T.C.

ÇANAKKALE ONSEKİZ MART ÜNİVERSİTESİ

LİSANSÜSTÜ EĞİTİM ENSTİTÜSÜ

MATEMATİK ANABİLİM DALI

KUANTUM DİJİTAL İMZA PROTOKOLLERİ VE UYGULAMALARI

DOKTORA TEZİ

ARZU AKTAŞ

Tez Danışmanı

Prof. Dr. İhsan YILMAZ

ÇANAKKALE – 2023

T.C.

ÇANAKKALE ONSEKİZ MART ÜNİVERSİTESİ

LİSANSÜSTÜ EĞİTİM ENSTİTÜSÜ

MATEMATİK ANABİLİM DALI

KUANTUM DİJİTAL İMZA PROTOKOLLERİ VE UYGULAMALARI

DOKTORA TEZİ

ARZU AKTAŞ

Tez Danışmanı

Prof. Dr. İhsan YILMAZ

ÇANAKKALE – 2023

T.C.
ÇANAKKALE ONSEKİZ MART ÜNİVERSİTESİ
LİSANSÜSTÜ EĞİTİM ENSTİTÜSÜ

Arzu AKTAŞ tarafından Prof. Dr. İhsan YILMAZ yönetiminde hazırlanan ve **15/08/2023** tarihinde aşağıdaki juri karşısında sunulan **"Kuantum Dijital İmza Protokolleri ve Uygulamaları"** başlıklı çalışma, Çanakkale Onsekiz Mart Üniversitesi Lisansüstü Eğitim Enstitüsü **Matematik Anabilim**'nda **DOKTORA TEZİ** olarak oy birliği ile kabul edilmiştir.

Jüri Üyeleri	**İmza**
Prof. Dr. İhsan YILMAZ (Danışman)	.....
Prof. Dr. Serkan TOPALOĞLU	.....
Dr. Öğr. Üyesi Engin ŞAHİN	.....
Dr. Öğr. Üyesi Aykut OR	.....
Dr. Öğr. Üyesi Ali AKMAN	.....

Tez No : 10566198
Tez Savunma Tarihi : 15/08/2023

.....
Prof. Dr. Ahmet Evren ERGİNAL
Enstitü Müdürü
.../...../2023

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.

Arzu AKTAŞ
15/08/2023

TEŞEKKÜR

Bu tezin geliştirilmesi ve ortaya çıkması sürecinde akademik anlamda tüm bilgi ve tecrübelerini benimle paylaşan, manevi anlamda yaşadığım her zorlu süreçte pes etmemem için elinden geleni yapıp bir an olsun yardımlarını esirgemeyen saygı değer danışman hocam Prof. Dr. İhsan YILMAZ'a, tezimizin gelişim ve oluşum sürecinde yaptığımız akademik çalışmaları sabırla dinleyip, kıymetli fikirlerini bizimle paylaşarak tezimizin bilimsel ve uygulanabilir bir çalışma haline gelmesinde çok büyük katkıları olan Tez İzleme Komitesi üyeleri Dr. Öğr. Üyesi Engin ŞAHİN'e ve Dr. Öğr. Üyesi Aykut OR'a, bu zorlu süreçte beni hiç yalnız bırakmayan, yaşam kaynağım kızlarım Su AKTAŞ ve Toprak AKTAŞ'ın hayatlarında eksik kaldığım zamanlarda bir an olsun yokluğumu hissettirmeyen ve bilgi ve tecrübesiyle her daim yanımda olan sevgili eşim Doç. Dr. Can AKTAŞ'a sonsuz teşekkürlerimi sunarım.

Ayrıca, Çanakkale Onsekiz Mart Üniversitesi YÖK 100/2000 "Kuantum Programlama" öncelikli alanlar doktora burs programı tarafından desteklenen tez çalışmamdan dolayı Yükseköğretim Kurulu'na teşekkür ederim.

Arzu AKTAŞ

Çanakkale, Ağustos 2023

ÖZET

KUANTUM DİJİTAL İMZA PROTOKOLLERİ VE UYGULAMALARI

Arzu AKTAŞ
Çanakkale Onsekiz Mart Üniversitesi
Lisansüstü Eğitim Enstitüsü
Matematik Anabilim Doktora Tezi
Danışman: Prof. Dr. İhsan YILMAZ
15/08/2023, 61

Bu çalışmada, dolaşıklık takası ve süperyoğun kodlama kullanılarak çok katılımcı için yüksek boyutlu bir kuantum dijital imza (QDS) şeması önerilmiştir. Gürültü problemlerinin üstesinden gelmek ve daha fazla bilgi aktarımı sağlamak gibi avantajları olan yüksek boyutun kullanılması, önerilen yüksek boyutlu kuantum dijital imzanın daha güvenli bilgi paylaşımı sunmasına olanak sağlamaktadır. Ayrıca, anahtar paylaşımı için süperyoğun kodlama kullanmak ve mesajları yeni bir temele dönüştürmek, önerilen protokolü daha güvenli hale getirmektedir. N boyutta, bir veriyi kodlamak için $\log_2 N$ klasik bit (veya kübit) gerekir. Yani boyut arttıkça bilgi kapasitesi de artmaktadır. $N \to \infty$ olduğunda, bilgi dizisinin uzunluğu da artacaktır. Bu nedenle, $n \to \infty$'a yaklaşır. $n \to \infty$ için $\frac{1}{4^n} \to 0$'a yaklaşır. Bu nedenle, dinleyicinin herhangi bir katılımcı tarafından paylaşılan genel anahtarı elde etme olasılığı sıfıra yaklaşır.

Anahtar sözcükler: Kuantum Dijital İmza, Yüksek Boyut, Dolaşıklık Takası, Süperyoğun Kodlama

ABSTRACT

QUANTUM DIGITAL SIGNATURE PROTOCOLS AND APPLICATIONS

Arzu AKTAŞ

Çanakkale Onsekiz Mart University

School of Graduate Studies

Doctoral Dissertation in Matematik

Supervisor: Prof. Dr. İhsan YILMAZ

08/15/2023, 61

In this study, a high dimensional quantum digital signature(QDS) scheme is proposed for multi-partied by using entanglement swapping and super-dense coding. The use of high dimension, which has advantages such as overcoming noise problems and enabling more information transfer, allows the proposed high-dimensional quantum digital signature to offer more secure information sharing. Furthermore, using super-dense coding for key sharing and converting messages into new basis make the proposed protocol more secure. In Ndimension, $\log_2 N$ classical bits (or qubits) are needed to encode a data. That is, as the size increases, the information capacity also increases. When $N \to \infty$, the length of the information string will also increase. Therefore, it approaches $n \to \infty$. For $n \to \infty$, it approaches $\frac{1}{4^n} \to 0$. Therefore, the probability of the listener obtaining the global key shared by the any participant approaches zero.

Keywords: Quantum Digital Signature, High Dimension, Entanglement Swapping, Superdence Coding

İÇİNDEKİLER

Sayfa No

SİMGELER VE KISALTMALAR

$\mathscr{H}$	Hilbert uzayı
$\|\psi\rangle$	Kuantum durumu
$\|+\rangle, \|0\rangle$	Spin-yukarı durumu
$\|-\rangle, \|1\rangle$	Spin-aşağı durumu
I	Birim matris
$\otimes$	Tensörel çarpım
$\oplus$	N modülünde toplam
σ_x	Pauli- X Kapısı
σ_y	Pauli- Y Kapısı
σ_z	Pauli- Z Kapısı
$P(\theta)$	Genel Faz Kapısı
H	Hadamard Kapısı
H_N	Genelleştirilmiş Hadamard Kapısı
CNOT	Kontrollü Not Kapısı
R_x,R_y,R_z	Döndürme Kapıları
SWAP	Yer Değiştirme Kapısı
CCNOT	Toffoli Kapısı
U	Birimsel dönüşüm
P_i	Katılımcı
$\|m_i\rangle$	Gönderilecek mesajın kuantum durumu
$\|\delta_i\rangle$	Uzayın bazları
p_i	i. katılımcıya ait özel anahtar
p_i^g	i. katılımcıya ait genel(global) anahtar
$U^\dagger$	U birimsel dönüşümünün Hermitiği
$Sig_{p_i}^G$	P_i katılımcısının genel imzası
$Sig_{P_m}^{P_i}$	P_i katılımcısı tarafından paylaşılıp, P_m katılımcısı tarafından hesaplanan imza
B_n	Kuantum blok zincirine ait n. blok
$\|data_i\rangle$	Gönderilecek verinin kuantum durumu
$\|xi_i\rangle$	Uzayın bazları
$(B_n)_p$	n. bloğa ait genel anahtar

$(B_n)_s$	n. bloğa ait özel anahtar
$ID_{B_n}^{G}$	n. bloğa ait genel kimlik
$ID_{B_n}^{B_m}$	B_m bloğundan paylaşılıp B_n bloğunda hesaplanan kimlik

ŞEKİLLER DİZİNİ

BİRİNCİ BÖLÜM
GİRİŞ

Kuantum mekaniği, diğer bir adıyla **kuantum fiziği**, atom ve atom altı parçacıkların özelliklerini ve davranışlarını inceleyen ve bunu açıklamaya çalışan bir temel fizik dalıdır.

20. yüzyılın başlarında Max Planck (karacisim ışıması), Albert Einstein (fotoelektrik olay), Niels Bohr (atom spektrumunun kuantal açıklaması), Werner Heisenberg (belirsizlik ilkesi), Erwin Schrödinger (dalga denklemi), Max Born (dalga fonksiyonunun istatistiksel yorumu), John von Neumann (kuantum alan kuramı), Paul Dirac (kuantum elektrodinamiği), Wolfgang Pauli (dışarlama ilkesi) gibi bilim insanları Kuantum mekaniğinin temellerini atmışlardır ve çeşitli kavram ve kuramlar geliştirmişlerdir. Klasik fiziğin sarsılmasına neden olan bu gelişim, aynı zamanda klasik fiziğin değişmesine de neden olmuştur (Nielsen ve Chuang, 2010).

Klasik fizik kuralları her ne kadar uygulama aşamasında başarılı olsada çıplak gözle gözlemleyemediğimiz ve yüksek hıza sahip atom ve atom altı parçaçıkların özelliklerini ve davranışlarını doğru bir biçimde açıklayamamaktadır. Klasik fiziğin açıklamakta zorlandığı bu küçük varlıklara kuanta adı verilmektedir. Kuantaların dünyasına hükmeden Kuantum Kuramına göre evrende var olan her şey hem tanecik hem de dalga yapısına sahiptir. Ayrıca bu küçük varlıkların sahip olduğu süperpozisyon, dolaşıklık(entanglement), dolaşıklık transferi, teleportasyon ve no-cloning gibi özellikler bilim dünyasını bu alanda çok önemli çalışmalara sevk etmiştir. Bu çalışma alanlarının başlıcalarını, kriptografi, kuantum bilgisayarlar, tıbbi görüntüleme, sensörler, yenilenebilir enerji, nanoteknoloji, savunma sanayi şeklinde sıralayabiliriz.

Kuantum teknolojilerinin bir kısmı hızlı bir şekilde hayatımıza girmeye başlamıştır. Bunların başında, en güçlü işlemciye ve en yüksek hıza sahip bir klasik bilgisayarın bile çözümünde ciddi anlamda zaman harcadığı problemleri, çok daha kısa zamanda çözüme ulaştıran kuantum bilgisayarları gelmektedir. Kuantum bilgisayarlar sayesinde çok parametli çalışmalar ve problemler klasik bilgisayarlara göre çok daha kısa sürede analiz edilmekte ve çözümlenmektedir. Bu durum **" kuantum üstünlük"** olarak adlandırılmaktadır. Bugün kuantumda üstünlük için IBM, Google ve Microsoft gibi dünyanın önde gelen teknoloji şirketleri çok ciddi bir yarış içinde bulunmaktadırlar.

Kuantum bilgisayarlarında bugün gelinen son noktada 60 civarında kubit bulunmaktadır. IBM'in ve Google'ın kuantum bilgisayarlar ile ilgili yakın planı ise sırası ile "2023 yılına kadar 1000 kubitlik" ve " 2029'a kadar bir milyon kubitlik " bir kuantum bilgisayar üretmektir. (*Google Quantum AI*, 2023; *IBM Quantum Computing*, 2023).

Japonya'da bulunan Hokkaido Üniversitesi'nden araştırmacılar 2014 yılında Dünya'nın ilk dolaşıklıkla güçlendirilmiş mikroskoplarını ürettiler (Ono, Okamoto, ve Takeuchi, 2013). Ayrıca Queensland Üniversitesi araştırmacıları tarafından yine kuantum dolaşıklığı mantığı ile çalışan ve hücreyi tahrip etmeden, hücrenin görüntülenmesinde %35 oranında daha yüksek netlik sağlayan bir kuantum mikroskop geliştirilmiştir (Casacio vd., 2021).

Kuantum bilgisayarlar ve kuantum iletişimi de ülkelerin, jeopolitik çıkarlarından dolayı çok önemsedikleri ve gelişmesi için yüksek fonlar ayırdığı bir teknolojidir. Bu nedenle Çin, binlerce kilometre uzunluğundaki fiber optik kablolar ile şimdiden Pekin ve Şangay arasında ilk kuantum bağlantısını oluşturmuştur (Chen vd., 2021). Bağlantı, tamamen gerçekleştirilmiş bir kuantum bağlantısı değildir: düğümler tarafından bölünmüştür çünkü fotonlar, fiberde gürültüye yenik düşmeden ancak bir yere kadar gidebilirler. Gerçek bir kuantum ağının çeşitli uygulamaları olabilir, ancak iki ana uygulama, hassas senkronizasyon ve hacklenemez iletişimdir.

Tüm dünyada veri ihlallerinin ciddi oranda artması ile kuantum kriptografi de tüm dünya genelinde çalışmaların yoğunlaştığı bir kuantum teknolojisi alanı olmuştur ve bu anlamda birçok şifreleme protokolleri geliştirilmiştir. Kuantum bilgisayarların hızlı bir biçimde hayatımıza girdiği düşünüldüğünde güvenliği sağlamak adına kuantum kriptografide de her geçen gün kırılması zor kodlar, kopyalanmsı zor dijital imzalar, sahtecilik yapılması ve inkar edilmesi neredeyse imkansız protokoller geliştirilmişve geliştirilmeye de devam edilmektedir. Hatta bu protokollerde 2-boyutta karşılaşılan problemleri ortadan kaldırmak adına yüksek boyutta oluşturulan protokoller tercih edilmektedir. Bu tercihin üç temel sebebi bulunmaktadır:

- Günümüzde 2- boyutta var olan teknolojilerde veri bütünlüğünü etkileyecek biçimde bir gürültü problemi mevcuttur. Bu gürültü probleminin halledilmesinin tek yolu da yüksek boyutta çalışmaktır. Çünkü yüksek boyut, düşük boyuttaki ya da 2-boyuttaki

gürültülerden etkilenmemektir.

- Günümüzde var olan teknolojilerde (2-boyuttaki teknolojiler) bir fotonla bir kubit gönderilmektedir.Ama yüksek boyutta, bir fotonla içinde bulunulan boyutun derecesine göre daha fazla kubit gönderilmektedir. Şu anki teknolojilerde 56 boyutta, 72 boyutta fotonlardan yararlanarak yüksek boyutta dolaşıklık ya da yüksek boyutta rastgele anahtar üretilmektedir. Bu uygulanabilir bir durumdur.

- 2-boyutta yukarıda bahsettiğimiz işlemlerin gerçekleştirilmesi için kuantum hafıza gerekmektedir. Ama yüksek boyutta çalışıldığında 2 boyutta gereken hafızanın çok daha azı gerekmektedir. Hatta iyi ve doğru kurgulandığı takdirde kuantum hafızaya bile gerek olmayabilir.

Bu nedenle bu tezde yüksek boyutun avantajları kullanılarak, kuantum kriptolojinin önemli konularından biri olan " **Kuantum Dijital İmza Şeması Protokolü**" ve "**Zaman Dolaşıklı Blokzincir Protokolü**" önerilmektedir.

İKİNCİ BÖLÜM
ÖNCEKİ ÇALIŞMALAR

Kuantum dijital imzası, hem kuantum kriptografisi hem de güvenli kuantum iletişimi için gereklidir. QDS(Quantum Digital Signature) ilk olarak Gottesman ve Chuang tarafından tanımlanmıştır (Gottesman ve Chuang, 2001). Literatürde QDS ile ilgili birçok çalışma bulunmaktadır.

Zhao vd. (2019) dolaşıklık takası ile yeni çok katılımcılı kuantum anahtarı anlaşma protokolü önerdi. Li vd. (2019) dolaşıklık takası ile verimli bir kuantum özel karşılaştırma protokolü oluşturdu. Cai vd. (2019) çok parçalı bir kuantum dijital imza şemasının kriptanalizini ve ardından yeni bir saldırı stratejisini inceledi. 2020'de, Song tarafından kuantum dolaşıklığı olan kör bir imza öne sürüldü (Song, 2020). Qu vd. (2019) gereksiz kuantum bağlantıları sorununu etkili bir şekilde çözebilecek çok taraflı bir genel QDS şemasını araştırdı. Huawang vd. (2020) kuantum (t,n) eşik grubu imzası önerdi. Weng vd. (2021), bu zorlukların üstesinden gelmek için altı durumlu ortogonal olmayan bir kodlama protokolüne dayanan etkili bir çok katılımcılı QDS protokolü önerdi.

Bu çalışmalara ek olarak, kuantum teknolojilerinin gelişmesi nedeniyle deneysel olarak kuantum dijital imzalar kullanılmaya başlanmıştır. Clarke vd. (2012) kuantum dijital imzaların bir göndericiden iki alıcıya mesaj göndermeye izin verdiği, sahteciliğe ve reddedilmeye karşı garantili olduğu bir deney gösterdi. Wang vd. (2015) tarafından klasik mesajlar için kuantum dijital imzaların güvenliği gösterildi. Yin vd. (2016) kimliği doğrulanmış kuantum kanalları varsayımını ortadan kaldıran ve saldırılara karşı güvenli bir kuantum dijital imza protokolü sunmuştur. Yin vd. (2017) herhangi bir güvenli kanal varsayımı olmaksızın bir kuantum dijital imza protokolünü deneysel olarak göstermiştir. Yin vd. (2017) bir büyükşehir ağı üzerinden deneysel ölçüm cihazından bağımsız kuantum dijital imzaları göstermiştir. Lu vd. (2021) simetrik bir adım kullanmadan verimli bir kuantum dijital imza şeması önerdi. Dijital imzalar ve şifreleme ile deneysel bir kuantum güvenli ağ, Yin vd. (2021) tarafından gösterilmiştir. Pelet vd. (2022) güvenilir düğümler olmadan tamamen bağlı bir kuantum ağında uygulanan koşulsuz olarak güvenli bir dijital imza protokolünün deneysel bir gösterimini sunmuştur. Mooney vd. (2021) süper iletken bir kuantum bilgisayar kullanarak 27 kübit GHZ durumunun üretildiğini ve doğrulandığını göstermiştir.

Yukarıdaki çalışmalarda kuantum dijital imzalar 2 boyutta geliştirilmiştir. 2 durumlu kuantum ağlarda güvenlik, gürültü ve düşük seviyeli anahtar oluşturma sorunları vardır. Günümüzün pratik kübit tabanlı 2 boyutlu teknolojilerinin en büyük sorunu bilgi kaybı, gürültü ve daha fazla bellek ihtiyacı olarak ifade edilebilir. Yukarıdaki sorunlardan dolayı pratik uygulamalarda büyük zorluklarla karşılaşılmaktadır. Yüksek boyutlu kuantum süreçleri, bilgi kaybı, gürültü sorunu ve daha fazla bellek ihtiyacı sorunlarına çözüm bulmaktadır (Vagniluca vd., 2020).

Bu bağlamda literatürde pratik yüksek boyutlu kuantum işlemleri için teknolojiler geliştirilmektedir. Literatürde çok sayıda deneysel yüksek boyutlu çalışma vardır ve bunlar aşağıdaki gibi özetlenebilir. Imany vd. (2018) yüksek boyutlu frekans kutu kodlu kuantum hesaplama ve yoğun kuantum anahtar dağıtımı için bir kaynak olarak entegre optik mikro rezonatörlerin kurulumunu gösterdi. Paesani vd. (2021) doğrusal optikli GHZ durumları için evrensel yüksek boyutlu kuantum hesaplama algoritmasını sunmuştur. Shen vd. (2021) sekiz boyutta çok parçalı klasik dolaşık ışığın nasıl oluşturulacağını ve kontrol edileceğini gösterdi. Srivastav vd. (2022a) 53 boyuta kadar kuantum yönlendirmeyi deneysel olarak gösterdi ve kübit tabanlı sistemlere göre iyileştirmeler ve yüksek boyutta kayıp ve gürültünün üstesinden geldi. Hu ve Kais (2022) kuantum dalga kapılarının var olduğunu ve küdit kuantum uzayının dalga-parçacık ikiliğini gösterdi.

Literatürde yüksek boyutlu QDS çalışmalarına rastlanmamıştır. Ayrıca, yüksek boyutlu deneysel çalışmaların varlığı, yüksek boyutlu QDS'nin pratik olarak uygulanmasına izin verir. Yüksek boyutlu kuantum hesaplama, gürültü probleminin üstesinden gelmeye, daha fazla veri aktarmaya ve yüksek oranda anahtar üretmeye izin verdiğinden, bu çalışmada, çoklu katılımcılar için yüksek boyutlu dolaşıklık takasına bağlı olarak güvenli bir kuantum dijital imza protokolü geliştirilmiştir.

Cozzolino vd. (2019) yüksek boyutlu kuantum hesaplamanın artan bilgi ve iletişim kapasitesi, daha yüksek gürültü direnci, kuantum klonlama için geliştirilmiş sağlamlık, yerel teorilerin daha büyük ihlalleri ve iletişim karmaşıklığı sorunları gibi avantajlara sahip olduğunu gösterdi.

Yukarıda özetlenen çalışmalarda uzay dolaşıklığı kullanılmıştır. Ancak son zamanlarda güvenlik protokol temelli çalışmalar da var olan güvenlik açıklarını gidermek

adına zaman dolaşıklığı kullanılmıştır. Zaman dolaşıklığı kullanılarak oluşturulan kuantum blok zincir ile ilgili çalışmalar aşağıdaki gibi özetlenebilir.

Rajan ve Visser (2019) zamanda dolaşıklığı kullanan kuantum blok zincir önermişlerdir. Gao vd. (2020) tarafından zaman dolaşıklığına ve devredilen pay kanıtına (DPoS) dayanan yeni bir kuantum blok zinciri şeması önerilmiştir. Ayrıca no-cloning teoremine dayanarak, kuantum madeni para olarak adlandırılan yeni bir kripto para birimi tanımlamışlardır.

ÜÇÜNCÜ BÖLÜM
ARAŞTIRMA YÖNTEMİ/MATERYAL VE YÖNTEM

Bu bölümde kuantum hesaplamalarda kullanılan temel tanımlar ve kavramlardan bahsedilecek ve kuantumun üstünlükleri olarak ifade edilen **süperpozisyon, dolaşıklık, teleportasyon, no-cloning** ve **dolaşıklık transferine** değinilecektir.

3.1. Temel Tanım ve Kavramlar

3.1.1. Kuantum Durum

Bir kuantum mekanik sisteminin bulunabileceği olası durumlardan herhangi birine bir kuantum durum denir (Nielsen ve Chuang, 2010). Kuantum durumu, bir vektör uzayında teorik olarak kuantum sistemin hakkında istatistiksel bilgiler içeren bir durum vektörü olarak tanımlanabilir. Bir kuantum sisteminin kuantum durumunu ifade etmek için Dirac tarafından geliştirilen **"bra-ket"** gösterimi kullanılır. Bra-ket gösterimi "$\langle\,|\,\rangle$" şeklinde sembolize edilip, bu gösterim basit anlamda elimizdeki durumları ve elde etmek istediğimiz durumları ayırarak göstermeye yarar. Elimizde var olan durum ket kısmına yazılır. Örneğin; "$|p\rangle$" gösterimi, parçacığın p momentumunda olduğunu ifade etmektedir. "ket" kısmı elimizde ki bilgileri temsil ettiği için başlangıç vektörü veya başlangıç durumu olarak da ifade edilebilir.

3.1.2. Kübit

Bilginin kuantumda ifade edilebilmesi için klasik bilgisayarlarda kullanılan bit $\{1,0\}$ yerine "**kübit**" adı verilen kuantum biti kullanılmaktadır. Bir kübit, iki seviyeli (veya iki durumlu) bir kuantum mekanik sistemi olup, kuantum mekaniğinin özelliklerini gösteren en basit kuantum sistemlerinden biridir. Bir bit gibi, bir kübitte iki durumdan birinde olabilir. Bu iki durum $|0\rangle$ ve $|1\rangle$ olarak ifade edilir. Burada; $\{|0\rangle,|1\rangle\}$, Hilbert uzayında ($\mathbb{C}^2$) kullanılan temel baz vektörleridir. Bu vektörler, bir atomun farklı spinlerini, farklı enerji seviyelerini, farklı polarizasyonlarını kısacası iki farklı durumunu gösterir ve

$$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \quad ve \quad |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

$$\langle 0| = \begin{pmatrix} 1 & 0 \end{pmatrix} \quad ve \quad \langle 1| = \begin{pmatrix} 0 & 1 \end{pmatrix}$$

$$\langle 0|0\rangle = 1 \quad \langle 1|1\rangle = 1 \quad \langle 0|1\rangle = \langle 1|0\rangle = 0$$

biçiminde ifade edilmektedir (Nielsen ve Chuang, 2010).

3.1.3. Tensörel Çarpım

Daha büyük vektör uzayları oluşturmak için yani var olan vektör uzayını genişletmek için vektör uzaylarını bir araya getirmek gerekir. Bu işlem için de tensör çarpımı kullanılır. Tensör çarpımı, çok parçacıklı sistemlerin kuantum mekaniğini anlamak için kullanılan çok önemli bir işlemdir. Örneğin elimizde n-kübitlik bir sitem olsun. n-kübit, 2^n durumun kompleks lineer kombinasyonunu ifade eder.

$n = 1$ için, $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ olmak üzere bu durumun n defa tensör çarpımını alarak aşağıdaki gibi n-kübitlik çok parçacıklı bir sistem elde edebiliriz (Nielsen ve Chuang, 2010).

$$\begin{aligned} |q^n\rangle &= |\psi_1\rangle \otimes |\psi_2\rangle \otimes \cdots \otimes |\psi_n\rangle \\ &= (\alpha_1|0\rangle + \beta_1|1\rangle) \otimes (\alpha_2|0\rangle + \beta_2|1\rangle) \otimes \cdots \otimes (\alpha_n|0\rangle + \beta_n|1\rangle) \\ &= \gamma_0|00\cdots00\rangle + \gamma_1|00\cdots01\rangle + \cdots + \gamma_{N-1}|11\cdots11\rangle \end{aligned}$$

olup, burada $\gamma_0 = \alpha_1\alpha_2\cdots\alpha_n, \ldots, \gamma_{N-1} = \beta_1\beta_2\cdots\beta_n$ ve $N = 2^n$ dir.

3.1.4. Ölçme

Bir kuantum sistemin durumunun ölçülmesi onun klasik durumlardan birine çökmesine neden olur. Böylece diğer durumların bilgisini de saklayan süperpozisyon durumunu kaybetmiş oluruz. Ölçme, sistemin durumunu bozduğu için hesaplama işlemleri arasında en son yapılması gereken işlemdir. Örneğin,

$$|\phi_{ab}\rangle = (\alpha|0_a\rangle + \beta|1_a\rangle) \otimes (\gamma|0_b\rangle + \delta|1_b\rangle)$$

durumunda a kübitini ölçelim. Bu biti $|\alpha|^2$ olasılıkla 0 durumunda bulabiliriz. Bu ölçüm sonucunda sistemin durumu

$$\begin{aligned} |\psi_{ab}\rangle &= |0_a\rangle \otimes (\gamma|0_b\rangle + \delta|1_b\rangle) \\ &= \gamma|0_a 0_b\rangle + \delta|0_a 1_b\rangle \end{aligned}$$

olur. Eğer sistemin durumu dolaşık ise

$$|\psi_{ab}\rangle = \frac{1}{\sqrt{2}}(|0_a 0_b\rangle + |1_a 1_b\rangle)$$

kuantum durumunda a kübitini $\frac{1}{2}$ olasılıkla sıfır ölçeriz. Bu durumda sistemin son durumu $|\psi_{ab}\rangle = |0_a 0_b\rangle$ olur. Bu durumda b kübiti de $|0\rangle$ ölçülmüş olur (Nielsen ve Chuang, 2010).

3.1.5. Birimsel ve Hermitik Dönüşümler

Kuantum hesaplamada kübitlerden oluşan sistem üzerinde ölçüm dışında yapılabilen tek işlem tipi birimsel dönüşümlerdir. Bir operatörün transpozesinin kompleks eşleniği kendisine eşit ise bu operatör Hermitik, tersine eşit ise birimsel operatördür. Yani,

$$\begin{aligned} (U^T)^* = U \Rightarrow &\quad U \text{ Hermitik dönüşüm} \\ (U^T)^* = U^{-1} \Rightarrow &\quad U \text{ Birimsel dönüşüm} \end{aligned}$$

şeklindedir. Tüm kuantum hesaplama algoritmaları eşit olasılık genliklerine sahiptir. Tüm olası durumların süperpozisyonundan başlar ve belirli sayıda gerekli birimsel dönüşümlerin uygulanması sonucu hesaplamanın doğru sonucunun maksimum olasılık genliğine sahip olmasının sağlanması temelinde çalışır (Nielsen ve Chuang, 2010).

3.2. Kuantum Üstün Özellikler

3.2.1. Süperpozisyon

Bir kubit $|0\rangle$ ya da $|1\rangle$ durumlarında var olabildiği gibi bu durumların lineer kombinasyonlarında da var olabilir. Bu var oluş durumuna **"süperpozisyon"** durumu denir. Yani bir sistem iki veya daha fazla alt sistemden oluşuyorken, bu sistemin alt sistemleri

cinsinden ifade edilmesidir. Örneğin; atom ve atom altı parçacıkların kendi eksenleri etrafında spin olarak adlandırılan hem yukarı, hem aşağı yönelimleri aynı anda mevcuttur. Bu durumda birçok işlemin aynı anda yapılabilmesi ve değerlendirilmesi olanağı sunmaktadır.

Fiziksel sistemin durumu, $|\psi\rangle$ durum vektörü ile temsil edilir. Bu vektör kompleks Hilbert uzayına aittir ve süperpozisyon ilkesi sağlanır. Yani, $(|\phi_1\rangle, |\phi_2\rangle, \ldots, |\phi_n\rangle)$, Hilbert uzayında tanımlı ketler olmak üzere bu ketlerin lineer kombinasyonları yani süperpozisyonları da Hilbert uzayında tanımlı ve geçerli bir durumu temsil eder.

$$|\psi\rangle = \alpha_1|\phi\rangle_1 + \alpha_2|\phi\rangle_2 + \cdots + \alpha_n|\phi\rangle_n$$

olmak üzere, $\alpha_i \in \mathbb{C}$ dır. Durumların normalize oluşundan dolayı

$$\langle\psi|\psi\rangle = |\alpha_1|^2 + |\alpha_2|^2 + \cdots + |\alpha_n|^2 = 1$$

dir. Durum uzayı 2-boyutlu ortonormal $\{|0\rangle, |1\rangle\}$ bazlarından oluşur. Bu uzaya ait olan keyfi bir $|\psi\rangle$ durumu

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$$

olarak yazılır. Burada α ve β birer kompleks sayı olup, kuantum mekaniği yasalarına göre,

$|\alpha|^2, |\psi\rangle$ durumunun $|0\rangle$ durumunda bulunma olasılığını,

$|\beta|^2, |\psi\rangle$ durumunun $|1\rangle$ durumunda bulunma olasılığını

vermektedir. Bu nedenle $|\alpha|^2 + |\beta|^2 = 1$ olmalıdır (Nielsen ve Chuang, 2010).

3.2.2. Dolaşıklık

Atom ve atom altı parçacıkların dünyasında gerçekleşen önemli bir diğer üstünlük ise dolaşıklıktır. Bazı özellikleri daha önceden birbiriyle ilişkili 2 veya daha fazla parçacığın, aralarındaki mesafe ne kadar uzak olursa olsun varolan özelliklerinin birbiriyle ilişkili kalması durumuna dolaşıklık denir. Dolaşıklık sayesinde bu parçacıklardan her hangi birinde yapılan incelemeyle, aradaki mesafeye bakılmaksızın diğer parçacıklar hakkında da bilgi sahibi olunur. Ayrıca, parçacıklardan her hangi birine yapılan herhangi bir

müdahale ya da değişiklik durumunda diğer parçacıklar da etkilenecektir (Gisin, 2014).

Hilbert uzayında tanımlanan bir kuantum sisteminin dolaşık olabilmesi için bu uzayın bir çarpım uzayı şeklinde yazılamıyor olması gerekmektedir. Örneğin, Hilbert uzayındaki bir $|\psi\rangle$ durumunu ele alalım. $\mathscr{H} = \mathscr{H}_A \otimes \mathscr{H}_B$ olmak üzere, $|a\rangle \in \mathscr{H}_A$ ve $|b\rangle \in \mathscr{H}_B$ olacak biçimde $|\psi\rangle$ durumu $|a\rangle$ ve $|b\rangle$ durumlarının çarpımı biçiminde yazılamıyorsa dolaşıktır anlamına gelir (Şahin, 2019).

Dolaşık olmayan bir kuantum durumunu dolaşık hale getirmek için sırasıyla Hadamard ve CNOT kapıları uygulanır.

$$H|0\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}} \qquad H|1\rangle = \frac{|0\rangle - |1\rangle}{\sqrt{2}}$$

olmak üzere, iki kübitli dolaşık durumlar Bell durumları olarak adlandırılır. 2-boyutta Bell durumlarının genel hali ise aşağıdaki gibidir.

$$\left.\begin{aligned} CNOT\,(H|00\rangle) &= \frac{|00\rangle + |11\rangle}{\sqrt{2}} = |B_{00}\rangle \\ CNOT\,(H|01\rangle) &= \frac{|01\rangle + |10\rangle}{\sqrt{2}} = |B_{01}\rangle \\ CNOT\,(H|10\rangle) &= \frac{|00\rangle - |11\rangle}{\sqrt{2}} = |B_{10}\rangle \\ CNOT\,(H|11\rangle) &= \frac{|01\rangle - |10\rangle}{\sqrt{2}} = |B_{11}\rangle \end{aligned}\right\} \text{Bell Durumları}$$

$$\left|B_{xy}\right\rangle = \frac{|0y\rangle + (-1)^x|1\bar{y}\rangle}{\sqrt{2}}$$

şeklindedir. $d-$ boyutlu(yüksek boyutlu) genelleştirilmiş Bell durumları ise aşağıdaki gibi ifade edilir.

$$\left|\psi_{xy}^{d}\right\rangle = \frac{1}{\sqrt{d}} \sum_{j} w^{jx} |j\rangle \otimes |j + y \mod d\rangle$$

Burada, $w = e^{\frac{2\pi i}{d}}$, $j,x,y = 0,\ldots(d-1)$ ve "$+$" sembolü de $d-$ modülünde toplama işlemini belirtir (Zhao-Xu ve Tian-Yu, 2017).

Dolaşıklık iki kübit için gerçekleştirilebildiği gibi en az üç alt sistemi içeren durumlar için de gerçekleştirilebilir. Bu durumlar Greenberger-Horne-Zeilinger durumu

(GHZ durumu) olarak adalandırılır.

GHZ durumlarının en basiti, çok parçalı dolaşıklık sergileyen üç kübit GHZ durumudur ve aşağıdaki gibi tanımlıdır (Greenberger vd., 1989).

$$GHZ = \frac{|000\rangle + |111\rangle}{\sqrt{2}}$$

GHZ durumlarının 2-boyutta n-kübite genellenmiş durumu;

$$GHZ = \frac{|0\rangle^{\otimes n} + |1\rangle^{\otimes n}}{\sqrt{2}}$$

iken, GHZ durumlarının d-boyutta n kübit için genelleştirilmiş durumu aşağıdaki gibidir.

$$|GHZ(x_1,\ldots,x_n)\rangle = \frac{1}{\sqrt{d}} \sum_{j=0}^{d-1} \omega^{jx_1} |j, j+x_2, \ldots, j+x_n\rangle$$

burada $\omega = e^{\frac{2\pi i}{d}}$, $x_1,\ldots,x_n \in \{0,\ldots(d-1)\}$ ve "$+$" sembolü de $d-$ modülünde toplama işlemini belirtir (Bai vd., 2017).

3.2.3. Dolaşıklık Transferi

Dolaşıklık transferi(dolaşıklık takası) geçmişte hiç etkileşime girmemiş kuantum sistemlerinin dolaşık hale gelebildiği bir protokoldür (Nielsen ve Chuang, 2010).

Örneğin,

Alice ve Bob

$$|B_{0_A 0_B}\rangle = \frac{|0_A\rangle|0_B\rangle + |1_A\rangle|1_B\rangle}{\sqrt{2}}$$

durumu ile dolaşık olsun.

Bob ile Charlie de

$$\left|B_{0_B 0_C}\right\rangle = \frac{|0_B\rangle|0_C\rangle + |1_B\rangle|1_C\rangle}{\sqrt{2}}$$

durumu ile dolaşık olsun.

Bob, Bell durumunda ölçüm yaparak Alice ile olan dolaşıklığını Charlie'ye aktarıp dolaşıklık transferini gerçekleştirmiş olur. Bu durumda Alice ile Charlie arasında

$$\left|B_{0_A 0_C}\right\rangle = \frac{|0_A\rangle|0_C\rangle + |1_A\rangle|1_C\rangle}{\sqrt{2}}$$

dolaşık durumu meydana gelir.

3.2.4. Teleportasyon

Bilinmeyen bir kuantum durumunun bir noktadan başka bir noktaya taşınmasıdır. Taşımak istediğimiz kuantum durumu;

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$$

olsun (Gisin, 2014). Burada α ve β değerleri birer kompleks sayıdır.

Alice ve Bob ararsında gerçekleşecek bir teleportasyon örneği verelim. Alice kendinde bulunan $|\psi\rangle$ kuantum durumunu Bob'a göndermek istesin. Bunun için sırasıyla aşağıdaki adımlar izlenir.

Adım 1: Alice ve Bob dolaşık parçacık çiftini paylaşır.

$$|B_{00}\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}} = \frac{|0_A\rangle|0_B\rangle + |1_A\rangle|1_B\rangle}{\sqrt{2}}$$

Adım 2: Alice elindeki $|\psi\rangle$ kuantum durumu ile dolaşık β_{00} durumunun tensörel çarpımına CNOT kapısını uygular ve $|\chi\prime\rangle$ durumunu elde eder.

$$\begin{aligned} |\chi\rangle &= |\psi\rangle \otimes |\beta_{00}\rangle = (\alpha|0\rangle + \beta|1\rangle) \otimes \left(\frac{|00\rangle + |11\rangle}{\sqrt{2}}\right) \\ CNOT|\chi\rangle &= |\chi\prime\rangle = \frac{\alpha\left(|000\rangle + |011\rangle\right) + \beta\left(|110\rangle + |101\rangle\right)}{\sqrt{2}} \end{aligned}$$

Adım 3: Alice $|\chi\prime\rangle$ durumuna Hadamard kapısını uygular.

$$(H\otimes I\otimes I)|\chi\prime\rangle = \frac{1}{2}\Big[|0_A0_A\rangle(\alpha|0_B\rangle+\beta|1_B\rangle)+|0_A1_A\rangle(\alpha|1_B\rangle+\beta|0_B\rangle) \\ +|1_A0_A\rangle(\alpha|0_B\rangle-\beta|1_B\rangle)+|1_A1_A\rangle(\alpha|1_B\rangle-\beta|0_B\rangle)\Big]$$

Adım 4: Alice kendisine ait olan kübit çiftini ölçer.

Alice	**Bob daki bitlerin durumu**	**Uygulanacak Kapı**
00	$\alpha\|0\rangle+\beta\|1\rangle$	I
01	$\alpha\|1\rangle+\beta\|0\rangle$	X
10	$\alpha\|0\rangle-\beta\|1\rangle$	Z
11	$\alpha\|1\rangle-\beta\|0\rangle$	$Y=ZX$

Alice kendi ölçüm değerini Bob'a söylemelidir. Böylece Bob yapması gerekli olan işlemi bilir.

3.2.5. Süperyoğun Kodlama

Süperyoğun kodlamada, iki bitlik klasik bilginin bir kuantum kübit(dolaşık) yardımıyla bir yerden başka bir yere anlık olarak gönderilmesi olarak tanımlanır. Süperyoğun kodlama algoritması aşağıdaki şekilde gerçekleştirilir (Nielsen ve Chuang, 2010).

Alice Bob'a iki klasik bit($\{00,01,10,11\}$) veri göndermek istiyor. Bu işlemi tek bir kübit ile gerçekleştirebilir. Alice ve Bob bir dolaşık parçacık çiftini paylaşsınlar. Bu dolaşık parçacık çiftleri yani Bell durumları şu şekilde tanımlıdır.

$$|B_{00}\rangle = \frac{|00\rangle+|11\rangle}{\sqrt{2}} \qquad |B_{01}\rangle = \frac{|01\rangle+|10\rangle}{\sqrt{2}}$$

$$|B_{10}\rangle = \frac{|00\rangle-|11\rangle}{\sqrt{2}} \qquad |B_{11}\rangle = \frac{|01\rangle-|10\rangle}{\sqrt{2}}$$

Her Bell durumu bir klasik bit çiftini ifade etsin.

$$00 = |B_{00}\rangle \qquad 01 = |B_{01}\rangle \qquad 10 = |B_{10}\rangle \qquad 11 = |B_1\rangle$$

Alice ve Bob aşağıdaki Bell durumunu paylaşsınlar.

$$|B_{00}\rangle = \frac{|0_A 0_B\rangle + |1_A 1_B\rangle}{\sqrt{2}}$$

Alice Bob'a (00) verisi gönderecekse, $|B_{00}\rangle$ durumunu direkt gönderir.

Gönderilecek	**Duruma Uygulanan**	**Bob'a giden**
00	$I\|B_{00}\rangle$	$\|B_{00}\rangle$
01	$(X \otimes I)\|B_{00}\rangle$	$\|B_{01}\rangle$
10	$(Z \otimes I)\|B_{00}\rangle$	$\|B_{10}\rangle$
11	$(iY \otimes I)\|B_{00}\rangle$	$\|B_{11}\rangle$

Bob Alice'den gelen kübiti ölçerek bulduğu duruma göre Alice'in gönderdiği veriyi anlar.

3.2.6. No-Cloning

Bir kuantum sistemin ölçüme maruz kaldığı durumda sistemin tüm olası durumlardan tek bir duruma çöktüğünü biliyoruz. Bu nedenle kuantum teknolojilerde bir veri akışında üçüncü bir kişinin araya girip bu akıştaki verileri almaya kalkması demek bu sistemde ölçüm yapması anlamına gelir. Sistemin dışındaki üçüncü bir kişinin ölçüm yapması sonucunda da kuantum sistemin değişikliğe uğraması ve tek duruma çökmesi aşikardır. Bu nedenle kuantum verinin üçüncü kişiler tarafından tamamının alınması mümkün olmayacaktır. Bu da bilginin kopyalanamaması yani no-cloning teorem olarak adlandırılır (Nielsen ve Chuang, 2010).

3.2.7. Terslenebilirlik

Kuantum mekaniğinin birimselliği, işlem görmüş herhangi bir kuantum durumunu(ölçüm yapılmadığı yani çökme olamadığı taktirde) başlangıç durumuna dönüştürmemize olanak sağlamaktadır. Bu durum terslenebilirlik olarak adlandırılır. Kuantum mekaniği yasaları nedeniyle kuantum kapıları tersine çevrilebilir olmalıdır.

Kuantum mekaniği, bir kuantum sisteminin durumunun yalnızca tersine çevrilebilir bir dönüşüm olan birimsel bir dönüşümle değiştirilebileceğini belirtir. Başka bir deyişle, bir kuantum kapısı tersine çevrilebilir olmalıdır çünkü aksi takdirde sistemin toplam kuantum durumunu koruyamaz. Ek olarak, tersine çevrilemeyen kuantum kapıları, kuantum hesaplamasında hesaplamanın doğruluğunu tehlikeye atacak tutarsızlıklar ve hatalar yaratabilir (Nielsen ve Chuang, 2010)

3.3. Kuantum Bilgisayarlarda Temel Kapılar

Klasik bilgisayarlarda olduğu gibi kuantum bilgisayarlarda da, kuantum bilgisini taşımak ve işlemek için temel mantık kapıları kullanılır. Bu kapılar aşağıdaki gibi tanımlıdır.

3.3.1. Birim Kapı

Kimlik operatörü olarak da adlandırılan birim kapının matris gösterimi ve bir kübit üzerindeki etkileri aşağıdaki gibidir (Acar, 2021; Nielsen ve Chuang, 2010).

$$I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = |0\rangle\langle 0| + |1\rangle\langle 1|$$

$$I|0\rangle = |0\rangle \qquad I|1\rangle = |1\rangle$$

3.3.2. Pauli-X(NOT) Kapısı

X kapısının matris gösterimi aşağıdaki gibidir.

$$\sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = |0\rangle\langle 1| + |1\rangle\langle 0|$$

X kapısı, durumların genliklerini değiştirir. X kapısının bir kübit üzerindeki etkisini görmek için, kübitin durum vektörünü X kapısı ile çarpmamız yeterlidir (Acar, 2021; Nielsen ve Chuang, 2010).

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

3.3.3. Pauli-Y(Döndürme) Kapısı

Y kapısının matris gösterimi aşağıdaki gibidir.

$$\sigma_y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} = -i|0\rangle\langle 1| + i|1\rangle\langle 0|$$

Y kapısı, kuantum durumları $y-$ekseni etrafında π radyan kadar döndüren kapıdır. Bu kapı,

$$Y|0\rangle = i|1\rangle$$

$$Y|1\rangle = i|0\rangle$$

dönüşümlerini sağlar (Acar, 2021; Nielsen ve Chuang, 2010).

3.3.4. Pauli-Z(Faz) Kapısı

Faz kapısı olarak da adlandırılan Z kapısının matris gösterimi aşağıdaki gibidir.

$$\sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} = |0\rangle\langle 0| - |1\rangle\langle 1|$$

Z kapısı ise kuantum durumları $z-$ekseni etrafında π radyan kadar döndüren kapıdır. Bu kapı,

$$Z|0\rangle = |0\rangle$$

$$Z|1\rangle = -|1\rangle$$

dönüşümlerini sağlar (Acar, 2021; Nielsen ve Chuang, 2010).

3.3.5. Genel Faz Kapısı

Genel faz kapısının matris gösterimi,

$$P(\theta) = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\theta} \end{pmatrix} = |0\rangle\langle 0| + e^{i\theta}|1\rangle\langle 1|$$

olup, $e^{i\theta} = \cos\theta + i\sin\theta$ dır. Burada,

- $\theta = \pi$ ise $P(\theta)$, Z kapısını,
- $\theta = \frac{\pi}{2}$ ise $P(\theta)$, S kapısını,
- $\theta = \frac{\pi}{4}$ ise $P(\theta)$, T kapısını,

temsil eder (Acar, 2021; Nielsen ve Chuang, 2010).

3.3.6. Hadamard Kapısı

Kuantum bilgi sistemini $\{|0\rangle, |1\rangle\}$ bazlarında süperpozisyon durumuna getirmek için Hadamard kapısı kullanılır. Hadamard kapısının matris gösterimi aşağıdaki gibidir.

$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} = \frac{1}{\sqrt{2}} (|0\rangle\langle 0| + |0\rangle\langle 1| + |1\rangle\langle 0| - |1\rangle\langle 1|)$$

olmak üzere, bu kapının $|0\rangle$ ve $|1\rangle$ bazlarına etkisi,

$$H|0\rangle = \frac{1}{\sqrt{2}} (|0\rangle + |1\rangle)$$

$$H|1\rangle = \frac{1}{\sqrt{2}} (|0\rangle - |1\rangle)$$

biçimindedir (Acar, 2021; Nielsen ve Chuang, 2010).

Genelleştirilmiş Hadamard kapısı ise aşağıdaki gibidir (Acar vd., 2022).

$$H_N = \frac{1}{\sqrt{N}} \sum_{j,l=0}^{N-1} w^{jl} |j\rangle\langle l| \tag{3.1}$$

3.3.7. Kontrollü NOT Kapısı(CNOT)

Bell durumlarını dolaşık hale getirmek ve çözmek için kullanılan ve iki kübite etki eden bir kapıdır. Bu kapıda birinci kübit kontrol kübiti, ikinci kübit ise hedef kübiti olarak adlandırılmaktadır. Bu kapıda kontrol kübiti 0 ise, hedef kübiti aynı kalır yani hedef kübitine etki etmez. Ancak kontrol kübiti 1 ise hedef kübitinin değilini oluşturur. CNOT kapısının

matris gösterimi

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

şeklindedir. Bu kapının $|00\rangle, |01\rangle, |10\rangle, |11\rangle$ durumlarına etkisi,

$$CNOT|00\rangle = |00\rangle$$

$$CNOT|01\rangle = |01\rangle$$

$$CNOT|10\rangle = |11\rangle$$

$$CNOT|11\rangle = |10\rangle$$

şeklindedir (Acar, 2021; Nielsen ve Chuang, 2010).

3.3.8. Döndürme Kapıları

Bloch küresi üzerinde bir kuantum durumunu x, y ve z eksenleri etrafında θ açısı kadar döndürmeyi sağlayan kapılardır. Döndürme kapılarının matris gösterimi aşağıdaki şekildedir (Acar, 2021; Nielsen ve Chuang, 2010).

$$R_x(\theta) = \begin{pmatrix} \cos\frac{\theta}{2} & -i\sin\frac{\theta}{2} \\ -i\sin\frac{\theta}{2} & \cos\frac{\theta}{2} \end{pmatrix}$$

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

$$R_z(\theta) = \begin{pmatrix} e^{-i\frac{\theta}{2}} & 0 \\ 0 & e^{i\frac{\theta}{2}} \end{pmatrix}$$

3.3.9. Genel Kontrollü Kapı

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

matrisini aşağıdaki gibi bloklara ayıracak olursak,

$$\begin{pmatrix} \boxed{\begin{matrix} 1 & 0 \\ 0 & 1 \end{matrix}} & \boxed{\begin{matrix} 0 & 0 \\ 0 & 0 \end{matrix}} \\ \boxed{\begin{matrix} 0 & 0 \\ 0 & 0 \end{matrix}} & \boxed{\begin{matrix} 0 & 1 \\ 1 & 0 \end{matrix}} \end{pmatrix}$$

$$CNOT = \begin{pmatrix} I & 0 \\ 0 & X \end{pmatrix}$$

şeklinde tanımlayabiliriz. Bu nedenle benzer işlemi Y, Z ve Hadamard kapılarında da uygulayabiliriz. Bu durumda kontrollü Hadamard kapısının matris gösterimi aşağıdaki gibi olur.

$$CH = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ 0 & 0 & \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \end{pmatrix}$$

Kontrollü Z kapısı ise,

$$CZ = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix}$$

şeklindedir (Acar, 2021; Nielsen ve Chuang, 2010).

3.3.10. Yer Değiştirme(SWAP) Kapısı

İki kübite uygulanan ve uygulama sonucunda kübitlerin yer değiştirmesini sağlayan bir kapıdır. Matris gösterimi,

$$SWAP = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

şeklindedir. Bu kapının matematiksel gösterimi aşağıdaki gibidir (Acar, 2021; Nielsen ve Chuang, 2010).

$$SWAP|xy\rangle = |yx\rangle$$

3.3.11. Toffoli(CCNOT) Kapısı

Toffoli kapısı(CCNOT kapısı) üç kübite etki eden bir tersinir mantık kapısıdır. Kontrollü CNOT kapısı olarak da bilinir. İlk iki kübite bakılarak üçüncü kübit hakkında karar verilir. Toffoli kapısının matris gösterimi

$$Toffoli = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix}$$

şeklindedir (Acar, 2021; Nielsen ve Chuang, 2010).

DÖRDÜNCÜ BÖLÜM
ARAŞTIRMA BULGULARI VE TARTIŞMA

4.1. Ön Hazırlık

Kuantum bilgi işlemede kullanılan, ölçüm dışındaki tüm işlemler birimsel(üniter) dönüşümlerle gerçekleştirilir. Birimsel dönüşüm matematiksel olarak aşağıdaki gibi ifade edilir.

$$(U^*)^t = U^{-1} \Rightarrow U \text{ is unitary.} \tag{4.1}$$

Kuantumdaki $n-$parçacıklı kuantum durumu aşağıdaki gibi tanımlanır (Zhao-Xu ve Tian-Yu, 2017).

$$|\psi(x_1,\ldots,x_n)\rangle = \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} w^{jx_1} |j, j+x_2, \ldots, j+x_n\rangle \tag{4.2}$$

$x_1,\ldots,x_n$ değerleri 0 ile $N-1$ arasında değişir ve $w = e^{\frac{2\pi i}{N}}$ dir. (4.2) denklemiyle verilen kuantum durumları tam ve ortonormaldir.

(4.1) denklemindeki U birimsel dönüşümü, Hadamard(H), X, Y, Z dönüşümleri ise bu dönüşümler kuantum bilgisinde sırasıyla H, X, Y, Z kapıları olarak adlandırılır. Benzer şekilde, U birimsel dönüşümü kullanılarak 2-kübit ve 3-kübit kuantum kapıları elde edilebilir. Kuantumun üstün özelliklerinden biri olan süperpozisyon özelliği, kübitlere Hadamard kapısı uygulanarak elde edilir. Kübitlere Hadamard kapısı ve kontrollü NOT kapısı uygulanarak kuantumun üstün özelliklerinden biri olan dolaşıklık elde edilir. Dolaşık iki parçacık bireysel kuantum hallerini kaybederler ve ne kadar uzakta olurlarsa olsunlar tek ve birleşik bir durumu paylaşırlar.

Yüksek boyutlu dolaşık Bell durumlarının (Zhao-Xu ve Tian-Yu, 2017).

$$|\psi(x,y)\rangle = \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} w^{jx} |j\rangle \otimes |j+y \mod N\rangle \tag{4.3}$$

şeklinde olduğu, burada, x, y değerlerinin 0 ile $N-1$ arasında değiştiği ve $w = e^{\frac{2\pi i}{N}}$ olduğu biliniyor (Zhao-Xu ve Tian-Yu, 2017).

(4.3) eşitliğinde $x = y = 0$, için aşağıdaki durum elde edilir (Zhao-Xu ve Tian-Yu, 2017).

$$|\psi(0,0)\rangle = \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} |j\rangle \otimes |j\rangle \tag{4.4}$$

$\left|U_{(x,y)}\right\rangle$ dönüşümü, Bell bazlarımızı, hesaplanabilir bazlara çeviren birimsel bir dönüşümdür. Yüksek boyutlarda sıklıkla kullanılan birimsel kapılar aşağıdaki şekilde ifade edilebilir (Wang vd., 2020).

$$\left|U_{(x,y)}\right\rangle = \sum_{j=0}^{N-1} w^{xj} |j+y \mod N\rangle\langle j| \tag{4.5}$$

Herhangi bir $|\psi(x,y)\rangle$ Bell durumu, denklem (4.5) tarafından verilen $\left|U_{(x,y)}\right\rangle$'nin $|\psi(0,0)\rangle$ üzerindeki etkisiyle üretilir (Zhao-Xu ve Tian-Yu, 2017).

$$\left(I \otimes \left|U_{(x,y)}\right\rangle\right) |\psi(0,0)\rangle = |\psi(x,y)\rangle \tag{4.6}$$

Kuantumun bir başka öne çıkan özelliği, geçmişte hiç etkileşime girmemiş kuantum sistemlerini karıştırmak için kullanılan dolaşıklık transferi protokolüdür. $|\psi(x,y)\rangle_{s,s'}$ Bell durumu ve $\left|\psi_(x_1,\ldots,x_n)\right\rangle_{1,\ldots,n}$ ket durumu arasında ki dolaşıklık transferi aşağıdaki gibi formülize edilmektedir (Zhao-Xu ve Tian-Yu, 2017).

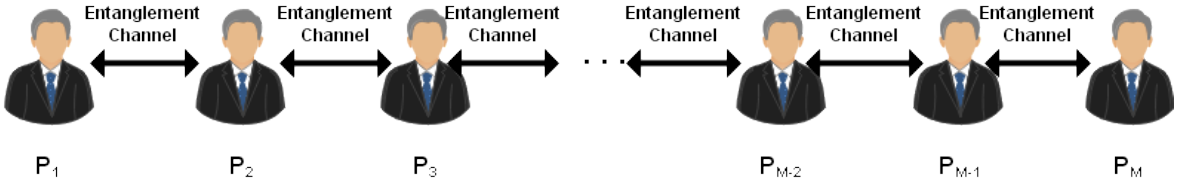
$$\begin{aligned} |\psi(x_1,\ldots,x_n)\rangle_{1,\ldots,n} \otimes |\psi(x,y)\rangle_{s,s'} = & \frac{1}{N} \sum_{k,l=0}^{N-1} w^{lk} |\psi(x_1+k, x_2, \ldots, y+l, \ldots, x_n)\rangle_{1,2,\ldots,s',\ldots,n} \\ & \otimes |\psi(x - k x_m - l)\rangle_{s,m} \end{aligned}$$

4.2. Yüksek Boyutta Önerilen Çok Katılımcılı Kuantum Dijital İmza Şeması

$P_1, \ldots, P_M$ katılımcılar olmak üzere, P_1 katılımcısı $m_i^1 = m_1^1 m_2^1 ... m_n^1$ mesajını P_M katılımcısına göndermek istesin.

Tüm katılımcılar aralarında $\left|(\psi(0,0))_{i,i+1}\right\rangle^{\otimes n}$ ($i = 1, \ldots, M-1$ olmak üzere) Bell çiftini paylaşır. Bu işlem (4.3) denklemi ile gerçekleşir. Bu durum şekil-1 de gösterilmiştir.

Genel olarak QDS protokolleri, anahtar paylaşım adımı, mesajlaşma ve doğrulama



Şekil 1. Katılımcılar ararsında dolaşıklık kanalının oluşturulması şeması

adımı gibi adımlardan oluşur. Önerilen kuantum dijital imza protokolü şu şekilde tanımlanabilir:

4.2.1. Anahtar Üretim ve Paylaşım Adımı

Anahtar paylaşım adımı aşağıdaki gibi tanımlanır.

1. P_1 katılımcısının P_M katılımcısına göndermek istediği $m_i^1 = m_1^1 m_2^1 \cdots m_n^1$ şeklindeki mesajın kuantum durumu (4.7) denkleminde verilmiştir.

$$\left|\psi_{P_1}^m\right\rangle = \otimes_{i=1}^n \left|m_i^1\right\rangle \tag{4.7}$$

Protokol güvenliğini artırmak için gönderilecek mesaj $\{|\delta_0\rangle, |\delta_1\rangle, \ldots, |\delta_{N-1}\rangle\}$ yeni bazlara dönüştürülür.

$$U = \left|U_{(x,y)}\right\rangle H_N \tag{4.8}$$

(4.8) denklemi ile verilen U birimsel operatörü, (4.7) denklemine uygulandığında P_1 katılımcısının mesajı yeni bazlarda ifade edilmiş olur . Yeni bazlarda ifade edilen mesaj aşağıda verilmiştir.

$$|\psi_{P_1}\rangle = \otimes_{i=1}^n U\left|m_i^1\right\rangle = \otimes_{i=1}^n \left|\delta_{m_i^1}\right\rangle \tag{4.9}$$

2. P_{M-1} katılımcısı, P_{M-2} katılımcısı ile olan dolaşıklık kanalını dolaşıklık takası yolu ile P_M katılımcısına aktarır. P_{M-1} katılımcısı kendi kübitlerinde Bell durum ölçümü yaparak takası gerçekleştirmiş olur ve

$$val_{M-1}^1 val_{M-1}^2 = \{00, 01, 02, \ldots, 0(N-1), \ldots, (N-1)(N-1)\} \tag{4.10}$$

değerlerinden birini elde eder. Daha sonra aşağıdaki değerleri hesaplar.

$$p_{M-1} = \otimes_{i=1}^{n}((val_{M-1}^{1})_i(val_{M-1}^{2})_i) \tag{4.11}$$

p_{M-1}, P_{M-1} katılımcısının $2n$-uzunluğundaki özel anahtarını temsil eder. Ayrıca $(val_{M-1}^{1})_i(val_{M-1}^{2})_i$ değerleri P_{M-1} katılımcısının ölçüm sonuçlarını ifade eder. Bu sonuçlar (4.10) denklemi ile verilen kümenin herhangi bir elemanıdır.

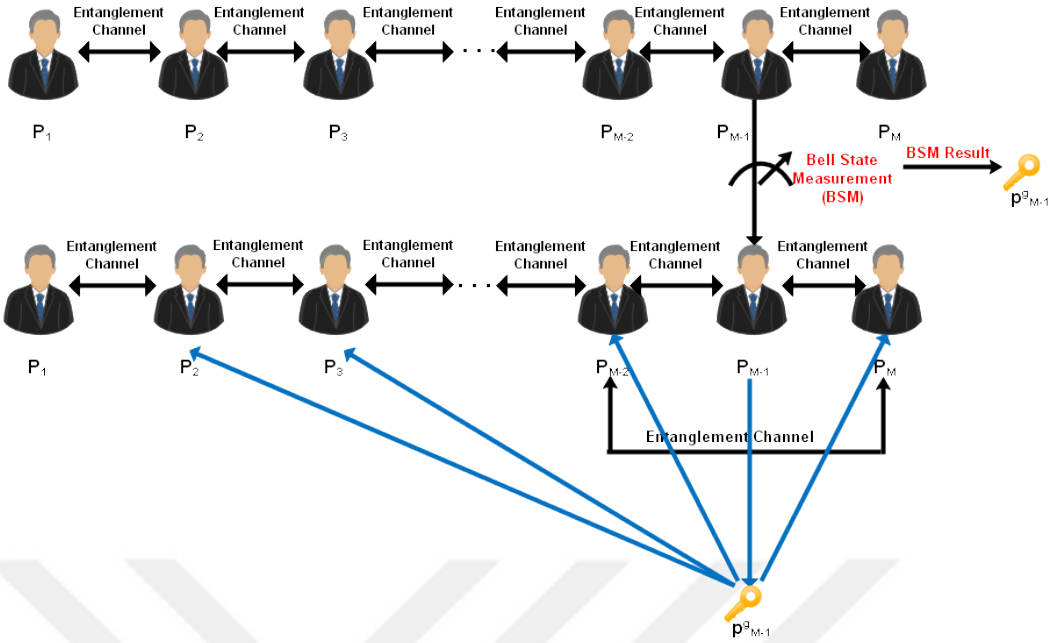
$$p_{M-1}^{g} = \otimes_{i=1}^{n}\left((val_{M-1}^{1})_i \oplus (val_{M-1}^{2})_i\right) \tag{4.12}$$

p_{M-1}^{g}, P_{M-1} katılımcısının $n-$uzunluğundaki genel anahtarını temsil eder. Burada $\oplus$ işlemi N modülünde toplama işlemini temsil eder.

P_{M-1} katılımcısı güvenli bir şekilde dolaşıklık kanalı üzerinden, süperyoğun kodlama kullanarak p_{M-1}^{g} anahtarını tüm P_i $(i = 2,\ldots,M, i \neq M-1$ olmak üzere) katılımcılarına gönderir (F. Wang vd., 2017). p^g klasik bitlere sahip olduğundan sadece klasik yolla paylaşılabilir. Ancak bu paylaşım güvenli olmayacağından dolayı anahtar paylaşımı süperyoğun kodlama ile yapılmıştır (F. Wang vd., 2017). Bu nedenle (4.13) denklemindeki p^{gg} verisi p^g verisindeki bit değerlerinin kopyalanması ile elde edilmiştir.

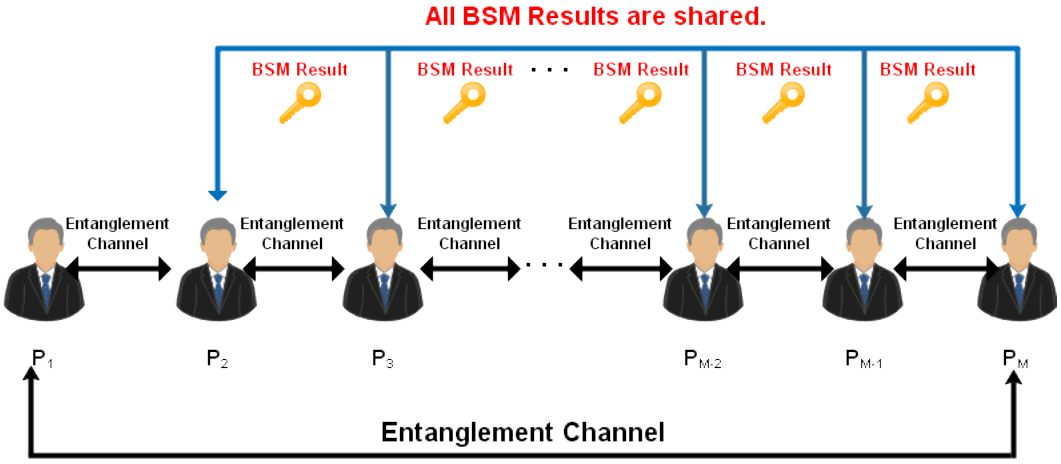
$$p_{M-1}^{gg} = \otimes_{i=1}^{n}(p_{M-1}^{g})_i(p_{M-1}^{g})_i \tag{4.13}$$

P_{M-1} katılımcısının yaptığı ölçüm sonucunda, P_{M-2} ve P_M katılımcıları arasında oluşan dolaşıklık kanalının şeması şekil-2 de verilmiştir. Şema ayrıca P_{M-1} katılımcısının genel anahtarını tüm katılımcılar ile (P_1 katılımcısı hariç) paylaşımını da göstermektedir.



Şekil 2. Birinci dolaşıklık takası ve anahtar paylaşım şeması

3. Yukarıdaki işlemlerin tümü birbiri ardına ve tüm P_j ($j = (M-2), \ldots, 2$ olmak üzere) katılımcıları için aynı şekilde yapılmalıdır. Tüm dolaşıklık takası işlemlerinden sonra gönderici P_1 katılımcısı ile alıcı P_M katılımcısı arasında bir dolaşıklık kanalı oluşmuş olur. Diğer P_j katılımcılarının tüm $val_i^1 val_i^2$ ölçüm sonuçları, kanalın oluşumunda etkilidir. Bu adım şekil 3 de görülür.



Şekil 3. Son dolaşıklık takası ve anahtar paylaşım adımı şeması

4. P_1 katılımcısı, P_M katılımcısı ile aralarında oluşan dolaşıklık kanalında, kendi kübitlerinde ölçüm yaparak

$$val_1^1 val_1^2 = \{00, 01, 02, \ldots, 0(N-1), \ldots, (N-1)(N-1)\}$$

değerlerinden herhangi birini ölçer. Daha sonra P_1 katılımcısı $val_1^1 val_1^2$ değerlerini kullanarak aşağıdaki değerleri hesaplar ve $\{p_1, p_1^g\}$ anahtar çiftini elde eder. P_1 katılımcısı p_1 anahtarını kendine özel anahtar olarak, p_1^g anahtarını ise sadece P_M katılımcısı ile paylaşacağı genel anahtar olarak saklar.

$$p_1 = \otimes_{i=1}^{n}((val_1^1)_i(val_1^2)_i) \tag{4.14}$$

$$p_1^g = \otimes_{i=1}^{n}((val_1^1)_i \oplus (val_1^2)_i) \tag{4.15}$$

Böylece, P_M katılımcısı aşağıdaki duruma sahip olur.

$$|\psi_{P_M}\rangle = \otimes_{i=1}^{n} U_{j_i k_i}^{\dagger} |\psi_{P_1}\rangle \tag{4.16}$$

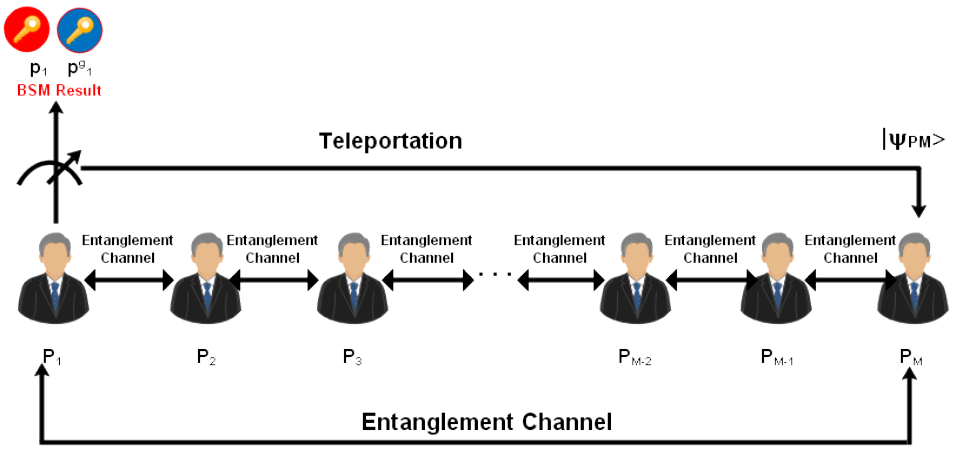
Burada, $U^{\dagger}$ matrisi, U matrisinin hermityen matrisidir, ayrıca

$$j_i = \oplus_{r=1}^{M-1}(p_r^1)_i = (val_1^1)_i \oplus \cdots \oplus (val_{M-1}^1)_i$$

ve

$$k_i = \oplus_{r=1}^{M-1}(p_r^2)_i = (val_1^2)_i \oplus \cdots \oplus (val_{M-1}^2)_i$$

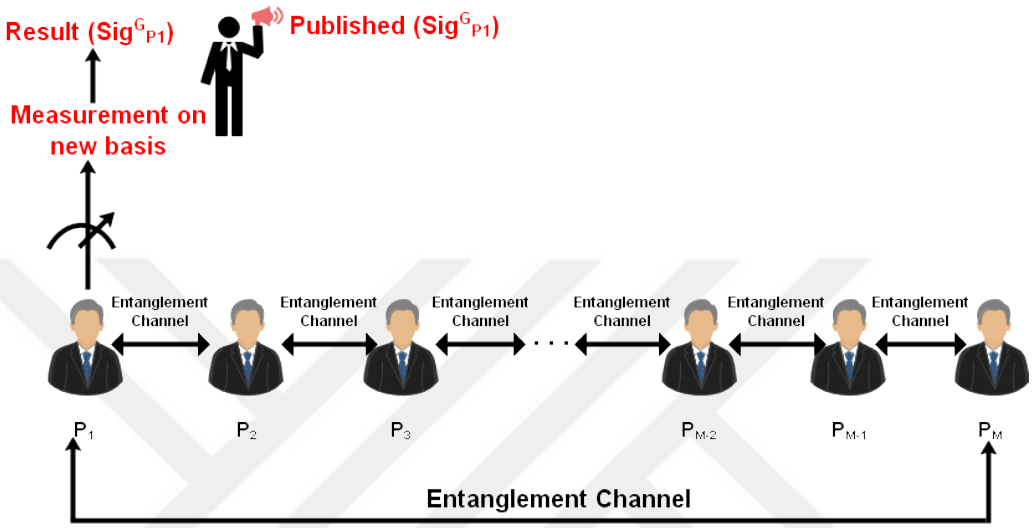
dir. Bu adım şekil-4 de gösterilmiştir.



Şekil 4. Kuantum durumun teleportasyon şeması

P_1 katılımcısı (4.17) denklemindeki gibi yeni bazlarda $\{|\delta_0\rangle, |\delta_1\rangle, \ldots, |\delta_{N-1}\rangle\}$ ölçüm yapar. Daha sonra P_1 katılımcısı, $Sig_{P_1}^{G}$ genel imzasını hesaplar ve yayınlar. Bu adımı gösteren şema şekil-5 de verilmiştir.

$$\left|\psi_{P_1}^{G}\right\rangle = \otimes_{i=1}^{n} U_{val_1^1 val_1^2}^{\dagger} \left|\delta_{m_i^1}\right\rangle \tag{4.17}$$



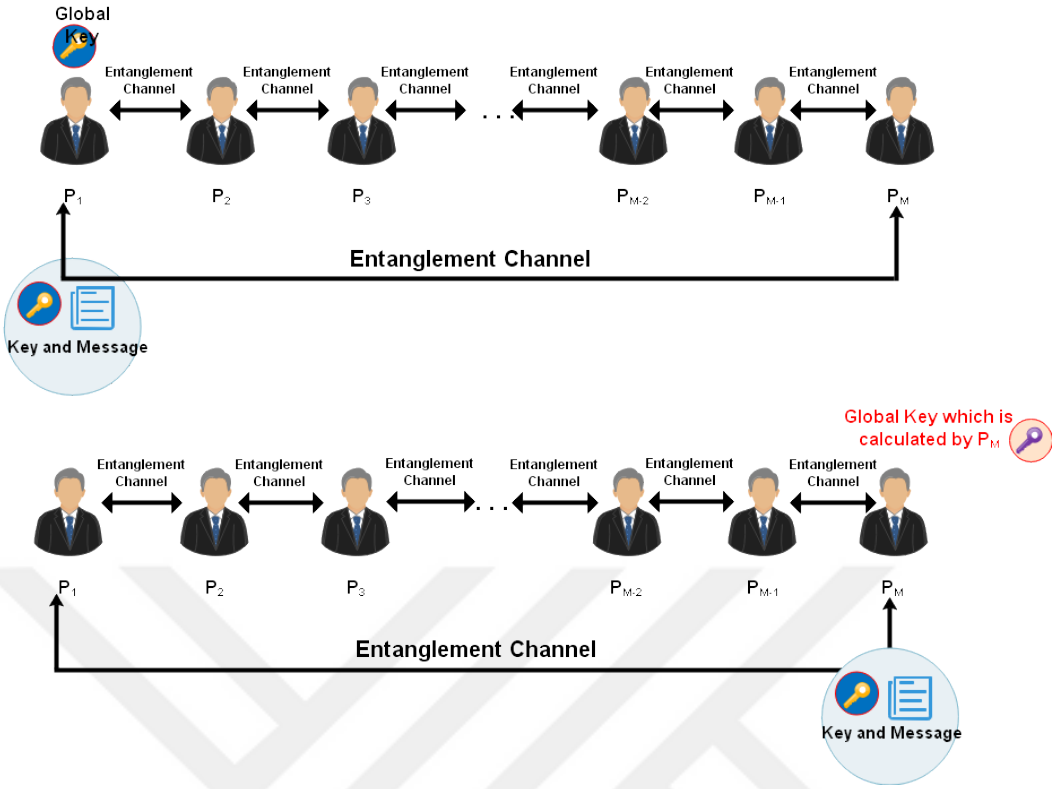
Şekil 5. P_1 katılımcısının genel imzasının oluşum ve paylaşım adımı şeması

5. P_M katılımcısı (4.16) denkleminde $\{|\delta_0\rangle, |\delta_1\rangle, \ldots, |\delta_{N-1}\rangle\}$ bazlarında ölçüm yapar ve P_1 katılımcısının imzasını $Sig_{P_M}^{P_1}$ olarak hesaplar. Burada, üst simge ve alt simge sırasıyla gerçek sahibi ve alıcıyı gösterir.

4.2.2. Mesajlaşma ve Doğrulama Adımı

1. P_1 katılımcısı m_i^1 mesajını ve kendi global anahtarı p_1^g yi $\{m_i^1, p_1^g\}$ çifti olarak P_M katılımcısına gönderir.

2. P_M katılımcısı herhangi bir reddetme olup olmadığını belirlemek için P_1 katılımcısından alınan $\{\overline{m}_i^1, \overline{p}_1^g\}$ ikliyi kontrol eder. Bu nedenle, P_M katılımcısı aşağıdaki doğrulamaları gerçekleştirir. Burada, $\{\overline{m}_i^1, \overline{p}_1^g\}$ ikilisi P_1 tarafından gönderilen $\{m_i^1, p_1^g\}$ ikilisinin sahte durumlarını ifade eder. Eğer P_1 katılımcısı güvenilir ise $\{m_i^1, p_1^g\}$ ikilisini, değil ise $\{\overline{m}_i^1, \overline{p}_1^g\}$ ikilisini gönderir. Bu adımlar Şekil - 6 de görülebilir.



Şekil 6. Çoklu katılımcı için mesajlama adımı

(a) Doğrulama Adımı-1: P_M katılımcısı (4.17) denklemini ve $\{\overline{m}_i^1, \overline{p}_1^g\}$ çiftini kullanarak $\overline{Sig}_{P_1}^G$' yi hesaplar.Daha sonra P_M katılımcısı hesapladığı $\overline{Sig}_{P_1}^G$ ile P_1 katılımcısının genel imzası olan $Sig_{P_1}^G$'in eşitliğini aşağıdaki gibi kontrol eder.

$$(\overline{Sig}_{P_1}^G)_i = (Sig_{P_1}^G)_i,\ i = 1,\ldots,n \tag{4.18}$$

(b) Doğrulama Adımı-2: P_M katılımcısı diğer katılımcılar tarafından gönderilen anahtarları kullanarak $Sig_{P_1}^G$ imzasının, hesapladığı $Sig_{P_M}^{P_1}$ imzası ile eşitliğini kontrol eder.

$$i = 1,\ldots,n \quad \begin{cases} (Sig_{P_1}^G)_i = (Sig_{P_M}^{P_1})_i, & \text{eğer } \oplus_{r=2}^{M-1} \left(p_r^g\right)_i = 0 \\ (Sig_{P_1}^G)_i \neq (Sig_{P_M}^{P_1})_i, & \text{eğer } \oplus_{r=2}^{M-1} \left(p_r^g\right)_i \neq 0 \end{cases} \tag{4.19}$$

3. P_M katılımcısı, P_1 katılımcısının gönderdiği mesajın doğru ve geçerli olduğunu kabul ettiğinde $\{\overline{m}_i^1, \overline{p}_1^g, \overline{Sig}_{P_M}^{P_1}\}$ üçlüsünü diğer P_T ($1 < T < M$ olmak üzere) katılımcılarına gönderir. P_T katılımcısı, mesajın doğru ya da sahte ve red edilmiş ya da kabul edilmiş

olduğunu belirlemek için aşağıdaki doğrulamaları gerçekleştirir.

(a) Doğrulama Adımı-3: İmza hesaplaması P_1 katılımcısının genel imzası kullanılarak gerçekleştirilir. Yani P_M katılımcısı tarafından gönderilen herhangi bir değer kullanılmaz.

i) Diğer katılımcılar P_1 katılımcısının genel imzasını kullanarak aşağıdaki durumu hazırlar.

$$\otimes_{i=1}^{n} U_{j_i k_i}^{\dagger}(|\psi_{P_1}\rangle)_i = \otimes_{i=1}^{n} U_{(p_T^1)_i (p_T^2)_i}^{\dagger} \left(\left| \psi_{P_1}^{G} \right\rangle \right)_i \tag{4.20}$$

burada

$$j_i = \oplus_{r=2, r\neq T}^{M-1} (p_r^1)_i$$

ve

$$k_i = \oplus_{r=2, r\neq T}^{M-1} (p_r^2)_i$$

şeklindedir.

ii) P_T katılımcısı $\{|\delta_0\rangle, |\delta_1\rangle, \ldots, |\delta_{N-1}\rangle\}$ bazları ile bu durumda ölçüm yapar ve $Sig_{P_T}^{P_M}$ imzasını elde eder. Daha sonra P_T katılımcısı, imzanın P_M katılımcısı tarafından gönderilen imza ile eşitliğini aşağıdaki şekilde kontrol eder.

$$i = 1, \ldots, n \quad \begin{cases} (Sig_{P_T}^{P_M})_i = (\overline{Sig}_{P_M}^{P_1})_i, & \text{if } \oplus_{r=2, r\neq T}^{M-1} (p_r^g)_i = 0 \\ (Sig_{P_T}^{P_M})_i \neq (\overline{Sig}_{P_M}^{P_1})_i, & \text{if } \oplus_{r=2, r\neq T}^{M-1} (p_r^g)_i \neq 0 \end{cases} \tag{4.21}$$

Bu sayede P_T katılımcısı, P_M katılımcısının sahtecilik yapıp yapmadığını kontrol eder.

(b) P_T katılımcısı da, P_M katılımcısı gibi Doğrulama-1 ve Doğrulama-2 adımlarını gerçekleştirir. Böylece P_T katılımcısı, P_1 katılımcısı tarafından herhangi bir reddetme olup olmadığını belirler.

4. P_M katılımcısı mesajın doğru ve geçerli olduğunu kabul ederse, P_{M-1} katılımcısına $\{\overline{m}_i^1, \overline{p}_1^g, \overline{Sig}_{P_M}^{P_1}\}$ üçlüsünü gönderebilir. P_{M-1} katılımcısı da P_T katılımcısı gibi aynı doğrulama adımlarını gerçekleştirir. Ayrıca P_{M-1} katılımcısı mesajı kabul ederse, hesaplanan $\overline{Sig}_{P_{M-1}}^{P_M}$ değerini P_{M-2} katılımcısına $\{\overline{m}_i^1, \overline{p}_1^g, \overline{Sig}_{P_{M-1}}^{P_M}\}$ üçlüsü ile birlikte gönderebilir. Bu sayede, doğrulama işlemi $P_{M-1}, \ldots, P_2$ ye kadar sıralı olarak gerçekleştirilmiş olur. Böylece her katılımcı, mesajın doğruluğunu ve geçerliliğini incelemek ve önceki katılımcı tarafından herhangi bir sahtecilik olup olmadığını tespit etmek için daha az doğrulama anahtarı kullanılmış olunacaktır.

4.3. Örnek

Önerilen kuantum dijital imza protokolünü dört katılımcı ile örnekleyelim. Burada Alice gönderici, Bob alıcı, Charlie ve David ise denetleyici katılımcılardır. Alice

$$m_i^a = m_1 m_2 \ldots m_n$$

mesajını Bob'a göndermek ister. Burada Alice birinci, Charlie ikinci, David üçüncü ve Bob ise dördüncü katılımcıdır.

Bunun için,

- Alice ve Charlie n Bell çifti $|\psi(0,0)_{AC}\rangle^{\otimes n}$ paylaşır.

  $$Alice \xleftrightarrow{\text{Dolaşıklık Kanalı}} Charlie$$

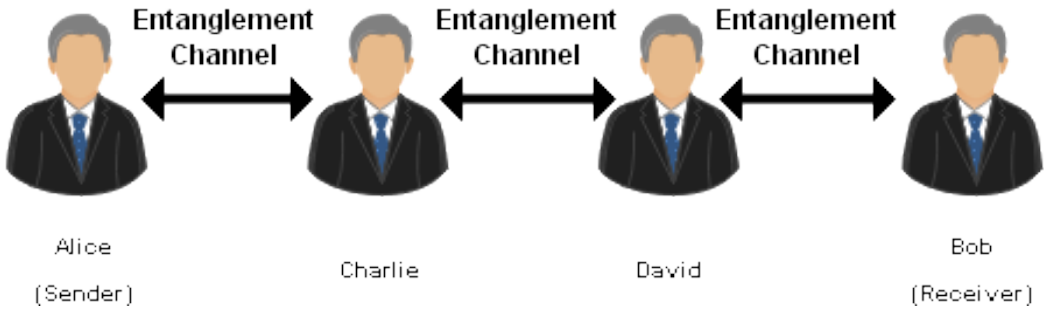
- Charlie ve David n Bell çifti $|\psi(0,0)_{CD}\rangle^{\otimes n}$ paylaşır.

  $$Charlie \xleftrightarrow{\text{Dolaşıklık Kanalı}} David$$

- David ve Bob n Bell çifti $|\psi(0,0)_{DB}\rangle^{\otimes n}$ paylaşır.

  $$David \xleftrightarrow{\text{Dolaşıklık Kanalı}} Bob$$

Bell çifti (4.3) denkleminden elde edilir. Dolaşık çiftlerin paylaşımı sonucunda katılımcılar arasında oluşan dolaşıklık kanalı şekil - 7 de verilmiştir.



Şekil 7. Katılımcılar arasında dolaşıklık kanalının oluşum şeması

4.3.1. Anahtar Üretim ve Paylaşım Adımı

1. Alice'in, Bob'a göndermek istediği

$$m_i^a = m_i^1 = m_1^1 m_2^1 \cdots m_n^1$$

mesajının kuantum durumu (4.22) denkleminde verilmiştir.

$$|\psi_{Alice}^m\rangle = \otimes_{i=1}^n |m_i\rangle \tag{4.22}$$

Daha sonra Alice (4.5) denklemini kullanarak bu kübitleri $\{|\delta_0\rangle, |\delta_1\rangle, \ldots, |\delta_{N-1}\rangle\}$ yeni bazlarına dönüştürür.

Alice'in yeni bazlardaki durumu (4.23) denkleminde görülmektedir.

$$|\psi_{Alice}\rangle = \otimes_{i=1}^n U|m_i\rangle = \otimes_{i=1}^n |\delta_{m_i}\rangle \tag{4.23}$$

2. David, Bob ile olan Bell kanalında kendi kübitlerinde Bell durum ölçümü gerçekleştirerek, Charlie ile olan dolaşıklık kanalını yer değiştirerek Bob'a aktarır. Bu sayede Charlie ile Bob arasında bir dolaşıklık kanalı oluşmuş olur. David'in Bell durum ölçümü

$$d^1 d^2 = \{00, 01, 02, \ldots, 0(N-1), \ldots, (N-1)(N-1)\}$$

kümesinin elemanlarından herhangi biridir. Daha sonra David aşağıdaki değerleri

hesaplar.

$$d = \otimes_{i=1}^{n} \left(d_i^1 d_i^2 \right) \tag{4.24}$$

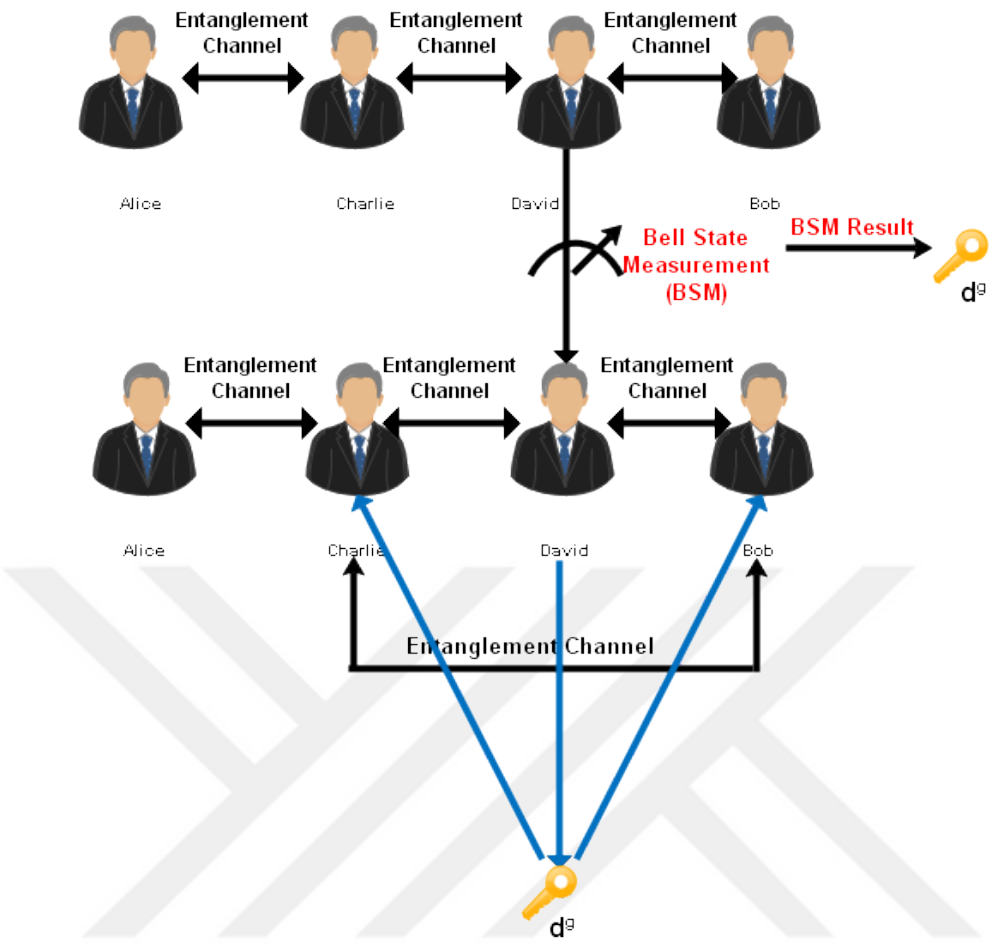
$$d^g = \otimes_{i=1}^{n} \left(d_i^1 \oplus d_i^2 \right) \tag{4.25}$$

David d^g değerini Bob ve Charlie'ye kimliği doğrulanmış klasik kanalla gönderir ve d değerini de özel anahtar olarak kendine saklar. Herhangi bir klasik verinin katılımcılara gönderiminde protokoldeki güvenliği artırmak adına süperyoğun kodlama kullanılmaktadır (F. Wang vd., 2017). Bu amaçla, tüm d^g bit değerleri aşağıdaki gibi kopyalanmıştır.

$$d^{gg} = \otimes_{i=1}^{n} (d^g)_i (d^g)_i \tag{4.26}$$

Daha sonra d^{gg} bit değerleri Bob ve Charlie'ye süperyoğun kodlama yardımı ile gönderilir. Tüm alıcılar yaptıkları Bell durum ölçümleri sonucunda d^g değerini elde eder ve saklarlar.

David'in ölçümü sonucunda Charlie ve Bob arasında oluşan dolaşıklık kanalı şekil-8 verilmiştir. Şekil aynı zamanda David'in ölçüm sonucunda elde ettiği genel anahtarın Charlie ve Bob ile paylaşımını da göstermektedir.



Şekil 8. d^g anahtarının paylaşımı ve Charlie ile Bob arasında dolaşıklık kanalı oluşum şeması

3. David gibi, Charlie de, Bob ile olan dolaşıklık kanalında kendi kübitlerinde ölçüm yaparak Alice ile olan dolaşıklık kanalını Bob'a aktarmış olur. Charlie ölçüm sonucunda

$$c^1c^2 = \{00,01,02,\ldots,0(N-1),\ldots,(N-1)(N-1)\}$$

değerlerinden herhangi birini elde eder ve daha sonra aşağıdaki değerleri hesaplar.

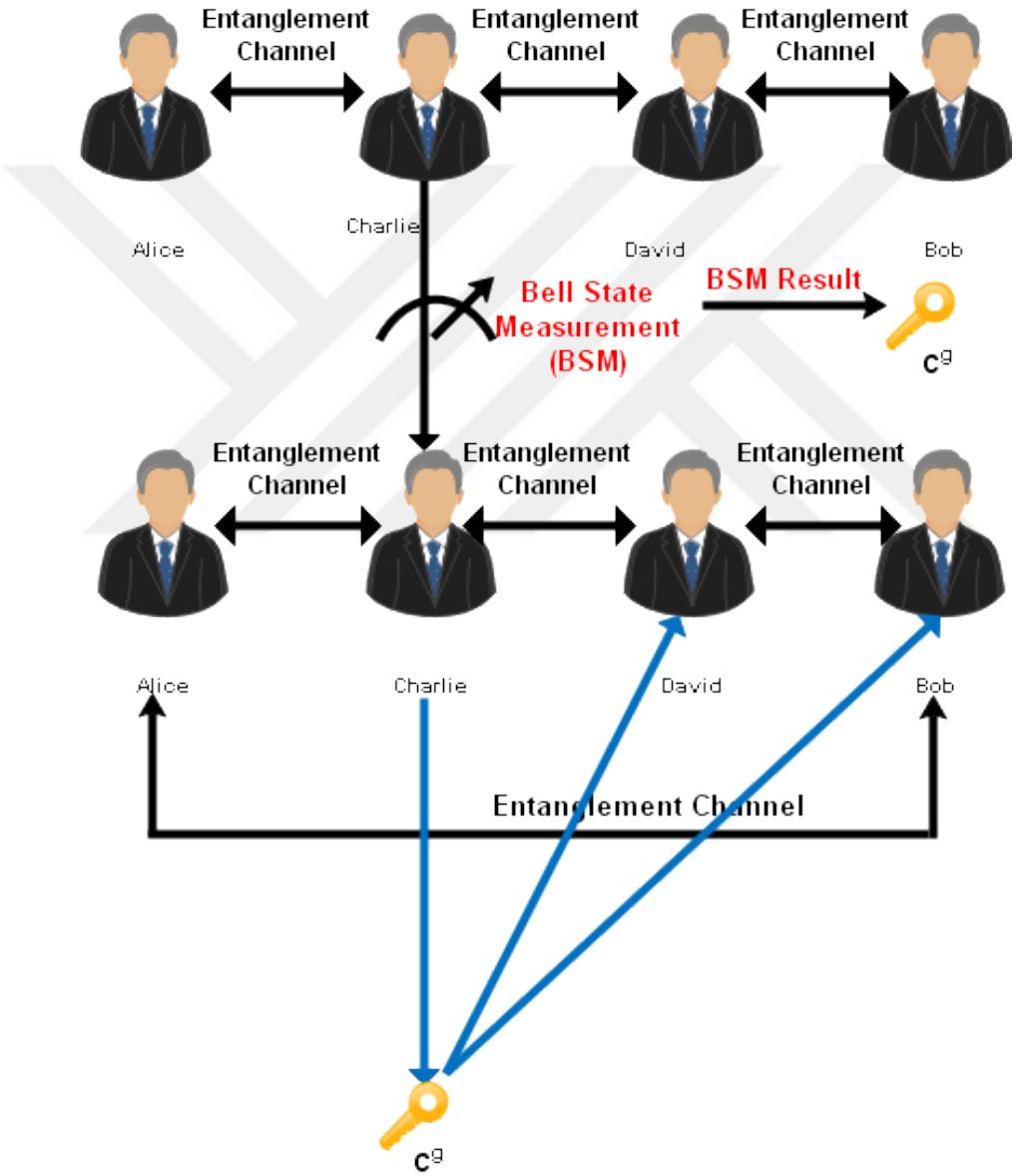
$$c = \otimes_{i=1}^{n} \left(c_i^1 c_i^2\right) \tag{4.27}$$

$$c^g = \otimes_{i=1}^{n} \left(c_i^1 \oplus c_i^2\right) \tag{4.28}$$

$$c^{gg} = \otimes_{i=1}^{n} \left((c^g)_i (c^g)_i\right) \tag{4.29}$$

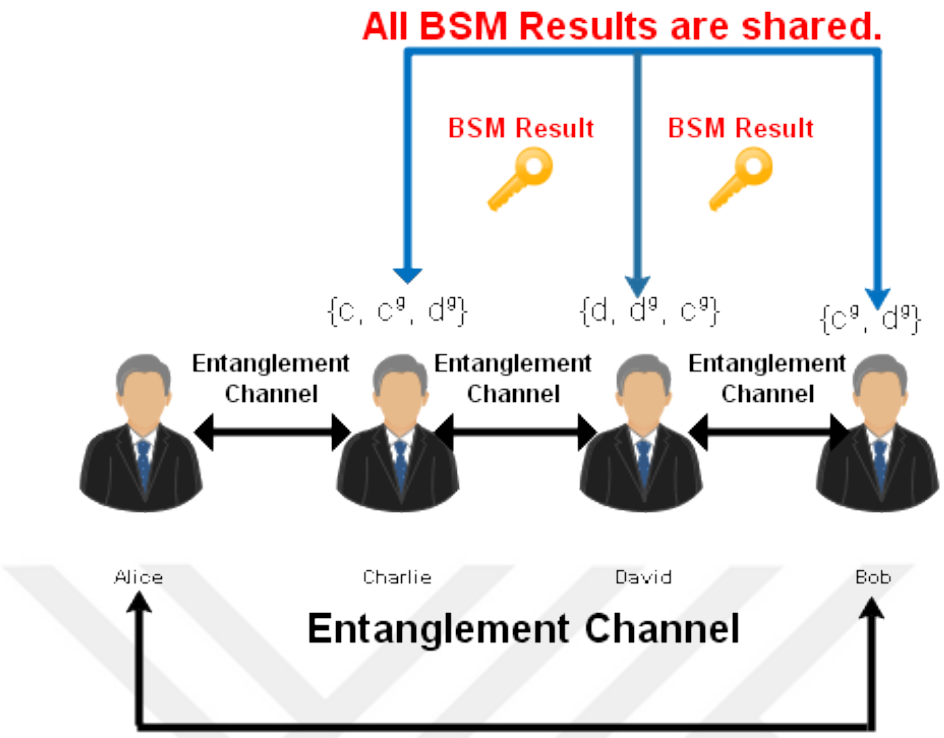
Charlie süperyoğun kodlama aracılığı ile c^{gg} değerini David ve Bob'a gönderir. Daha sonra c değerini özel anahtar olarak kendine saklar. David ve Bob yaptıkları Bell ölçümü sonucunda gerçek c^{g} değerini hesaplar ve saklarlar.

Charlie'nin ölçümü sonucunda Alice ile Bob arasında oluşan dolaşıklık kanalı şekil-9 da verilmiştir. Şekil ayrıca Charlie'nin yaptığı ölçüm sonucunda elde ettiği genel anahtarın David ve Bob ile paylaşımını da göstermektedir.



Şekil 9. c^{g} anahtarının paylaşımı ve Alice ile Bob arasında dolaşıklık kanalı oluşum şeması

Bell ölçümü sonucunda oluşan anahtarların dağılımı şekil-10 de gösterilmiştir.



Şekil 10. Anahtar paylaşım adımı şeması

4. Alice, Bob ile olan dolaşıklık kanalında kendi kübitlerinde Bell durum ölçümü gerçekleştirerek $|\psi_{Alice}\rangle$ yi Bob'a teleport eder . Alice ölçüm sonucunda

$$a^1a^2 = \{00,01,02,\ldots,0(N-1),\ldots,(N-1)(N-1)\}$$

değerlerinden birini elde eder ve aşağıdaki değerleri hesaplar.

$$a = \otimes_{i=1}^{n}\left(a_i^1 a_i^2\right) \tag{4.30}$$

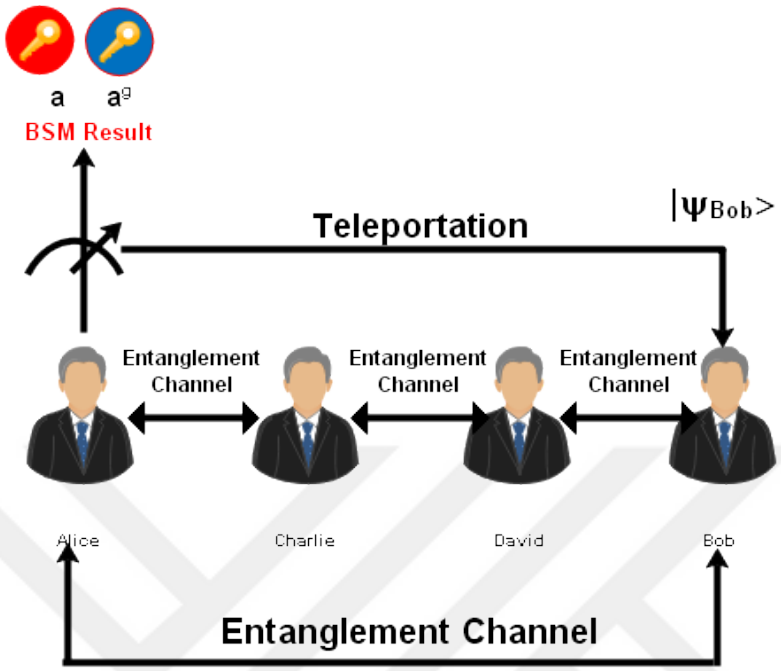
$$a^g = \otimes_{i=1}^{n}\left(a_i^1 \oplus a_i^2\right) \tag{4.31}$$

Alice, a anahtarını kendi özel anahtarı olarak ve a^g anahtarını yalnızca Bob ile paylaşacağı genel anahtar olarak saklar. Alice'in kendi kübitlerinde yaptığı Bell durum ölçümleri sonucunda Bob'da (4.32) denkleminin verdiği kuantum durumu oluşur.

$$|\psi_{Bob}\rangle = \otimes_{i=1}^{n} U_{j_i k_i}^{\dagger}(|\psi_{Alice}\rangle)_i \tag{4.32}$$

burada, $j_i = a_i^1 \oplus c_i^1 \oplus d_i^1$ ve $k_i = a_i^2 \oplus c_i^2 \oplus d_i^2$. $U_{j_i k_i}^{\dagger}$ teleportasyon takasından gelen birimsel bir dönüşümdür.

Alice'in kendi kübitinde yaptığı Bell durum ölçümü sonucu teleportasyon adımı ve anahtar oluşumu şekil-11 de verilmiştir.



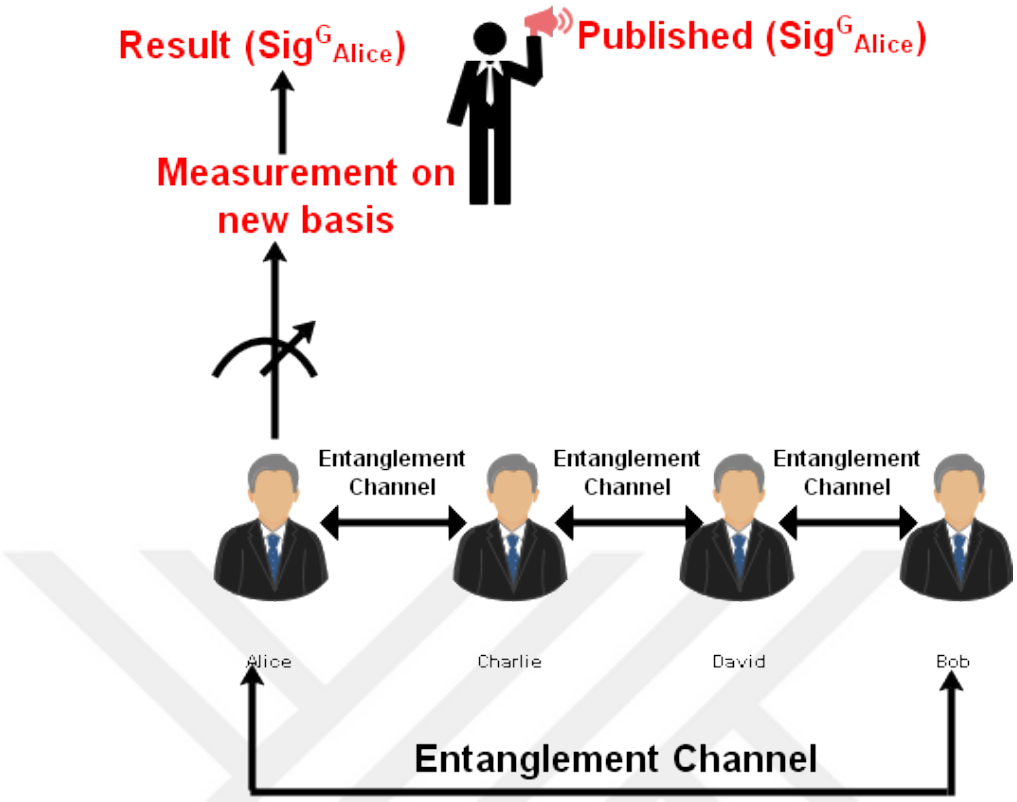
Şekil 11. Kuantum durumun teleportasyon şeması

5. Bob kendisindeki $|\psi_{Bob}\rangle$ durumunda $\{|\delta_0\rangle, |\delta_1\rangle, \ldots, |\delta_{N-1}\rangle\}$ bazlarında ölçüm gerçekleştirir. Daha sonra ölçüm sonucunu da Sig_{Bob}^{Alice} olarak saklar.

6. Alice aşağıdaki denklemi kullanarak kendi genel imzasını hesaplar.

$$\left|\psi_{Alice}^{G}\right\rangle = \otimes_{i=1}^{n} U_{a_i^1 a_i^2}^{\dagger}(|\psi_{Alice}\rangle)_i \tag{4.33}$$

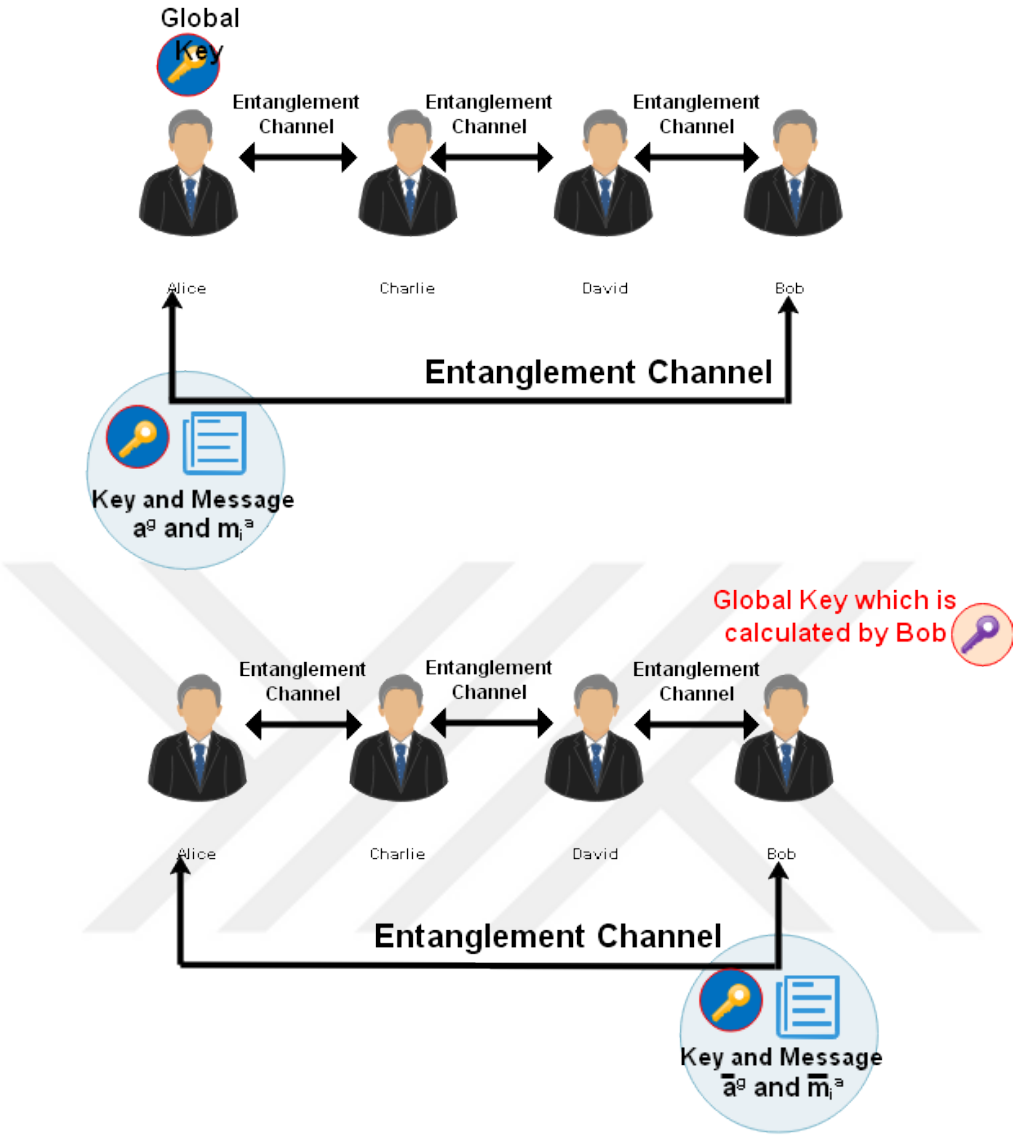
Daha sonra Alice $\{|\delta_0\rangle, |\delta_1\rangle, \ldots, |\delta_{N-1}\rangle\}$ bazlarında ölçüm yapar ve elde ettiği Sig_{Alice}^{G} sonucunu genel imzası olarak elde eder ve yayınlar. Bu adım şekil-12 de verilmiştir.



Şekil 12. Alice'in genel imzasının oluşum ve paylaşım adım şeması

4.3.2. Mesaj Gönderme ve Doğrulama Adımı

1. Notasyonda $\overline{a}$, gerçek a nın herhangi bir nedenden ya da gönderici tarafından değiştirilmiş biçimini simgelemektedir. Alice'in mesaj ve anahtarda bir sahtecilik yapmış olma ihtimalinden dolayı Bob'a göndereceği $\{m_i^a, a^g\}$ çiftini $\{\overline{m}_i^a, \overline{a}^g\}$ olarak göstereceğiz. Alice'in $\{\overline{m}_i^a, \overline{a}^g\}$ çiftini paylaşma adımı şekil-13 de verilmiştir.



Şekil 13. Dört katılımcı için mesajlaşma şeması

Bob aşağıdaki doğrulama adımlarını gerçekleştirir.

(a) Doğrulama-1: Bob $\{\overline{m}_i^a, \overline{a}^g\}$ çiftini ve (4.33) denklemini kullanarak, Alice ait $\overline{Sig}_{Alice}^G$ imzasını hesaplar ve hesapladığı $\overline{Sig}_{Alice}^G$ ile Alice tarafından yayınlanan Sig_{Alice}^G imzasının eşitliğini karşılaştırır.

$$(\overline{Sig}_{Alice}^G)_i = (Sig_{Alice}^G)_i, \qquad i = 1, \ldots, n \tag{4.34}$$

(b) Doğrulama-2: Daha sonra David ve Charlie tarafından gönderilen d^g, c^g değerlerini

kullanarak denklem (4.35) deki kontrolleri gerçekleştirir.

$$i=1,\ldots,n \quad \begin{cases} (Sig^{G}_{Alice})_i = (Sig^{Alice}_{Bob})_i, & \text{eğer } c^{g_i} \oplus d^{g_i} = 0 \\ (Sig^{G}_{Alice})_i \neq (Sig^{Alice}_{Bob})_i, & \text{eğer } c^{g_i} \oplus d^{g_i} \neq 0 \end{cases} \tag{4.35}$$

2. Bob'un Alice tarafından gönderilen değerlere dayalı olarak ilk doğrulamayı yaptığına dikkat edin. Daha sonra Bob, Alice'in genel imzası ve diğer katılımcılar tarafından gönderilen d^g, c^g değerleri ile ikinci doğrulamayı gerçekleştirilir. İkinci doğrulama, Alice'in a^1a^2 ölçüm sonuçlarına bağlı değildir. Alice, değiştirilen $\{m^a_i, a^g\}$ değerlerini Bob'a göndererek ilk doğrulamayı geçse de, ikinci doğrulama adımında başarısız olacaktır.

Eğer Bob mesajın doğruluğundan emin ise $\{\overline{m}^a_i, \overline{a}^g, \overline{\overline{Sig}^{Alice}_{Bob}}\}$ üçlüsünü David'e gönderir. Böylece mesajın aktarılabilirliği test edilecektir.

3. Doğrulama-3: David, Alice'in genel imzasını kullanarak aşağıdaki gibi $\{Sig^{Alice}_{Bob}\}$ imzasını hesaplar.

$$\otimes^{n}_{i=1}\left(U^{\dagger}_{c^1_i c^2_i}(|\psi_{Bob}\rangle)_i = U^{\dagger}_{d^1_i d^2_i}(\left|\psi^{G}_{Alice}\right\rangle)_i\right) \tag{4.36}$$

Daha sonra bu durumu $\{|\delta_0\rangle, |\delta_1\rangle, \ldots, |\delta_{N-1}\rangle\}$ bazlarında ölçer ve Sig^{Bob}_{David} değerini elde eder. Sig^{Bob}_{David} değerini kullanarak aşağıdaki eşitliği kontrol eder.

$$i=1,\ldots,n \quad \begin{cases} (\overline{\overline{Sig}^{Alice}_{Bob}})_i = (Sig^{Bob}_{David})_i, & \text{eğer } c^{g_i} = 0 \\ (\overline{\overline{Sig}^{Alice}_{Bob}})_i \neq (Sig^{Bob}_{David})_i, & \text{eğer } c^{g_i} \neq 0 \end{cases} \tag{4.37}$$

4. David, Bob'un yaptığı doğrulama adımlarını gerçekleştirir ve Alice'in reddetme yapıp yapmadığını kontrol eder. Tüm doğrulamalar doğruysa, mesajın aktarılabilir olduğuna karar verebiliriz. Daha sonra David $\{\overline{m}^a_i, \overline{a}^g, \overline{\overline{Sig}^{Alice}_{Bob}}\}$ üçlüsünü Charlie'ye gönderir.

5. Charlie doğrulama yapmak için d^g değerini kullanır.

$$\otimes^{n}_{i=1}\left(U^{\dagger}_{d^1_i d^2_i}(|\psi_{Bob}\rangle)_i = U^{\dagger}_{c^1_i c^2_i}(\left|\psi^{G}_{Alice}\right\rangle)_i\right) \tag{4.38}$$

Daha sonra (4.38) denkleminde verildiği gibi $\{|\delta_0\rangle, |\delta_1\rangle, \ldots, |\delta_{N-1}\rangle\}$ bazlarında ölçüm

yapar ve $Sig^{Bob}_{Charlie}$ değerini alır ve aşağıdaki eşitliği kontrol eder.

$$i = 1..n, \begin{cases} (\overline{Sig}^{Alice}_{Bob})_i = (Sig^{Bob}_{Charlie})_i, & \text{eğer } d^{g_i} = 0 \\ (\overline{Sig}^{Alice}_{Bob})_i \neq (Sig^{Bob}_{Charlie})_i, & \text{eğer } d^{g_i} \neq 0 \end{cases} \tag{4.39}$$

6. Protokolde istenirse David'in $\{\overline{m}^a_i, \overline{a}^g, \overline{Sig}^{Bob}_{David}\}$ üçlüsünü Charlie'e göndermesi sağlanabilir. Bu durumda Charlie David'den gelen verinin doğrulamasını aşağıdaki gibi kolayca yapabilir.

$$\otimes^n_{i=1} \left((|\psi_{Bob}\rangle)_i = U^{\dagger}_{c^1_i c^2_i} (\left| \psi^G_{Alice} \right\rangle)_i \right) \tag{4.40}$$

Charlie daha sonra (4.40) denklemindeki gibi $\{|\delta_0\rangle, |\delta_1\rangle, \ldots, |\delta_{N-1}\rangle\}$ bazlarında ölçüm yaparak $Sig^{David}_{Charlie}$ değerini elde eder ve aşağıdaki kontrolü gerçekleştirir.

$$\left((Sig^{David}_{Charlie})_i = (\overline{Sig}^{Bob}_{David})_i \right), \; i = 1, \ldots, n \tag{4.41}$$

4.4. Zaman Dolaşıklığı ile Kuantum Blok Zincir Protokolü

$B_1, B_2, \ldots, B_n$ blokları bir klasik blok zincirine ait bloklar olsun. Klasik blok zincirde bloklar zaman damgalı olacak şekilde kriptografik hash fonksiyonları aracılığıyla kronolojik sırayla birbirine bağlıdır. Bu kriptografik hash fonksiyonları her hangi bir bloğa dışarıdan gerçekleşen bir müdahale ile bu bloğu takip eden gelecekteki tüm blokların geçersiz olmasını sağlamaktadır. Bu da klasik blok zincirinin dışarıdan müdahalelere karşı son derece hassas ve kırılgan olduğunu göstermektedir. Bu nedenle Rajan ve Visser (2019) ile Gao vd. (2020) zaman dolaşıklığı kullanılan bir kuantum blok zincir protokolü önermişlerdir.

$2-$bitlik klasik kaydı olan bir bloğun belirli bir zamanda(örneğin $t = 0$) geçici bir Bell durumuna dönüştürülmesi

$$\left| B_{b_1 b_2} \right\rangle^{0,\tau} = \frac{1}{\sqrt{2}} \left(\left| 0^0 \right\rangle |b^{\tau}_2\rangle + (-1)^{b_1} \left| 1^0 \right\rangle \left| \overline{b}^{\tau}_2 \right\rangle \right) \tag{4.42}$$

eşitliği ile gerçekleşmektedir. Buradaki üst simgeler fotonun emildiği zamanı ifade etmektedir (Gao vd., 2020; Rajan ve Visser, 2019).

Uzamsal olarak dolaşık kübitler, polarize fotonlar aracılığıyla

$$|\phi\pm\rangle = \frac{1}{\sqrt{2}}\left(|H_1H_2\rangle \pm |V_1V_2\rangle\right) \tag{4.43}$$

$$|\varphi\pm\rangle = \frac{1}{\sqrt{2}}\left(|H_1V_2\rangle \pm |V_1H_2\rangle\right) \tag{4.44}$$

biçiminde ifade edilir. Burada $|H\rangle$ fotonun yatay, $|V\rangle$ ise fotonun dikey polarizasyonunu ifade eder (Rajan ve Visser, 2019). Peryodik τ zamanlı ayrılmış, ard arda uzamsal olarak dolaşık çiftler

$$|\varphi-\rangle_{1,2}^{0,0} \otimes |\varphi-\rangle_{1,2}^{\tau,\tau} = \frac{1}{2}\left[\left(\left|H_1^0V_2^0\right\rangle - \left|V_1^0H_2^0\right\rangle\right) \otimes \left(|H_1^\tau V_2^\tau\rangle - |V_1^\tau H_2^\tau\rangle\right)\right] \tag{4.45}$$

şeklinde gösterilir. Burada üst simgeler, fotonlar için zaman damgası oluşturur. Dolaşık her foton çiftlerinden birine, bir τ zaman ötelemesi(time delay) süresi eklendiğinde

$$|\varphi-\rangle_{1,2}^{0,\tau} \otimes |\varphi-\rangle_{1,2}^{\tau,2\tau} = \frac{1}{2}\left[\left(\left|H_1^0V_2^\tau\right\rangle - \left|V_1^0H_2^\tau\right\rangle\right) \otimes \left(\left|H_1^\tau V_2^{2\tau}\right\rangle - \left|V_1^\tau H_2^{2\tau}\right\rangle\right)\right] \tag{4.46}$$

eşitliği elde edilir. $t = \tau$ zamanında iki foton üzerinde Bell durum ölçümü gerçekleştirildiğinde, daha önce hiç bir arada bulunmayan $t = 0$ ve $t = 2\tau$ zamanlarında emilen fotonlar arasında dolaşıklık oluşturulmuş olur. Yani, dolaşıklık transferi gerçekleşir (Rajan ve Visser, 2019; Xing vd., 2023).

Biz de bu çalışmamızda var olan kauntum blok zincirinde bilgi kapasitesini ve güvenliği arttırmak adına bloklardaki Bell durumlarını yüksek boyuta taşıyıp uzay-zaman dolaşıklığı gerekleştireceğiz. Yüksek boyutta gerçekleştirilecek Bell durumları (dolaşıklık) ve ölçüm sırasıyla HDBS (High Dimensional Bell State) ve HDBM (High Dimensional Bell Measurement) olarak ifade edilecektir.

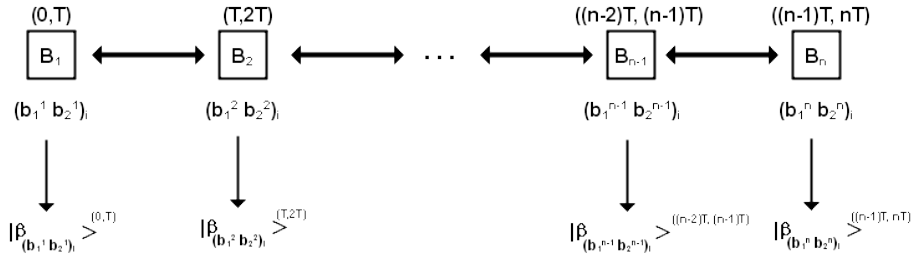
$B_1, B_2, \ldots, B_n$ blokları bir kuantum blok zincirine ait bloklar olsun. Öncelikle bu bloklar;

$$\left|HDBS_{b_1b_2}\right\rangle^{(0,t)} = \left|\beta_{b_1b_2}\right\rangle^{(0,t)} = \frac{1}{\sqrt{N}}\sum_{j=0}^{N-1} w^{jb_2}\left|j^0\right\rangle\left|(b_1+j)^t\right\rangle \tag{4.47}$$

denklemi yardımıyla belirli bir zamanda üretilen geçici bir Bell durumuna dönüştürülür.

Burada $b_1b_2 = \{00,01,02,\ldots,(N-1)(N-1)\}$ şeklinde olup, $w = e^{\frac{2\pi i}{N}}$ dir.

Bilgi kapasitesini ve güvenliği artırmak adına her bloktaki klasik b_1b_2 kaydını, $(b_1b_2)_i$ (burada $i = 1,2,\ldots,m$ olmak üzere) olacak biçimde yüksek boyuta taşıyalım. Bu durumu gösteren şema şekil-14 de verilmiştir.



Şekil 14

Önerdiğimiz kuantum blok zinciri protokolü **anahtar üretim ve paylaşım adımı** ve **mesajlaşma ve doğrulama adımı** olmak üzere iki aşamadan oluşmaktadır.

4.4.1. Anahtar Üretim ve Paylaşım Adımı

1. B_1 bloğunda bulunan

$$(data)_i^1 = data_1^1 data_2^1 data_1^3 \ldots data_m^1 \tag{4.48}$$

verisi B_n bloğuna aktarılmak istenmektedir. Bu verinin kuantum durumu

$$|d_{B_1}\rangle = \otimes_{i=1}^{m} \left|data_i^1\right\rangle = \left|data_1^1\right\rangle \left|data_2^1\right\rangle \ldots \left|data_m^1\right\rangle \tag{4.49}$$

biçimindedir. Protokol güvenliğini artırmak adına aktarılmak istenen veri yeni bazlara dönüştürülür. Bu durumda $|d_{B_1}\rangle$ verisinin $\{|\xi_0\rangle,|\xi_1\rangle,\ldots,|\xi_{N-1}\rangle\}$ yeni bazlarındaki durumu;

$$|ID_{B_1}\rangle = \otimes_{i=1}^{m} U\left(\left|data_i^1\right\rangle\right) = \otimes_{i=1}^{m} \left|\xi_{data_i^1}\right\rangle \tag{4.50}$$

biçimindedir.

2. Yukarıdaki kuantum blok zincirinde B_{n-1} bloğunda $t = (n-1)T$ zamanda iki foton üzerinde yüksek boyutlu Bell ölçümü(HDBM) yapılarak $t = (n-2)T$ ile $t = nT$

zamanlarında emilen fotonlar arasında dolaşıklık oluşturulur. Benzer biçimde sırasıyla $(n-2)T, (n-3)T, \ldots, T$ zamanda iki foton üzerinde HDBM yapılarak daha önce hiç bir arada bulunmayan $t = 0$ ve $t = nT$ zamanlarında emilen fotonlar arasında dolaşıklık oluşturularak B_1 ve B_n blokları arasında zamansal dolaşıklığa bağlı bir dolaşıklık kanalı oluşmuş olur. Ayrıca yapılan bu ölçümler sayesinde her blokta verinin üretildiği, değiştirildiği, gönderildiği, alındığı, kaydedildiği ve bu işlemlerin ne zaman gerçekleştiğine dair kayıtlılar oluşturulmuş olacaktır. Verinin ve aktarım yapan bloğa ait kimliğin doğruluğunu, ayrıca dışarıdan herhangi bir müdahale yapılıp yapılmadığını test etmek amacıyla, yapılan ölçüm sonuçlarında sistemdeki her bloğa bir genel (B_p) bir de özel (B_s) anahtarları üretilecektir.

3. B_{n-1} bloğunda yüksek boyutta yapılan Bell ölçüm sonucu

$$B^1_{n-1}B^2_{n-1} = \{00, 01, \ldots, (N-1)(N-1)\}$$

değerlerinden herhangi biridir. Bu ölçüm sonuçları kullanılarak B_{n-1} bloğuna ait

$$(B_{n-1})_s = \otimes_{i=1}^{m} \left((B^1_{n-1})_i (B^2_{n-1})_i\right)$$

özel anahtarı ve

$$(B_{n-1})_p = \otimes_{i=1}^{m} \left((B^1_{n-1})_i \oplus (B^2_{n-1})_i\right)$$

genel anahtarı üretilmiş olur. Burada $\oplus$ sembolü N modülünde toplama işlemini temsil eder.

Elde edilen bu anahtarlardan $(B_{n-1})_s$ özel anahtar olarak B_{n-1} bloğunda saklanırken, $(B_{n-1})_p$ genel anahtar olarak B_1 bloğu hariç tüm bloklara süperyoğun kodlama yardımıyla gönderilir. Bunun için de $(B_{n-1})_p$ genel anahtarı kopyalanarak

$$(B_{n-1})_{pp} = \otimes_{i=1}^{m} \left((B_{n-1})_{p_i} (B_{n-1})_{p_i}\right)$$

biçimine dönüştürülür. Genel anahtarın paylaşıldığı bloklarda yapılan yüksek boyutlu Bell ölçümü sonucunda gerçek $(B_{n-1})_p$ değeri hesaplanıp saklanır.

4. Tüm bloklarda benzer biçimde, yapılan ölçüm sonuçları kullanılarak bir özel ve bir de genel anahtar üretilmiş olur. Özel anahtarlar bloklarda saklanırken, genel anahtarlar (B_1

bloğu hariç) diğer tüm bloklarla süperyoğun kodlama yardımıyla paylaşılır.

5. B_1 bloğunda $t = T$ zamanda iki foton üzerinde yapılan HDBM sonucunda

$$B_1^1 B_1^2 = \{00, 01, \ldots, (N-1)(N-1)\}$$

değerlerinden herhangi biri elde edilir. Bu ölçüm sonuçları kullanılarak

$$(B_1)_s = \otimes_{i=1}^{m} \left((B_1^1)_i (B_1^2)_i \right)$$

özel ve

$$(B_1)_p = \otimes_{i=1}^{m} \left((B_1^1)_i \oplus (B_1^2)_i \right)$$

genel anahtarı oluşturulur. Burada $(B_1)_s$ özel anahtar olarak, $(B_1)_p$ ise sadece B_n bloğu ile paylaşılacak genel anahtar olarak B_1 bloğunda saklanır.

B_1 bloğunda yapılan ölçüm sonucunda ve B_1 bloğu ile B_n bloğu arasında oluşan dolaşıklık kanalı aracığıyla B_n bloğunda;

$$|d_{B_n}\rangle = \otimes_{i=1}^{m} U_{j_i k_i}^{\dagger} |d_{B_1}\rangle \tag{4.51}$$

(4.51) denklemiyle verilen kuantum durumu oluşur. Burada,

$$j_i = \oplus_{r=1}^{n-1} (B_r)_{p_i^1} = (B_1)_{p_i^1} \oplus (B_2)_{p_i^1} \oplus \cdots \oplus (B_{n-1})_{p_i^1}, \qquad (i = 1, 2, \ldots, m)$$

ve

$$k_i = \oplus_{r=1}^{n-1} (B_r)_{p_i^2} = (B_1)_{p_i^2} \oplus (B_2)_{p_i^2} \oplus \cdots \oplus (B_{n-1})_{p_i^2}, \qquad (i = 1, 2, \ldots, m)$$

şeklinde tanımlıdır. Ayrıca B_1 bloğu $t = T$ anında yeni bazlarda yaptığı ölçüm sonucunda zaman damgalı $ID_{B_1}^G$ genel kimliğini elde eder.

$$ID_{B_1}^G = \otimes_{i=1}^{m} U^{\dagger}_{\left((B_1)_{p_i^1}\right)\left((B_1)_{p_i^2}\right)} \left| \xi_{data_i^1} \right\rangle \tag{4.52}$$

$ID_{B_1}^G$ yi genel kimliği olarak yayınlar.

6. B_n bloğunda (4.51) denkleminde yeni bazlarda ölçüm gerçekleştirilerek B_1 bloğuna ait kimliği $D_{B_n}^{B_1}$ olarak hesaplar. Burada alt ve üst simge sırasıyla verinin aktarılacağı bloğu ve kimliğin gerçek sahibi olan bloğu ifade eder.

4.4.2. Mesajlaşma ve Doğrulama Adımı

1. B_1 bloğundan B_n bloğuna $\{data_i^1, (B_1)_p\}$ çifti teleport edilir. B_1 bloğundan teleport edilen $\{data_i^1, (B_1)_p\}$ çiftinin her hangi bir nedenden dolayı (çevresel faktörkler ya da dışarıdan müdahale) değiştiğin varsayarak $\{\overline{data}_i^1, (\overline{B_1})_p\}$ biçiminde gösterelim.

(a) Doğrulama-1: B_n bloğunda (4.52) denklemi ve $\{\overline{data}_i^1, (\overline{B_1})_p\}$ çifti kullanılarak $\overline{ID}_{B_1}^G$ değeri hesaplanır ve B_1 bloğundan yayınlanan $ID_{B_1}^G$ kimliği ile eşitliği kontrol edilir.

$$(\overline{ID}_{B_1}^G)_i = (ID_{B_1}^G)_i, \qquad (i = 1, 2, \ldots, m)$$

(b) Doğrulama-2: Bu adımda B_n bloğunda B_1 bloğu tarafından yayınlanan $ID_{B_1}^G$ ile B_n bloğunda yeni bazlarda yapılan ölçüm sonucunda elde edilen $ID_{B_n}^{B_1}$ kimliğinin eşitliği kontrol edilir.

$$i = 1, \ldots, m \quad \begin{cases} (ID_{B_1}^G)_i = (ID_{B_n}^{B_1})_i, & \text{eğer } \oplus_{r=2}^{n-1} (B_r)_{p_i} = 0 \\ (ID_{B_1}^G)_i = (ID_{B_n}^{B_1})_i, & \text{eğer } \oplus_{r=2}^{n-1} (B_r)_{p_i} \neq 0 \end{cases} \tag{4.53}$$

2. B_n bloğunda yapılan kontroller sonucunda verinin doğruluğu ile geçerliliği kabul edilirse, $\{\overline{data}_i^1, (\overline{B_1})_p, \overline{ID}_{B_n}^{B_1}\}$ üçlüsü $(1 < l < n)$ diğer B_l bloğuna aktarılır. Bu blokta ise verinin doğru ya da sahte ve reddedilmiş ya da kabul edilmiş olduğunu belirlemek için aşağıdaki doğrulama adımları gerçekleştirilir.

(a) Kimlik hesaplaması, B_1 bloğunun yayınladığı $ID_{B_1}^G$ genel kimlik ile yapılacaktır.Yani doğru karar vermek adına B_n bloğundan aktarılan her hangi bir veri kullanılmayacaktır.

i) Diğer bloklarda B_1 bloğuna ait $ID_{B_1}^G$ kullanılarak,

$$\otimes_{i=1}^{m} U_{j_i k_i}^{\dagger}(|ID_{B_1}\rangle)_i = \otimes_{i=1}^{m} U_{(B_m)_{s_i^1 s_i^2}}^{\dagger}\left(\left|ID_{B_1}^G\right\rangle\right)_i$$

burada,

$$j_i = \oplus_{r=2, r\neq l}^{n-1}(B_r)_{p_i^1}, \qquad (i = 1,2,\ldots,m)$$

ve

$$k_i = \oplus_{r=2, r\neq l}^{n-1}(B_r)_{p_i^2}, \qquad (i = 1,2,\ldots,m)$$

şeklinde tanımlıdır.

ii) B_l bloğunda yeni bazlarda yapılan ölçüm sonucunda $ID_{B_l}^{B_n}$ elde edilir. Daha sonra B_l bloğunda hesaplanan kimlik ile B_n bloğundan aktarılan kimliğin eşitliği kontrol edilir.

$$i = 1,\ldots,m \quad \begin{cases} (ID_{B_l}^{B_n})_i = (\overline{ID}_{B_l}^{B_1})_i, & \text{eğer } \oplus_{r=2, r\neq l}^{n-1}(B_r)_{p_i} = 0 \\ (ID_{B_l}^{B_n})_i = (\overline{ID}_{B_l}^{B_1})_i, & \text{eğer } \oplus_{r=2, r\neq l}^{n-1}(B_r)_{p_i} \neq 0 \end{cases} \tag{4.54}$$

Bu sayede B_l bloğunda, B_n bloğunda her hangi bir sahtecilik yapılıp yapılmadığı kontrol edilmiş olur.

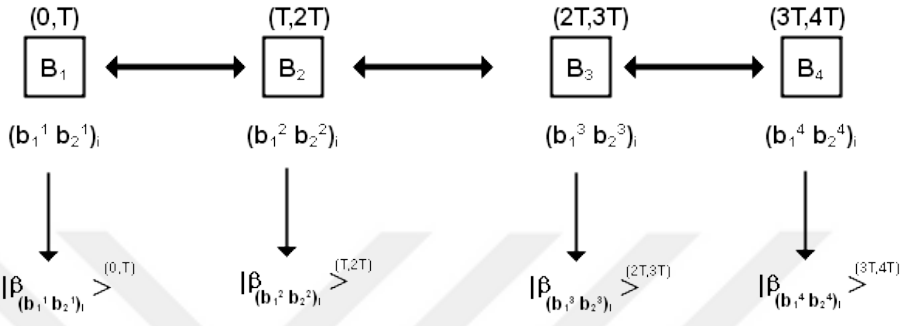
(b) B_l bloğunda B_n bloğundaki gibi Doğrulama-1 ve Doğrulama-2 adımları gerçekleştirilir ve B_1 bloğunda her hangi bir reddetme olup olmadığı belirlenir.

3. İkinci durumda B_n bloğunda verinin doğruluğu ve geçerliği kabul edilirse, $\{\overline{data}_i^1, (\overline{B_1})_p, \overline{ID}_{B_n}^{B_1}\}$ üçlüsü B_{n-1} bloğuna aktarılır. B_{n-1} bloğunda da B_l bloğunda yapıldığı gibi aynı doğrulama adımları gerçekleştirilir. Ayrıca; B_{n-1} bloğu veriyi kabul ederse daha sonra hesaplanan $\overline{ID}_{B_{n-1}}^{B_n}$ değerini B_{n-2} bloğuna $\{\overline{data}_i^1, (\overline{B_1})_p, \overline{ID}_{B_{n-1}}^{B_n}\}$ üçlüsü olarak aktarılır. Bu sayede doğrulama $B_{n-1}, B_{n-2}, \ldots, B_2$ bloklarında sıralı olarak gerçekleşmiş olur. Böylece her blok aktarılan verinin doğruluğunu ve geçerliliğini incelemek ve önceki bloklarda herhangi bir nedenden dolayı sahtecilik olup olmadığını tespit etmek için daha az doğrulama anahtarı kullanmış olacaktır.

4.5. Zaman Dolaşıklığı ile Kuantum Blok Zincir Protokolü Örneği

Bu bölümde zaman dolaşıklığı temelinde oluşturulan kuantum blok zincir protokolü, dört blok kullanılarak örneklendirilmiştir.

B_1, B_2, B_3, B_4 blokları bir klasik blok zincirine ait bloklar olsun.



Şekil 15

4.5.1. Anahtar Üretim ve Paylaşım Adımı

1. B_1 bloğunda bulunan

$$(data)_i^1 = data_1^1 data_2^1 data_1^3 \dots data_m^1 \tag{4.55}$$

verisi B_4 bloğuna aktarılmak istenmektedir. Bu verinin kuantum durumu

$$|d_{B_1}\rangle = \otimes_{i=1}^{m} \left|data_i^1\right\rangle = \left|data_1^1\right\rangle \left|data_2^1\right\rangle \dots \left|data_m^1\right\rangle \tag{4.56}$$

biçimindedir. Protokol güvenliğini artırmak adına aktarılmak istenen veri yeni bazlara dönüştürülür. Bu durumda $|d_{B_1}\rangle$ verisinin $\{|\xi_0\rangle, |\xi_1\rangle, \dots, |\xi_{N-1}\rangle\}$ yeni bazlarındaki durumu;

$$|ID_{B_1}\rangle = \otimes_{i=1}^{m} U\left(\left|data_i^1\right\rangle\right) = \otimes_{i=1}^{m} \left|\xi_{data_i^1}\right\rangle \tag{4.57}$$

biçimindedir.

2. Yukarıdaki kuantum blok zincirinde B_3 bloğunda $t = 3T$ zamanda iki foton üzerinde yüksek boyutlu Bell ölçümü (HDBM) yapılarak $t = 2T$ ile $t = 4T$ zamanlarında emilen fotonlar arasında dolaşıklık oluşturulur. Ayrıca B_3 bloğunda yüksek boyutta yapılan Bell

ölçüm sonucu,

$$B_3^1 B_3^2 = \{00, 01, \ldots, (N-1)(N-1)\}$$

değerlerinden herhangi biridir. Bu ölçüm sonuçları kullanılarak B_3 bloğuna ait

$$(B_3)_s = \otimes_{i=1}^{m} \left((B_3^1)_i (B_3^2)_i\right)$$

özel anahtarı ve

$$(B_3)_p = \otimes_{i=1}^{m} \left((B_3^1)_i \oplus (B_3^2)_i\right)$$

genel anahtarı üretilmiş olur. Burada $\oplus$ sembolü N modülünde toplama işlemini temsil eder.

Elde edilen bu anahtarlardan $(B_3)_s$ özel anahtar olarak B_3 bloğunda saklanırken, $(B_3)_p$ genel anahtar olarak B_2 ve B_4 bloklarına süperyoğun kodlama yardımıyla gönderilir. Bunun için de $(B_3)_p$ genel anahtarı kopyalanarak

$$(B_3)_{pp} = \otimes_{i=1}^{m} \left((B_3)_{p_i} (B_3)_{p_i}\right)$$

biçimine dönüştürülür. Genel anahtarın paylaşıldığı B_2 ve B_4 bloklarında yapılan yüksek boyutlu Bell ölçümü sonucunda gerçek $(B_3)_p$ değeri hesaplanıp B_2 ve B_4 bloklarında saklanır.

3. Benzer biçimde B_2 bloğunda $t = 2T$ zamanda iki foton üzerinde yüksek boyutlu Bell ölçümü (HDBM) yapılarak $t = T$ ile $t = 4T$ zamanlarında emilen fotonlar arasında dolaşıklık oluşturulur. Ayrıca B_2 bloğunda yüksek boyutta yapılan Bell ölçüm sonucu,

$$B_2^1 B_2^2 = \{00, 01, \ldots, (N-1)(N-1)\}$$

değerlerinden herhangi biridir. Bu ölçüm sonuçları kullanılarak B_2 bloğuna ait

$$(B_2)_s = \otimes_{i=1}^{m} \left((B_2^1)_i (B_2^2)_i\right)$$

özel anahtarı ve

$$(B_2)_p = \otimes_{i=1}^{m} \left((B_2^1)_i \oplus (B_2^2)_i\right)$$

genel anahtarı üretilmiş olur. Burada $\oplus$ sembolü N modülünde toplama işlemini temsil

eder.

Elde edilen bu anahtarlardan $(B_2)_s$ özel anahtar olarak B_2 bloğunda saklanırken, $(B_2)_p$ genel anahtar olarak B_3 ve B_4 bloklarına süperyoğun kodlama yardımıyla gönderilir. Bunun için de $(B_2)_p$ genel anahtarı kopyalanarak

$$(B_2)_{pp} = \otimes_{i=1}^{m} \left((B_2)_{p_i}(B_2)_{p_i}\right)$$

biçimine dönüştürülür. Genel anahtarın paylaşıldığı B_3 ve B_4 bloklarında yapılan yüksek boyutlu Bell ölçümü sonucunda gerçek $(B_2)_p$ değeri hesaplanıp B_3 ve B_4 bloklarında saklanır.

4. B_1 bloğunda $t = T$ zamanda iki foton üzerinde yapılan HDBM sonucunda

$$B_1^1 B_1^2 = \{00, 01, \ldots, (N-1)(N-1)\}$$

değerlerinden herhangi biri elde edilir. Bu ölçüm sonuçları kullanılarak

$$(B_1)_s = \otimes_{i=1}^{m} \left((B_1^1)_i (B_1^2)_i\right)$$

özel ve

$$(B_1)_p = \otimes_{i=1}^{m} \left((B_1^1)_i \oplus (B_1^2)_i\right)$$

genel anahtarı oluşturulur. Burada $(B_1)_s$ özel anahtar olarak, $(B_1)_p$ ise sadece B_4 bloğu ile paylaşılacak genel anahtar olarak B_1 bloğunda saklanır.

B_1 bloğunda yapılan ölçüm sonucunda ve B_1 bloğu ile B_4 bloğu arasında oluşan dolaşıklık kanalı aracığıyla B_4 bloğunda;

$$|d_{B_4}\rangle = \otimes_{i=1}^{m} U_{j_i k_i}^{\dagger} |d_{B_1}\rangle \tag{4.58}$$

(4.58) denklemiyle verilen kuantum durumu oluşur.

Burada,

$$j_i = \oplus_{r=1}^{3}(B_r)_{p_i^1} = (B_1)_{p_i^1} \oplus (B_2)_{p_i^1} \oplus (B_3)_{p_i^1}, \qquad (i = 1,2,\ldots,m)$$

ve

$$k_i = \oplus_{r=1}^{3}(B_r)_{p_i^2} = (B_1)_{p_i^2} \oplus (B_2)_{p_i^2} \oplus (B_3)_{p_i^2}, \qquad (i = 1,2,\ldots,m)$$

şeklinde tanımlıdır. Ayrıca B_1 bloğu $t = T$ anında yeni bazlarda yaptığı ölçüm sonucunda zaman damgalı $ID_{B_1}^G$ genel kimliğini elde eder.

$$ID_{B_1}^G = \otimes_{i=1}^{m} U^{\dagger}_{\left((B_1)_{p_i^1}\right)\left((B_1)_{p_i^2}\right)} \left|\xi_{data_i^1}\right\rangle \tag{4.59}$$

$ID_{B_1}^G$ yi genel kimliği olarak yayınlar.

5. B_4 bloğunda (4.58) denkleminde yeni bazlarda ölçüm gerçekleştirilerek B_1 bloğuna ait kimliği $ID_{B_4}^{B_1}$ olarak hesaplar. Burada alt ve üst simge sırasıyla verinin aktarılacağı bloğu ve kimliğin gerçek sahibi olan bloğu ifade eder.

4.5.2. Mesajlaşma ve Doğrulama Adımı

1. B_1 bloğundan B_4 bloğuna $\{data_i^1, (B_1)_p\}$ çifti teleport edilir. B_1 bloğundan teleport edilen $\{data_i^1, (B_1)_p\}$ çiftinin her hangi bir nedenden dolayı (çevresel faktörkler ya da dışarıdan müdahale) değiştiğini varsayarak $\{\overline{data}_i^1, (\overline{B_1})_p\}$ biçiminde gösterelim.

(a) Doğrulama-1: B_4 bloğunda (4.52) denklemi ve $\{\overline{data}_i^1, (\overline{B_1})_p\}$ çifti kullanılarak $\overline{ID}_{B_1}^G$ değeri hesaplanır ve B_1 bloğundan yayınlanan $ID_{B_1}^G$ kimliği ile eşitliği kontrol edilir.

$$(\overline{ID}_{B_1}^G)_i = (ID_{B_1}^G)_i, \qquad (i = 1,2,\ldots,m)$$

(b) Doğrulama-2: Bu adımda B_4 bloğunda B_1 bloğu tarafından yayınlanan $ID_{B_1}^G$ ile B_4 bloğunda yeni bazlarda yapılan ölçüm sonucunda elde edilen $ID_{B_4}^{B_1}$ kimliğinin eşitliği

kontrol edilir.

$$i=1,\ldots,m \quad \begin{cases} (ID_{B_1}^{G})_i = (ID_{B_4}^{B_1})_i, & \text{eğer } (B_2)_{p_i} \oplus (B_3)_{p_i} = 0 \\ (ID_{B_1}^{G})_i \neq (ID_{B_4}^{B_1})_i, & \text{eğer } (B_2)_{p_i} \oplus (B_3)_{p_i} \neq 0 \end{cases} \tag{4.60}$$

2. B_4 bloğunda yapılan kontroller sonucunda verinin doğruluğu ile geçerliliği kabul edilirse, $\{\overline{data}_i^1, (\overline{B_1})_p, \overline{ID}_{B_4}^{B_1}\}$ üçlüsü B_3 bloğuna aktarılır. Bu blokta ise verinin doğru ya da sahte ve reddedilmiş ya da kabul edilmiş olduğunu belirlemek için aşağıdaki doğrulama adımları gerçekleştirilir.

3. Kimlik hesaplaması, B_1 bloğunun yayınladığı $ID_{B_1}^{G}$ genel kimlik ile yapılacaktır.Yani doğru karar vermek adına B_4 bloğundan aktarılan her hangi bir veri kullanılmayacaktır.

B_3 bloğunda B_1 bloğuna ait $ID_{B_1}^{G}$ kullanılarak,

$$\otimes_{i=1}^{m} \left(U^{\dagger}_{(B_2)_{s_i^1 s_i^2}} (|d_{B_4}\rangle)_i = U^{\dagger}_{(B_3)_{s_i^1 s_i^2}} \left(\left| ID_{B_1}^{G} \right\rangle \right)_i \right)$$

B_3 bloğunda yeni bazlarda yapılan ölçüm sonucunda $ID_{B_3}^{B_4}$ elde edilir. Daha sonra B_3 bloğunda hesaplanan kimlik ile B_4 bloğundan aktarılan kimliğin eşitliği kontrol edilir.

$$i=1,\ldots,m \quad \begin{cases} (ID_{B_3}^{B_4})_i = (\overline{ID}_{B_3}^{B_1})_i, & \text{eğer } (B_2)_{p_i} = 0 \\ (ID_{B_3}^{B_4})_i = (\overline{ID}_{B_3}^{B_1})_i, & \text{eğer } (B_2)_{p_i} \neq 0 \end{cases} \tag{4.61}$$

Bu sayede B_3 bloğunda, B_4 bloğunda her hangi bir sahtecilik yapılıp yapılmadığı kontrol edilmiş olur.

4. B_3 bloğunda da B_4 bloğundaki gibi Doğrulama-1 ve Doğrulama-2 adımları gerçekleştirilir ve B_1 bloğunda her hangi bir reddetme olup olmadığı belirlenir. Tüm doğrulamalar doğru ise mesajın aktarılabilir olduğu belirlenmiş olur. Daha sonra B_3 bloğundan $\{\overline{data}_i^1, (\overline{B_1})_p, \overline{ID}_{B_4}^{B_1}\}$ üçlüsü B_2 bloğuna aktarılır.

5. B_2 bloğunda doğrulama yapmak için $(B_3)_p$ değeri kullanılır.

$$\otimes_{i=1}^{m}\left(U^{\dagger}_{(B_3)_{s_i^1 s_i^2}}\left(|d_{B_4}\rangle\right)_i = U^{\dagger}_{(B_2)_{s_i^1 s_i^2}}\left(\left|ID^G_{B_1}\right\rangle\right)_i\right)$$

B_2 bloğunda yeni bazlarda yapılan ölçüm sonucunda $ID^{B_4}_{B_2}$ elde edilir ve aşağıdaki kontroller yapılır.

$$i=1,\ldots,m \quad \begin{cases} (ID^{B_4}_{B_2})_i = (\overline{ID}^{B_1}_{B_4})_i, & \text{eğer } (B_3)_{p_i}=0 \\ (ID^{B_4}_{B_2})_i = (\overline{ID}^{B_1}_{B_4})_i, & \text{eğer } (B_3)_{p_i}\neq 0 \end{cases} \tag{4.62}$$

6. Protokolde ihtiyaç duyulursa B_3 bloğuna ait $\{\overline{data_i}^1, (\overline{B_1})_p, \overline{ID}^{B_1}_{B_3}\}$ üçlüsü B_2 bloğuna aktarılır. B_2 bloğunda doğrulama aşağıdaki gibi gerçekleşir.

$$\otimes_{i=1}^{m}\left(\left(|d_{B_4}\rangle\right)_i = U^{\dagger}_{(B_2)_{s_i^1 s_i^2}}\left(\left|ID^G_{B_1}\right\rangle\right)_i\right)$$

B_2 bloğunda yukarıdaki eşitlikte yeni bazlarda ölçüm yapılarak $ID^{B_3}_{B_2}$ değeri elde edilir ve aşağıdaki kontroller gerçekleştirilir.

$$\left((ID^{B_3}_{B_2})_i = (\overline{ID}^{B_4}_{B_3})_i\right), \;\; i=1,\ldots,m$$

BEŞİNCİ BÖLÜM
SONUÇ VE ÖNERİLER

5.1. Güvenlik Analizi

Önerilen protokol yüksek boyutlu olduğundan, herhangi birinin bilgi edinme olasılığı, kübit durumlarından çok daha düşüktür. $N-$ boyutunda çoklu katılımcılar için süperyoğun kodlama ve dolaşıklığa dayalı önerilen QDS'nin güvenlik analizi aşağıdaki gibidir.

1. **İnkar Etmeme:** Gönderici P_1 katılımcısı, $P_2, P_3, \ldots, P_{M-1}$ katılımcılarının p_i^g larını bilmiyorsa , m_i^1 ve p_1^g'ı değiştiremez, yani Doğrulama-1 ve Doğrulama-2'yi geçemez. Doğrulama-2, $P_2, \ldots, P_{M-1}$ katılımcılarının p_i^g $(i = 2, \ldots, M-1$ olmak üzere) özel anahtarlarına bağlıdır.

2. **Aktarılabilirlik:** P_M katılımcısı, P_1 katılımcısından gelen mesajın kimliğinin doğrulandığını kabul ederse, P_M katılımcısı mesajı P_T katılımcısına gönderir. P_T katılımcısı mesajın geçerli ve doğrulanmış olduğunu kabul etmezse, mesaj aktarılamaz. Ayrıca P_T katılımcısı, P_1 katılımcısının genel anahtarını kullanarak P_1 katılımcısından gelen mesajı hesaplar, ardından P_T katılımcısı, P_M katılımcısının Doğrulama-1 ve Doğrulama-2 işlemlerini gerçekleştirir. P_M katılımcısı sahtecilik yapmazsa, P_T katılımcısı mesajın geçerli ve doğrulanmış olduğunu kabul edecektir.

3. **Sahtecilik:** Eğer P_M katılımcısı P_T katılımcısına geçersiz $\{\overline{m}_i^1, \overline{p}_1^g, \overline{Sig}_{P_M}^{P_1}\}$ üçlüsünü gönderirse P_T katılımcısı mesajın doğrulanmış ve geçerli olduğunu kabul eder. Dolayısıyla P_M katılımcısı başarıyla sahtecilik yapmış olur. P_M katılımcısı $\{m^1, p_1^s\}$ ve $Sig_{P_1}^G$, $Sig_{P_M}^{P_1}$ değerlerini biliyor. Ancak P_T katılımcısı, Doğrulama-3'te P_M katılımcısı tarafından gönderilen değerler yerine, yalnızca P_1 katılımcısının genel anahtarını kullanır, bu nedenle P_M katılımcısı herhangi bir sahtecilik yapamaz.

4. **Alıcı tarafından mesaj oluşturma:** Bu mümkün değildir çünkü gönderenin genel imzası herkese açıktır ve her katılımcı bu genel imzayı doğrulama sürecinde kullanır.

5. **Mesajın alıcı tarafından değiştirilmesi:** Genel imza ve gönderilen mesaj, diğer katılımcılardan gelen bilgileri içerir, dolayısıyla bu mümkün değildir.

6. **İç Saldırı:** Önerilen QDS'deki doğrulama adımlarından (bkz. bölüm 3.2 ve 4.2) görülebileceği gibi her katılımcı birbirini kontrol eder, her katılımcı mesajın doğruluğunu ve geçerliliğini inceler ve önceki katılımcı tarafından herhangi bir sahtecilik olup olmadığını tespit edebilir. Bu işlemler için de daha az doğrulama anahtarı kullanılır.

7. **Dış Saldırı:** Eve adlı harici saldırganın P_M katılımcılarından bilgi almaya çalıştığını düşünelim. Gönderilecek mesaj farklı $N-$boyutlu tabanlara dönüştürüldüğünden ve katılımcılar arasında dolaşıklık olduğundan Eve'in araya girip mesajı ve anahtarı alması zordur. Yukarıda görüldüğü gibi, önerilen QDS dış saldırılara karşı dirençlidir.

5.2. Sonuçlar

Bu çalışmada, dolaşıklık, dolaşıklık takası ve süperyoğun kodlamaya dayalı çok katılımcılı N boyutlu bir kuantum dijital imza protokolü geliştirmeye çalıştık. Bazı kuantum imza protokollerinde, kuantum verilerinin bir kuantum belleğine kaydedilmesi gerekir. Bu, kısa kuantum uyumsuzluk süresi nedeniyle modern kuantum teknolojisi tarafından mümkün değildir. Bu protokolde, tüm veriler (kuantum ve klasik) dolaşıklık kanalları kullanılarak anında gönderilir. Ayrıca, protokolün güvenliğini artırmak için ölçüm sonuçları süperyoğun kodlama ile gönderilir.

Ayrıca, yüksek boyutlu bilgi paylaşımı ve kuantum hesaplama gürültü sorununun üstesinden gelmeye, daha fazla veri aktarmaya ve yüksek oranda anahtar üretmeye izin verdiği için daha güvenli bir bilgi paylaşımı sağlar (Cozzolino vd., 2019).

Bu durumu aşağıda kısaca örneklendirebiliriz. N boyutunda $\log_2 N$, aynı miktarda bilgiyi kodlamak için gereken kübit (veya klasik bit) sayısını verir (Cozzolino vd., 2019). Örneğin,

$N = 4$ için, $\log_2 4 = 2$ olduğundan, 2 bit bilgi kodlanabilir.

$$|0\rangle = 00, |1\rangle = 01, |2\rangle = 10, |3\rangle = 11$$

$N = 8$ için, $\log_2 8 = 3$ olduğundan, 3 bit bilgi kodlanabilir.

$$|0\rangle = 000, |1\rangle = 001, |2\rangle = 010, |3\rangle = 100,$$

$$|4\rangle = 011, |5\rangle = 101, |6\rangle = 011, |7\rangle = 111$$

Kuantum iletişimi için yüksek boyutun bir başka avantajı da, çevresel faktörlerden veya gizli dinleme saldırılarından kaynaklanan gürültüye karşı daha dayanıklı olmasıdır.

P_m herhangi bir katılımcı olsun. P_m katılımcısının Bell ölçüm sonucu aşağıdaki kümenin elemanların biri olsun.

$$p_m^1 p_m^2 = \{00, 01, \ldots, 0(N-1), \ldots, (N-1)(N-1)\} \tag{5.1}$$

Bu nedenle, P_m katılımcısının bu ölçüm sonuçlarından birini elde etme olasılığı $\frac{1}{2^N}$'dır. Bu nedenle, dışarıdan bir dinleyicinin P_m katılımcısının ölçüm sonucunu alma olasılığı da $\frac{1}{2^N}$'dır.

N boyutunda $N \to \infty$ için $\frac{1}{2^N} \to 0$ olacağından, boyut arttıkça dışarıdan bir dinleyicinin ölçüm sonucunu yakalama olasılığı sıfıra yaklaşacaktır. Yani imkansızdır.

P_m katılımcısı tarafından oluşturulan özel(p) ve genel(p_m^g) anahtarları aşağıdaki gibi olsun.

$$p = \otimes_{i=1}^{n} \left(p_i^1 p_i^2\right) = \underbrace{p_1^1 p_1^2 p_2^2 p_2^2 \ldots p_n^2 p_n^2}_{\text{2n uzunluğunda}}$$

$$\begin{aligned} p_m^g &= \otimes_{i=1}^{n} (p_i^1 \oplus p_i^2) \\ &= \underbrace{(p_1^1 \oplus p_1^2)(p_2^2 \oplus p_2^2) \ldots (p_n^2 \oplus p_n^2)}_{\text{n uzunluğunda}} \\ &= \underbrace{p_1^{12} p_2^{12} \ldots p_n^{12}}_{\text{n uzunluğunda}} \end{aligned}$$

P_m katılımcısı, p_m^g yi süperyoğun kodlama yardımıyla iletmek için aşağıdakileri yapar.

$$p_m^{gg} = \otimes_{i=1}^{n}(p_i^g \wedge p_i^g) = \underbrace{(p_1^g p_1^g)(p_2^g p_2^g)\ldots(p_n^g p_n^g)}_{\text{2n uzunluğunda}}$$

P_m katılımcısı, elde ettiği p_m^{gg} genel anahtarını süperyoğun kodlama yardımıyla diğer katılımcılarla paylaşır. P_m katılımcısı tarafından paylaşılan genel anahtarın bir dış dinleyici tarafından doğru bir şekilde elde edilme olasılığı $\frac{1}{2^{2n}} = \frac{1}{4^n}$'dır. N boyutta bir veriyi kodlamak için $\log_2 N$ klasik bit (veya kübit) gerekir. Yani boyut arttıkça bilgi kapasitesi de artar. $N \to \infty$ olduğunda, bilgi dizisinin uzunluğu da artacaktır. Bu nedenle $n \to \infty$ yaklaşır. $n \to \infty$ için, $\frac{1}{4^n} \to 0$ yaklaşıyor. Bu nedenle, dinleyicinin P_m katılımcısı tarafından paylaşılan genel anahtarı elde etme olasılığı sıfıra yaklaşır. Yani bu imkansızdır.

Dolaşıklık takası, iki kuantum sistemini doğrudan etkileşim olmadan dolaştırmamıza izin verdiği için, bilgi uzun mesafelerde herhangi bir değişiklik olmaksızın kolayca iletilebilir. Protokolün güvenliğini artırmak için herhangi bir klasik veri iletim gereksiniminde süperyoğun kodlama kullanılmıştır. Bu protokol Chi vd. (2022); Da Lio vd. (2021); Feng vd. (2022); Iqbal ve Krawec (2023); Srivastav vd. (2022b); Zhou vd. (2019) gibi deneysel yöntemler kullanılarak deneysel olarak gerçekleştirilmiştir.

KAYNAKLAR

Acar, E. (2021). *Hibrid kuantum-klasik makine öğrenmesi ile kovid-19 tespiti* (Doktora Tezi).

Acar, E., Gündüz, S., Akpınar, G., ve Yılmaz, I. (2022). High-dimensional Grover multi-target search algorithm on Cirq. *European Physical Journal Plus*, *137*(2), 244.

Bai, C.-M., Li, Z.-H., Xu, T.-T., ve Li, Y.-M. (2017). Quantum secret sharing using the d-dimensional GHZ state. *Quantum Information Processing*, *16*(3), 59.

Cai, X.-Q., Wang, T.-Y., Wei, C.-Y., ve Gao, F. (2019). Cryptanalysis of multiparty quantum digital signatures. *Quantum Information Processing*, *18*(8), 252.

Casacio, C. A., Madsen, L. S., Terrasson, A., Waleed, M., Barnscheidt, K., Hage, B., ... Bowen, W. P. (2021). Quantum-enhanced nonlinear microscopy. *Nature*, *594*(7862), 201-206.

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

Chi, Y., Huang, J., Zhang, Z., Mao, J., Zhou, Z., Chen, X., ... Wang, J. (2022). A programmable qudit-based quantum processor. *Nature Communications*, *13*, 1166.

Clarke, P. J., Collins, R. J., Dunjko, V., Andersson, E., Jeffers, J., ve Buller, G. S. (2012). Experimental demonstration of quantum digital signatures using phase-encoded coherent states of light. *Nature Communications*, *3*, 1174.

Cozzolino, D., Da Lio, B., Bacco, D., ve Katsuo Oxenløwe, L. (2019, October). High-dimensional quantum communication: benefits, progress, and future challenges. *arXiv e-prints*, arXiv:1910.07220.

Şahin, E. (2019). *Kuantum temelli görüntü işleme* (Doktora Tezi).

Da Lio, B., Cozzolino, D., Biagi, N., Ding, Y., Rottwitt, K., Zavatta, A., ... Oxenløwe, L. K. (2021). Path-encoded high-dimensional quantum communication over a 2-km multicore fiber. *npj Quantum Information*, *7*, 63.

Feng, T., Xu, Q., Zhou, L., Luo, M., Zhang, W., ve Zhou, X. (2022, Dec). Quantum information transfer between a two-level and a four-level quantum systems. *Photon. Res.*, *10*(12), 2854–2865.

Gao, Y.-L., Chen, X.-B., Xu, G., Yuan, K.-G., Liu, W., ve Yang, Y.-X. (2020). A novel quantum blockchain scheme base on quantum entanglement and DPoS. *Quantum Information Processing*, *19*(12), 420.

Gisin, N. s. (2014). *Quantum chance: Nonlocality, teleportation and other quantum marvels*. Springer.

Google quantum ai. (2023). https://quantumai.google/. (Erişim Tarihi: 18/07/2023)

Gottesman, D., ve Chuang, I. (2001). Quantum digital signatures. *eprint arXiv:quant-ph/0105032*.

Greenberger, D. M., Horne, M. A., ve Zeilinger, A. (1989). *Bell's theorem, quantum theory, and conceptions of the universe*. Kluwer Academics, Dordrecht, The Netherlands.

Hu, Z., ve Kais, S. (2022). The wave-particle duality of the qudit quantum space and the quantum wave gates.

Ibm quantum computing. (2023). https://www.ibm.com/quantum. (Erişim Tarihi: 18/07/2023)

Imany, P., Jaramillo-Villegas, J. A., Odele, O. D., Han, K., Leaird, D. E., Lukens, J. M., ... Weiner, A. M. (2018). 50-ghz-spaced comb of high-dimensional frequency-bin entangled photons from an on-chip silicon nitride microresonator. *Opt. Express*, *26*(2), 1825–1840.

Iqbal, H., ve Krawec, W. O. (2023, July). New Security Proof of a Restricted High-Dimensional QKD Protocol. *arXiv e-prints*, arXiv:2307.09560.

Li, C., Chen, X., Li, H., Yang, Y., ve Li, J. (2019). Efficient quantum private comparison protocol based on the entanglement swapping between four-qubit cluster state and extended Bell state. *Quantum Information Processing*, *18*(5), 158.

Lu, Y.-S., Cao, X.-Y., Weng, C.-X., Gu, J., Xie, Y.-M., Zhou, M.-G., ... Chen, Z.-B. (2021). Efficient quantum digital signatures without symmetrization step. *Opt. Express*, *29*(7), 10162–10171.

Mooney, G. J., White, G. A. L., Hill, C. D., ve Hollenberg, L. C. L. (2021). Generation and verification of 27-qubit Greenberger-Horne-Zeilinger states in a superconducting quantum computer. *Journal of Physics Communications*, *5*(9), 095004.

Nielsen, M. A., ve Chuang, I. L. (2010). *Quantum computation and quantum information: 10th anniversary edition*. Cambridge University Press.

Ono, T., Okamoto, R., ve Takeuchi, S. (2013). An entanglement-enhanced microscope. *Nature Communications*, *4*, 2426.

Paesani, S., Bulmer, J. F. F., Jones, A. E., Santagati, R., ve Laing, A. (2021). Scheme for Universal High-Dimensional Quantum Computation with Linear Optics. *Physical Review Letters*, *126*(23), 230504.

Pelet, Y., Puthoor, I. V., Venkatachalam, N., Wengerowsky, S., Lončarić, M., Neumann,

S. P., ... Joshi, S. K. (2022). Unconditionally secure digital signatures implemented in an eight-user quantum network. *New Journal of Physics*, *24*(9), 093038.

Qin, H., Tang, W. K. S., ve Tso, R. (2020). Quantum (t, n) threshold group signature based on Bell state. *Quantum Information Processing*, *19*(2), 71.

Qu, W., Zhang, Y., Liu, H., Dou, T., Wang, J., Li, Z., ... Ma, H. (2019). Multi-party ring quantum digital signatures. *Journal of the Optical Society of America B Optical Physics*, *36*(5), 1335.

Rajan, D., ve Visser, M. (2019). Quantum blockchain using entanglement in time. *Quantum Reports*, *1*(1), 3–11.

Shen, Y., Nape, I., Yang, X., Fu, X., Gong, M., Naidoo, D., ve Forbes, A. (2021). Creation and control of high-dimensional multi-partite classically entangled light. *Light: Science & Applications*, *10*(1), 50.

Song, Y. (2020, 01). A new efficient blind quantum signature scheme based on entanglement swapping. *DEStech Transactions on Engineering and Technology Research*.

Srivastav, V., Valencia, N. H., McCutcheon, W., Leedumrongwatthanakun, S., Designolle, S., Uola, R., ... Malik, M. (2022a). Quick Quantum Steering: Overcoming Loss and Noise with Qudits. *Physical Review X*, *12*(4), 041023.

Srivastav, V., Valencia, N. H., McCutcheon, W., Leedumrongwatthanakun, S., Designolle, S., Uola, R., ... Malik, M. (2022b). Quick Quantum Steering: Overcoming Loss and Noise with Qudits. *Physical Review X*, *12*(4), 041023.

Vagniluca, I., Da Lio, B., Rusca, D., Cozzolino, D., Ding, Y., Zbinden, H., ... Bacco, D. (2020). Efficient time-bin encoding for practical high-dimensional quantum key distribution. *Phys. Rev. Applied*, *14*, 014051.

Wang, F., Erhard, M., Babazadeh, A., Malik, M., Krenn, M., ve Zeilinger, A. (2017). Generation of the complete four-dimensional Bell basis. *Optica*, *4*(12), 1462.

Wang, T.-Y., Cai, X.-Q., Ren, Y.-L., ve Zhang, R.-L. (2015). Security of quantum digital signatures for classical messages. *Scientific Reports*, *5*, 9231.

Wang, Y., Hu, Z., Sanders, B. C., ve Kais, S. (2020). Qudits and high-dimensional quantum computing. *Frontiers in Physics*, *8*. doi: 10.3389/fphy.2020.589504

Weng, C.-X., Lu, Y.-S., Gao, R.-Q., Xie, Y.-M., Gu, J., Li, C.-L., ... Chen, Z.-B. (2021). Secure and practical multiparty quantum digital signatures. *arXiv e-prints*, arXiv:2104.12059.

Xing, W.-B., Hu, X.-M., Guo, Y., Liu, B.-H., Li, C.-F., ve Guo, G.-C. (2023). Preparation of multiphoton high-dimensional GHZ states. *Optics Express*, *31*(15), 24887.

Yin, H.-L., Fu, Y., ve Chen, Z.-B. (2016). Practical quantum digital signature. *Physical Review A*, *93*(3), 032316.

Yin, H.-L., Fu, Y., Li, C.-L., Weng, C.-X., Li, B.-H., Gu, J., ... Chen, Z.-B. (2021). Experimental quantum secure network with digital signatures and encryption. *arXiv e-prints*, arXiv:2107.14089.

Yin, H.-L., Fu, Y., Liu, H., Tang, Q.-J., Wang, J., You, L.-X., ... Pan, J.-W. (2017). Experimental quantum digital signature over 102 km. *Physical Review A*, *95*(3), 032334.

Yin, H.-L., Wang, W.-L., Tang, Y.-L., Zhao, Q., Liu, H., Sun, X.-X., ... Pan, J.-W. (2017). Experimental measurement-device-independent quantum digital signatures over a metropolitan network. *Physical Review A*, *95*(4), 042338.

Zhao, X.-Q., Zhou, N.-R., Chen, H.-Y., ve Gong, L.-H. (2019). Multiparty Quantum Key Agreement Protocol with Entanglement Swapping. *International Journal of Theoretical Physics*, *58*(2), 436-450.

Zhao-Xu, J., ve Tian-Yu, Y. (2017). Multi-party quantum private comparison based on the entanglement swapping of d-level cat states and d-level Bell states. *Quantum Information Processing*, *16*(7), 177.

Zhou, Y., Mirhosseini, M., Oliver, S., Zhao, J., Rafsanjani, S. M. H., Lavery, M. P. J., ... Boyd, R. W. (2019). Using all transverse degrees of freedom in quantum communications based on a generic mode sorter. *Optics Express*, *27*(7), 10383.