  # sim = QDNS.Simulator()

  # For distributed simulator
  sim = distribute_sim.Simulator()
  Sim.simulate(net, conf, network_conf,
  port, node=center_node)
```

Şekil 13. Geliştirilen eklenti ile dağıtık simülasyonun başlatılmasını sağlayan örnek Python kodu gösterilmektedir.

Kuantum ağ için düğüm senaryoları ilişkin cihazlara kodlandıktan sonra dağıtık simülasyon geliştirilen eklenti kullanılarak başlatılmalıdır. Şekil 13'te dağıtık simülasyonun başlatılmasını sağlayan örnek bir kod gösterilmektedir. Verilen kodda görüleceği üzere QDNS üzerindeki merkezi simülasyon modeli yerine eklentiden çağrılan dağıtık simülasyon modeli kullanılmaktadır.

DÖRDÜNCÜ BÖLÜM
ARAŞTIRMA BULGULARI

Kuantum ağ simülasyonunda dağıtık simülasyon modelinin merkezi modele avantajlarını görebilmek için test edilmesi gerekmektedir. Dağıtık yürütme modelinin testi için 3 farklı ağ senaryosu kurgulanmıştır. Kurgulanan bu ağ senaryoları hem merkezi hem de dağıtık model ile yapılan testlerde elde edilen sonuçlar sonrasında karşılaştırmalar yapılmıştır.



Şekil 14. Dağıtık simülasyon için hazırlanan test cihazlarını, ağ topolojisini ve sorumlu oldukları düğümleri göstermektedir.

4.1. Test Cihazları

Test ortamı için konak cihazlar olarak 1 adet Raspberry 4B+, 1 adet Raspberry 3B ve 2 adet Raspberry Zero modellerinde geliştirici bilgisayarlar ve 1 adet ARM tabanlı sanal makine ile merkez cihaz olarak bir masaüstü bilgisayar hazırlanmıştır. Şekil 14'te test için hazırlanan bu cihazlar ve kurulan yerel ağ görülmektedir. Raspberry Pi Zero v2 model cihazlar üreticisi tarafından sağlanan RapiOS Linux, diğer Pi modelleri ise Ubuntu Linux

işletim sistemi olarak koşmaktadır. Düğüm sayısı ile cihaz sayısı eşit olması gerektiğinden dolayı bir adet sanal makine ile geliştirilen eklentinin farklı parametreler ile nasıl çalıştığını test edilmesine ve çalışma sırasında takip yapmamıza olanak tanımaktadır. Bu sanal makine 8 çekirdekli x64 mimarisi içeren Debian bulunan sunucu makine üzerinde arm64 mimarisinde cortex-a72 işlemcisi ile çalışacak biçimde ayarlanmıştır. Tüm cihazlar 8 adet porta sahip sıradan bir yönlendiriciye CAT6 kablolar ile bağlanmıştır.

Orta veya büyük ölçekli kuantum ağın dağıtık simülasyonu için gereken cihaz sayısı ve başarım kalitesi yüksek olması gerekmektedir. Fakat küçük ölçekte bir ağı düşük başarımlı cihazlar ile yapılan farklı simülasyon modellerin karşılaştırılmasında elde edilen sonuçların benzeri biçimde ölçeklenecektir. Bu nedenle 8 düğüm içeren bir kuantum ağın gömülü sistem cihazları ile simülasyonunda elde edilen sonuçların orta ve büyük ölçekli simülasyon sonuçları ile bağlantılı olacaktır.

4.2. Simülasyon Parametreleri

Hazırlanan test ortamının parametreleri performansını ve simüle eden ağı etkileyen faktörler 2 parça olarak ele alınmıştır. Simülasyonun performansını etkileyebilecek faktörlerden olan işletim sistemi hizmetleri ve diğer arayüz gibi servisler devre dışı bırakılmıştır. Bu testlerde gömülü cihazlar tek çekirdek çalışacak düzeyde ayarlanmıştır. Kuantum ağ simülasyonunda kuantum kaynaklara direk etki eden faktörler olarak QDNS üzerinde gelen ön ayarlar kullanılmıştır. Her cihazda homojenik bir simülasyonun gerçekleşmesi gerektiğinden dolayı arka plan işleyicisi olarak Qiskit kullanılmıştır.

4.3. Simülasyon Senaryoları

Bu test için BB84 ve E91 kuantum ağ dağıtımı protokollerini farklı sırada çalıştıracak 3 farklı kuantum ağ senaryosu aşağıdaki gibi planlanmıştır:

- **Ayrık senaryo:** Bu senaryoda simülasyon başladığı anda Alice ile Daniel aralarında BB84 ve Bob ile Charlie aralarında E91 protokolü kullanarak anahtar üretimi yapacaktır. Tüm düğümler aynı anda en fazla bir adet ağ etkinliği yapmaktadır.
- **Ardışık senaryo:** Bu senaryoda simülasyon başladığı anda sırasıyla Alice ve Bob, Bob ve Charlie, Charlie ve Daniel, Daniel ve Alice etiketli düğüm ikilileri aralarında rastgele BB84 ve E91 protokolünden birini çalıştıracaktır. Bu senaryo ayrık senaryodan farklı olarak ağdaki herhangi bir düğüm aynı anda birden fazla ağ etkinliği yapmaktadır.
- **Bileşik senaryo:** Bu senaryoda ise simülasyon başladığı anda Alice aynı anda Bob, Charlie, Daniel ile aralarında rastgele BB84 ve E91 protokolü çalıştıracaktır. Bu senaryoda kuantum kaynakların tek bir düğümde toplandığı durum incelenmektedir.

Tüm senaryolarda Eve düğümünün kendisi üzerinde akan hem klasik hem de kuantum trafiği dinlemektedir. Böylelikle Eve düğümünü simüle eden cihazın çalışma zamanında dinlediği kanaldan geçen kübit kaynağını bulunduran cihaza istek atması sağlanarak her senaryolarda çalışma performansına direk etki eden bir parametre olması sağlanmıştır.

Testteki tüm senaryolarda protokol çalıştıran tarafalar aralarında 30 adet QKD protokolü çalıştıracaktır. Böylelikle simülasyon sonunda toplamda sonlanmış QKD protokolü sayısı ayrık senaryoda 60, ardışık senaryoda 120 ve bileşik senaryoda 90 adet olması beklenmektedir. Bu sayılar herhangi bir senaryonun çalışma zamanının donanım üzerinde stabil olarak test edilebilir ve fark edebilecek bir seviyede ölçülebilir sonuçları elde etmek üzere hesaplanmıştır.

4.4. Simülasyon Sonuçları

Dağıtık bir simülasyonda cihazların homojen olması her zaman daha stabil sonuçlar elde edileceği bilinse de bu testte farklı mimari ve özellikte olan cihazlar kullanarak bireysel cihazların sisteme etkileri de incelenmektedir.

Tablo 5

Hazırlanan test düzeneğinde bulunan cihazların göreceli bireysel performansı

Cihaz	Kaynak Üretimi	Kapı Uygulama	Durum Hazırlama	Ölçüm
Pi 4B+	1.0	0.6645	0.4914	0.1329
Pi 3B+	0.7407	0.4938	0.3795	0.0991
Pi Zero v2	0.5263	0.3515	0.2625	0.0701
Sanal Makine	0.4545	0.3021	0.227	0.065

Kuantum kaynakların yönetimi ile alakalı performans metriklerine en çok etkisi olan kaynak üretimi, durum hazırlama, kapı uygulama ve ölçüm yapma kategorileri altında cihazların senaryoların simülasyonunda çalıştırdıkları yükler sınıflandırıldı. Elde edilen sonuçlar Tablo 3'te verilmiştir. Sonuçlar sistemdeki en güçlü cihaz olan Pi 4B+ cihazının kaynak üretimi performansına göre göreceli olarak ölçeklendirilmiştir. Bu tablodan görüleceği üzere cihazların modeline göre cihazların çeşitli metriklerde işlemci gücüne paralel sonuçlar göstermiştir.

Tablo 6

Hazırlanan senaryoların çalışma zamanı (saniye)

Senaryo	Merkezi Model	Dağıtık Model	Dağıtık Model (Ağ gecikmesiz)
Ayrık Senaryo (60 QKD)	43.2	26.5	22.4
Ardışık Senaryo (120 QKD)	89.1	32.5	26.1
Bileşik Senaryo (90 QKD)	65.6	97.8	69.3

Hazırlanan senaryoların sonuçları Tablo 6'da verilmektedir. Ayrık ve ardışık senaryolar herhangi bir düğümde gerçekleşen QKD protokolünün kaynak olarak başka düğümlere bağlı olmadığı için merkez simülasyon modeline göre daha çabuk sonlanmakta olduğu saptanmıştır. Dağıtık simülasyon modeli yalnızca bileşik senaryoda merkeziye göre daha uzun zaman aldığı bulunmuştur. Cihazlar arsındaki iletişim ağ gecikmeleri çıkarıldığı durumda dağıtık modelin bileşik senaryoda da merkeziye yakın sonuçlar elde etmiştir.

BEŞİNCİ BÖLÜM
SONUÇ VE ÖNERİLER

Kuantum ağı simülasyonları, araştırmacıların protokolleri modellemesi ve optimize etmesi için sanal bir alan sağlayarak kuantum iletişimini geliştirmek için çok önemlidir. Süperpozisyon ve dolaşma gibi benzersiz kuantum özelliklerinin keşfedilmesine olanak tanıyarak kuantum iletişiminin daha derin anlaşılmasına olanak tanır. Simülasyonlar, protokol geliştirme ve test etmede önemli bir rol oynar; algoritmaları iyileştirmek ve hata modelleme ve düzeltmedeki zorlukları ele almak için kontrollü bir ortam sunar. Ek olarak, bu simülasyonlar kuantum protokollerinin ölçeklenebilirliğini değerlendirir, güvenlik analizlerine katkıda bulunur ve yeni teknolojileri keşfetmek, kaynak kullanımını optimize etmek ve kuantum bilgi biliminin dinamik alanında eğitim ve öğretimi kolaylaştırmak için uyarlanabilir platformlar olarak hizmet eder.

Ölçeklenebilir ağları simüle edebilen kuantum ağ simülasyonları, kuantum iletişim teknolojilerinin pratik uygulamasını ilerletmek için çok önemlidir. Kuantum ağları daha büyük ve daha karmaşık sistemlere doğru geliştikçe, bu simülasyonlar araştırmacılara kuantum protokollerinin davranışını ve performansını gerçekçi, büyük ölçekli senaryolarda değerlendirmek için kritik bir araç sağlar. Araştırmacılar, ölçeklenebilirliğin kuantum özellikleri, kaynak optimizasyonu ve ağ mimarisi üzerindeki etkisini modelleyerek zorlukları belirleyebilir, protokollerde ince ayar yapabilir ve kuantum ağlarının fizibilitesini ve sağlamlığını garanti edebilir. Bu simülasyonlar, güvenli iletişim, kuantum anahtar dağıtımı için kuantum iletişim teknolojilerinin geliştirilmesinde kilit rol oynamakta ve kuantum internetin gerçekleştirilmesinin önünü açmaktadır.

Bu nedenle orta ve büyük ölçekli kuantum ağlarını simüle etmenin yeni bir yöntemini öneren bu tez çalışması deneysel ağların kurulmadan önce daha etkin simüle edilmesinin önünü açacağı, fizibilite testlerine verebileceği katkı ile hatalı sistemlerin önüne geçebileceği aşikardır.

KAYNAKÇA

Aleksandrowicz, G., Alexander, T., Barkoutsos, P., Bello, L., Ben-Haim, Y., Bucher, D. and Marques, M. (2019). "Qiskit: An open-source framework for quantum computing". *Zenodo*, https://doi.org/10.5281/zenodo.2562111.

Barenco, A., Bennett, C. H., Cleve, R., DiVincenzo, D. P., Margolus, N., Shor, P. and Weinfurter, H. (1995). "Elementary gates for quantum computation." *Physical review A*, 52(5), 3457.

Bartlett, B. (2018). "A distributed simulation framework for quantum networks and channels". *arXiv preprint,* arXiv:1808.07047.

Bennett, C. H. and Brassard, G. (1984). "Quantum cryptography: Public key distribution and coin tossing". *Theoretical computer science,* 560, 7-11.

Bennett, C. H., Brassard, G. and Mermin, N. D. (1992). "Quantum cryptography without Bell's theorem". *Physical review letters,* 68(5), 557.

Bouwmeester, D., Pan, J. W., Mattle, K., Eibl, M., Weinfurter, H. and Zeilinger, A. (1997). "Experimental quantum teleportation". *Nature*, 390(6660), 575-579.

Ceylan, O. S. ve Yılmaz, İ. (2021, December). "QDNS: Quantum Dynamic Network Simulator Based on Event Driving", *In 2021 International Conference on Information Security and Cryptology (ISCTURKEY),* (pp. 45-50).

Chen, Y. A., Zhang, Q., Chen, T. Y., Cai, W. Q., Liao, S. K., Zhang, J. and Pan, J. W. (2021). "An integrated space-to-ground quantum communication network over 4,600 kilometres". *Nature*, 589(7841), 214-219.

Cirq Developers. (2021). "Cirq (v0.12.0)". *Zenodo,* https://doi.org/10.5281/zenodo.5182845

Coopmans, T., Knegjens, R., Dahlberg, A., Maier, D., Nijsten, L., Oliveira, J. and Wehner, S. (2020). "NetSquid, a discrete-event simulation platform for quantum networks". *arXiv e-prints,* arXiv-2010.

China's 2,000-km Quantum Link Is Almost Complete. (2016: 26 Ekim). *IEEE Spectrum: Technology, Engineering and Science News.*

Cramer, J., Kalb, N., Rol, M. A., Hensen, B., Blok, M. S., Markham, M. and Taminiau, T. H. (2016). "Repeated quantum error correction on a continuously encoded qubit by real-time feedback". *Nature communications*, 7(1), 11526.

Dahlberg, A. and Wehner, S. (2018). "SimulaQron—a simulator for developing quantum internet software". *Quantum Science and Technology*, 4(1), 015001.

DiAdamo, S., Nötzel, J., Zanger, B. and Beşe, M. M. (2021). "Qunetsim: A software framework for quantum networks". *IEEE Transactions on Quantum Engineering*, 2, 1-12.

Ekert, A. K. (1991). "Quantum cryptography based on Bell's theorem". *Physical review letters*, 67(6), 661.

Elliott, C. (2018). "The DARPA quantum network". *In Quantum Communications and cryptography,* pp. 91-110.

Gidney, C. (2021). "Stim: a fast stabilizer circuit simulator". *Verein zur Förderung des Open Access Publizierens in den Quantenwissenschaften*, 5(1), pp. 497.

Gisin, N., Ribordy, G., Tittel, W. and Zbinden, H. (2002). "Quantum cryptography". *Reviews of modern physics,* 74(1), 145.

Hensen, B., Bernien, H., Dréau, A. E., Reiserer, A., Kalb, N., Blok, M. S. and Hanson, R. (2015). "Loophole-free Bell inequality violation using electron spins separated by 1.3 kilometres". *Nature*, 526(7575), 682-686.

Inoue, K., Waks, E. and Yamamoto, Y. (2002). "Differential phase shift quantum key distribution". *Physical review letters*, 89(3), 037902.

Kimble, H. J. (2008). "The quantum internet". *Nature*, 453(7198), 1023-1030

Ljunggren, D. (2006). Entanglement in quantum communication: preparation and characterization of photonic qubits. Unpublished Ph.D. thesis, KTH Royal Institue of Technology, Institute for Management of Innovation and Technology, Stockholm, Sweeden.

QuISP - Quantum Internet Simulation Package. (2023, 12 Aralık). Erişim adresi: https://omnetpp.org/download-items/QuISP.html

Mu, Y., Seberry, J. and Zheng, Y. (1996). “Shared cryptographic bits via quantized quadrature phase amplitudes of light”. *Optics communications*, 123(1-3), 344-352.

Nielsen, M. A. and Chuang, I. L. (2010). “The quantum Fourier transform and its applications”. S. Capelin (ed.). in: *Quantum Computation and Quantum Information: 10th Anniversary Edition.* (pp. 216-242). Cambridge: Cambridge University Press: United Kingdom.

Peev, M., Pacher, C., Alléaume, R., Barreiro, C., Bouda, J., Boxleitner, W. and Zeilinger, A. (2009). “The SECOQC quantum key distribution network in Vienna”. *New Journal of Physics,* 11(7), 075001

Renner, R. (2008). “Security of quantum key distribution”. *International Journal of Quantum Information,* 6(01), 1-127.

Sasaki, M., Fujiwara, M., Ishizuka, H., Klaus, W., Wakui, K., Takeoka, M. and Zeilinger, A. (2011). *“*Field test of quantum key distribution in the Tokyo QKD Network”. *Optics express,* 19(11), 10387-10409.

Scarani, V., Bechmann-Pasquinucci, H., Cerf, N. J., Dušek, M., Lütkenhaus, N. and Peev, M. (2009). “The security of practical quantum key distribution”. *Reviews of modern physics*, 81(3), 1301.

Stucki, D., Brunner, N., Gisin, N., Scarani, V. and Zbinden, H. (2005). “Fast and simple one-way quantum key distribution”. *Applied Physics Letters,* 87(19).

Su, X., Tian, C., Deng, X., Li, Q., Xie, C. and Peng, K. (2016). *“*Quantum entanglement swapping between two multipartite entangled states”. *Physical Review Letters*, 117(24), 240503.

Valivarthi, R., Davis, S. I., Peña, C., Xie, S., Lauk, N., Narváez, L. and Spiropulu, M. (2020). “Teleportation systems toward a quantum internet”. *PRX Quantum,* 1(2), 020317.

Wallquist, M., Hammerer, K., Rabl, P., Lukin, M. and Zoller, P. (2009). “Hybrid quantum devices and quantum engineering”. *Physica Scripta*, 2009(T137), 014001.

Wang, C., Deng, F.-G., Li, Y.-S., Liu, X.-S. and Long, G. L. (2005). “Quantum secure direct communication with high-dimension quantum superdense coding”. *Physical Review A*, 71(4).

Wang, X. B. (2005). “Beating the photon-number-splitting attack in practical quantum cryptography”. *Physical review letters*, 94(23), 230503.

Williams, C. P. (2011). “Explorations in Quantum Computing”. *Springer*, pp. 25–29.

Wootters, W. K. (1998). “Entanglement of formation of an arbitrary state of two qubits”. *Physical Review Letter,* 80(10), 2245.

Wootters, W. K. and Zurek, W. H. (1982). “A single quantum cannot be cloned”. *Nature*, 299(5886), 802-803.

Wu, X., Kolar, A., Chung, J., Jin, D., Zhong, T., Kettimuthu, R. and Suchara, M. (2021). “SeQUeNCe: a customizable discrete-event simulator of quantum networks”. *Quantum Science and Technology*, 6(4), 045027.