BİLGİ TEKNOLOJİLERİ VE İLETİŞİM KURUMU

KUANTUM KRİPTOGRAFİ: TEHDİTLER VE ÖNLEMLER, DÜNYA ÖRNEKLERİNİN İNCELENMESİ VE ÜLKEMİZ İÇİN ÖNERİLER

Elif YILDIRIMLI AYDINLI

Bilişim Uzmanlığı Tezi

Ocak 2024

Ankara

BİLGİ TEKNOLOJİLERİ VE İLETİŞİM KURUMU

KUANTUM KRİPTOGRAFİ: TEHDİTLER VE ÖNLEMLER, DÜNYA ÖRNEKLERİNİN İNCELENMESİ VE ÜLKEMİZ İÇİN ÖNERİLER

Elif YILDIRIMLI AYDINLI

Bilişim Uzmanlığı Tezi

Ocak 2024

Ankara

Elif YILDIRIMLI AYDINLI tarafından hazırlanan “KUANTUM KRİPTOGRAFİ: TEHDİTLER VE ÖNLEMLER, DÜNYA ÖRNEKLERİNİN İNCELENMESİ VE ÜLKEMİZ İÇİN ÖNERİLER” adlı bu tezin Bilişim Uzmanlık tezi olarak uygun olduğunu onaylarım.

Mahire AKTAŞ

Tez Danışmanı

Bu çalışma, tez savunma komisyonumuz tarafından Bilişim Uzmanlığı tezi olarak kabul edilmiştir.

Başkan: Kurul II. Başkanı Selamettin ERMİŞ

Üye: Daire Başkanı, Afşin BÜYÜKBAŞ

Üye: Bilişim Başuzmanı, Özgür ÖZTÜRK

Üye: Daire Başkanı, Mahmut Esat YILDIRIM

Üye: Bilişim Uzmanı, Mahire AKTAŞ

Bu tez, Bilgi Teknolojileri ve İletişim Kurumu tez yazım kurallarına uygundur.

İÇİNDEKİLER

ÖZET

BİLGİ TEKNOLOJİLERİ VE İLETİŞİM KURUMU	
Tezin Adı	Kuantum Kriptografi: Tehditler ve Önlemler, Dünya Örneklerinin İncelenmesi, Ülkemiz İçin Öneriler
Türü	Bilişim Uzmanlığı Tezi
Yazar	Elif YILDIRIMLI AYDINLI
Teslim Tarihi	16.02.2024
Anahtar Kelimeler	Kuantum Kriptografi, Bilgi Güvenliği
Tez danışmanı	Mahire AKTAŞ
Sayfa Adedi	IX+158

Verinin yetkisiz kişilerce anlaşılmaz hale getirilmesinde kullanılan kriptografik yöntemler günümüzde dijital ortamda veri iletimi ile depolanması aşamalarında bilgi güvenliği sağlayabilmek amacıyla sıklıkla kullanılmaktadır. Kuantum hesaplama teknolojilerinde yaşanan gelişim ise günümüzde yaygın kullanım alanı bulunan şifreleme algoritmalarının güvenliğini tehdit etmektedir. Mevcut kriptografik algoritmalar için somut bir güvenlik tehdidi oluşturacak kadar gelişmiş bir kuantum bilgisayarın ne zaman gerçekleşeceği kesin olarak bilinmemekle birlikte kuantum siber saldırılardan korunmaya yönelik araştırmalar şimdiden başlatılmıştır. Kuantum sonrası kriptografi temel olarak iki güvenli haberleşme protokolünü temsil etmektedir. Birincisi temeli kuantum mekaniği ilkelerine dayanan ve kuantum iletişim kanallarının kullanılarak gizli anahtar dağıtımına imkan tanıyan kuantum anahtar dağıtımı protokolleridir. İkincisi ise kuantum güvenli kriptografi olarak adlandırılan ve klasik kriptografik algoritmalarda olduğu gibi matematiksel problemlerin çözümünün zorluğuna dayandırılan ancak yalnızca klasik bilgisayarların değil, kuantum bilgisayarların da saldırılarına dirençli matematiksel tekniklerin üzerine inşa edilen yeni kriptografik yöntemlerdir. Bu kapsamda kuantum hesaplama teknolojilerine yönelik bilgi güvenliğini sağlayabilmek amacıyla standardizasyon kuruluşları tarafından çeşitli standartlar belirlenmiş ve ülkeler tarafından rehber dokümanlar ve düzenlemeler yayımlanmıştır. Bu çalışmada kuantum kriptografi alanında ülkelerin ve kuruluşların çalışmaları incelenmiş, ülkemiz için düzenleme önerileri sunulmuştur.

ABSTRACT

INFORMATION TECHNOLOGIES AND COMMUNICATIONS AUTHORITY	
Thesis	Quantum Cryptography: Threats and Precautions, Examination of World Examples, Suggestions for Our Country
Type	ICT Expert Thesis
Author	Elif YILDIRIMLI AYDINLI
Submission Date	16.02.2024
Key Words	Quantum Cryptography, Information Security
Advisor	Mahire AKTAŞ
Total Page	IX+158

Cryptographic methods, which are used to make data unintelligible to unauthorized persons, are widely used today to provide information security at the stages of data transmission and storage in digital media. The development of quantum computing technologies threatens the security of today's widely used encryption algorithms. Although it is not known when a quantum computer advanced enough to pose a concrete security threat to existing cryptographic algorithms will be realised, research into protection against quantum cyber-attacks has already begun. Post-quantum cryptography is essentially two secure communication protocols. The first is quantum key distribution protocols, which are based on the principles of quantum mechanics and allow secret key distribution using quantum communication channels. The second is secure quantum cryptography, which is based on the difficulty of solving mathematical problems as in classical cryptographic algorithms, but is built on mathematical techniques that are resistant to attacks not only by classical computers but also by quantum computers. In this context, various standards have been set by standardization bodies and guidelines and regulations have been published by countries to ensure information security for quantum computing technologies. This study examines the studies carried out by countries and organizations in the field of quantum cryptography and proposes regulations for our country.

TEŞEKKÜR

Uzmanlık tezi süresi boyunca konu seçiminden hazırlanmasına her aşamasında kıymetli bilgi ve deneyimlerini paylaşarak desteklerini sunan danışmanım Mahire AKTAŞ'a, kıymetli tecrübelerini, zamanını ve desteğini hiç esirgemeyen Demet KABASAKAL'a ve Daire Başkanım Mahmut Esat YILDIRIM'a çalışma sürecimde destekleri ve fedakarlıklarıyla, her zaman olduğu gibi hep yanımda olan sevgili annem, babam ve canım kardeşime, manevi desteklerinden güç aldığım tüm dost ve çalışma arkadaşlarıma, özellikle Esra DURUOĞLU, Enes ERDOĞAN, Doğukan Ömer GÜR, Zehra YILMAZ ve Hasan YILMAZ'a, sabrı, desteği ve güzel kalbi ile her zaman yanımda olan biricik eşim Mehmet Fatih AYDINLI'ya teşekkürü bir borç bilirim.

TABLOLAR LİSTESİ

ŞEKİLLER LİSTESİ

KISALTMALAR LİSTESİ

3DES	Üçlü DES (Triple-DES)
AB	Avrupa Birliği (European Union)
ABD	Amerika Birleşik Devletleri
AES	Gelişmiş Şifreleme Standardı (Advanced Encryption Standard)
Ar-Ge	Araştırma ve Geliştirme
BİLGEM	Bilişim ve Bilgi Güvenliği İleri Teknolojiler Araştırma Merkezi
BTK	Bilgi Teknolojileri ve İletişim Kurumu
CACR	Çin Kriptoloji Araştırma Derneği (Chinese Association for Cryptologic Research)
C-DOT	Hindistan Telematik Geliştirme Merkezi (Centre for Development of Telematics)
CISA	Amerikan Siber Güvenlik ve Altyapı Güvenliği Ajansı (Cybersecurity and Infrastructure Security Agency)
COST	Bilim ve Teknoloji Alanında Avrupa İşbirliği (European Cooperation in Science and Technology)
COW	Coherent One-Way
CRYPTREC	Kriptografi Araştırma ve Değerlendirme Komiteleri (Cryptography Research and Evaluation Committees)
DARPA	Defense Advenced Research Projects Agency
DES	Veri Şifreleme Standardı (Data Encryption Standard)
DOE	Amerikan Enerji Bakanlığı (Department of Energy)
DoS	Hizmet Dışı Bırakma Saldırısı (Denial of Service)
DSA	Dijital İmza Algoritması (Digital Signature Algorithm)

EHK	5809 sayılı Elektronik Haberleşme Kanunu
ENISA	Avrupa Birliği Siber Güvenlik Ajansı (European Union Agency for Cybersecurity)
ERA-NET	Avrupa Araştırma Alanı Ağı (European Research Area Networks)
ESA	Avrupa Uzay Ajansı (European Space Agency)
ETSI	Avrupa Telekomünikasyon Standartları Enstitüsü (European Telecommunications Standards Institute)
EuroQCI	Avrupa Kuantum İletişim Altyapısı (European Quantum Communication Infrastructure)
GSMA	Küresel Mobil İletişim Sistemi Derneği (GSM Association)
HTTP	Hiper-Metin Transfer Protokolü (Hypertext Transfer Protocol)
HTTPS	Güvenli Hiper Metin Aktarım İletişim Protokolü (Hypertext Transfer Protocol Secure)
IDEA	Uluslararası Veri Şifreleme Algoritması (International Data Encryption Algorithm)
IEC	Uluslararası Elektroteknik Komisyonu (International Electrotechnical Commission)
IoT	Nesnelerin interneti (Internet of Things)
IP	İnternet Protokolü (Internet Protocol)
IPSec	İnternet Protokolü Güvenliği (Internet Protocol Security)
ISO	Uluslararası Standardizasyon Teşkilatı (International Organization for Standardization)
ISRO	Hindistan Uzay Araştırma Enstitüsü (Indian Space Research Organisation)

KOBİ	Küçük ve Orta Büyüklükteki İşletmeler
KUANTAL	Kuantum Araştırma Laboratuvarı
MadQCI	Madrid kuantum ağı
MDA	Mesaj Özeti Algoritmaları (Message Digest Algorithms)
NICT	Japon Ulusal Bilgi ve Teknolojisi Enstitüsü (National Institute of Information and Communications Technology)
NIST	Ulusal Standartlar ve Teknoloji Enstitüsü (National Istitute of Standards and Technology)
NM-QTA	Hindistan Kuantum Teknolojileri ve Uygulamaları Ulusal Misyonu (National Mission on Quantum Technologies & Applications)
NSA	Amerikan Ulusal Güvenlik Ajansı (National Security Agency)
NSA	Amerikan Ulusal Güvenlik Ajansı (National Security Agency)
NSF	Ulusal Bilim Vakfı (National Science Foundation)
PGP	Pretty Good Pivacy
PIN	Kişisel Kimlik Numaraları (Personal Identification Number)
PNS	Photon Number Splitting
QT-Flagship	Kuantum Teknolojileri Amiral Gemisi (Quantum Technologies Flagship)
QuantERA	Kuantum Teknolojileri Avrupa Araştırma Alanı Ağı (The Quantum ERA-NET)
QUESS	Uzay Ölçeğinde Kuantum Deneyleri (Quantum Experiments at Space Scale)
REDIMadrid	Madrid Araştırma Ağı
RSA	Rivest- Shamir- Adleman

SHA	Güvenli Özet Algoritması (Secure Hash Algorithm)
SIKE	Süpersingüler İzojen Tabanlı Anahtar Değişimi (Supersingular Isogeny Key Exchange)
SSL	Güvenli Soket Katmanı (Secure Sockets Layer)
SVP	En Kısa Vektör Problemleri (Shortest Vector Problems)
TLS	Taşıma Katmanı Güvenliği (Transport Layer Security)
TÜBİTAK	Türkiye Bilimsel ve Teknolojik Araştırma Kurumu
UEKAE	Ulusal Elektronik ve Kriptoloji Araştırma Enstitüsü
VPN	Sanal Özel Ağ (Virtual Private Network)
WEP	Kabloluya Eşdeğer Gizlilik (Wired Equivalent Privacy)
WPA	Wi-Fi Korumalı Erişim (Wi-Fi Protected Access)

GİRİŞ

Bilgi ve iletişim güvenliği bir vatandaşlık hakkı olmanın yanı sıra ülkeler için ulusal güvenliği koruma aracıdır. Kriptografi ise etkileşimde bulunan iki tarafın kimliğini doğrulamak, tarafların işleme katılımını inkar etmesini engellemek, iletişimlerini gizli dinlemelere karşı koruyarak gizliliği sağlamak, iletilen verinin yalnızca yetkili kişilerce değiştirilmesine imkan tanıyarak veri bütünlüğü korumak ve depolanmış verileri korumak için kullanılan temel bir gizlilik ve güvenlik aracıdır.

Günümüzde kullanılan modern kriptografik teknikler, bilinen en iyi algoritmalar ve mevcut en güçlü bilgisayarlarda bile çözümlerinin son derece uzun bir zaman gerektirmesi nedeniyle makul zaman aralığında çözülemeyen hesaplama problemlerine dayanmaktadır. Kuantum hesaplama teknolojilerinde yaşanan gelişmeler sonucu geliştirilen kuantum algoritmalar ise mevcut kriptografik sistemler için bir tehdit oluşturmakta, özellikle mesajı şifrelemek ve şifresini çözmek için farklı anahtarların kullanıldığı asimetrik kriptografi algoritmalarının, büyük ölçekli kuantum bilgisayarların ortaya çıkmasıyla birlikte savunmasız kalması beklenmektedir.

Mevcut kriptografik algoritmalar için somut bir güvenlik tehdidi oluşturacak kadar gelişmiş bir kuantum bilgisayarın ne zaman gerçekleşeceği kesin olarak bilinmemektedir. Ancak yeterli bilgi işlem gücüne sahip bir kuantum bilgisayarın inşası halinde ülkelerin ulusal güvenliğinin tehdit altına girecek olması nedeniyle kuantum siber saldırılardan korunmaya yönelik araştırmalar şimdiden başlatılmıştır.

Kuantum sonrası kriptografi temel olarak iki tür güvenli haberleşme protokolünü temsil etmektedir. Birincisi, temeli kuantum mekaniği ilkelerine dayanan ve kuantum iletişim kanallarının kullanılarak gizli anahtar dağıtımına imkan tanıyan kuantum anahtar dağıtımı protokolleridir. İkincisi ise kuantum güvenli kriptografi olarak adlandırılan ve klasik kriptografik algoritmalarda olduğu gibi matematiksel problemlerin çözümünün zorluğuna dayandırılan ancak yalnızca klasik bilgisayarların değil, kuantum bilgisayarların da saldırılarına dirençli matematiksel tekniklerin üzerine inşa edilen yeni kriptografik yöntemlerdir. Bu tez kapsamında kuantum hesaplama teknolojilerine dirençli tüm kriptografik teknikler kuantum kriptografi başlığı altında incelenmiştir.

Bu çerçevede, ülkemizin yakın gelecekte ortaya çıkabilecek olası kuantum siber saldırılardan korunabilmesi için kamu kurum ve kuruluşları ile kritik altyapı sektörleri öncellikli olmak şartıyla veri iletiminde veya uygulama altyapılarında kullanılan kriptografik algoritmalarının kuantum hesaplama teknolojilerine dirençli kriptografik algoritmalarla değiştirilmesine yönelik bir ulusal politikanın belirlenerek kuantum kriptografi ile ortaya çıkabilecek tehditlere yönelik yol haritasının oluşturulması büyük önem arz etmektedir.

Bu tezin amacı kriptografi, kuantum mekaniği ve kuantum teknolojileri alanlarında bilgi sunarak kuantum teknolojileri ile birlikte gelişen kuantum siber saldırılara karşı oluşturulan kuantum güvenli kriptografi ve kuantum anahtar dağıtımı yöntemlerinin incelenmesidir. Tez kapsamında kuantum kriptografi alanında gerçekleştirilen ulusal ve uluslararası çalışmalar incelenmiş olup ülkemizin kuantum siber saldırılardan korunmasına yönelik düzenleme önerileri sunulmuştur.

Tezin birinci bölümünde kriptografi kavramı ele alınarak geçmişten günümüze gelişimi incelenmiş, kullanım alanlarına değinilerek günümüzde yaygın olarak kullanıldığı teknolojilere yer verilmiştir.

Tezin ikinci bölümünde, kuantum mekaniği ve temel ilkeleri özetlenerek kuantum mekaniği ile birlikte gelişen kuantum teknolojilerine değinilmiş, günümüzde yaygın olarak kullanılan kriptografik algoritmaları savunmasız bırakacak olan kuantum hesaplama teknolojilerinde yararlanılması muhtemel kuantum bilgisayar çeşitleri ile kriptografi üzerindeki muhtemel etkilerine yer verilmiş ve kuantum anahtar dağıtım yöntemlerinin uygulanarak kuantum bilgisayarların, simülatörlerin ve sensörlerin birbirine bağlandığı iletişim ağını ifade eden kuantum iletişimden bahsedilerek kuantum teknolojilerinin sektörler üzerindeki etkisi incelenmiştir.

Tezin üçüncü bölümünde yeterli bilgi işlem gücüne sahip kuantum bilgisayarın inşası halinde bilgi güvenliğinin korunmasında kullanılması planlanan kuantum güvenli kriptografi ve kuantum anahtar dağıtım yöntemleri hakkında bilgi verilmiştir.

Tezin dördüncü bölümünde kuantum kriptografi alanında yayımlanan standartlar ve rehber dokümanlar incelenmiştir.

Tezin beşinci bölümünde kuantum kriptografi hususunda uluslararası kuruluşların çalışmaları, ülkelerin düzenlemeleri ve uygulamaları ele alınmış, ülkemiz mevzuatı ve uygulamaları hakkında bilgi verilmiştir.

Tezin sonuç bölümünde ise tez kapsamında ele alınan konular değerlendirilerek ülkemiz için öneriler sunulmuştur.

1. KRİPTOGRAFİ

Bu bölümde kriptografi kavramı, kriptografinin geçmişten günümüze gelişimi ve kullanım alanları ele alınmıştır.

1.1. Kriptografi Kavramı

Kriptografi, köken olarak Yunanca "gizli, saklı" anlamına gelen *kryptos* ve "yazmak" anlamına gelen *graphein* sözcüklerinden türetilmiş olup bilginin yetkisiz kişilerce anlaşılmaz hale getirilmesinde kullanılan matematiksel tekniklerdir (Grindlay, 2003). Tarihsel süreçte askeri ve diplomatik iletişimde hassas mesajların gizliliğini korumak için kullanılan kriptografi, bilgi ve iletişim teknolojilerinin gelişmesi ile birlikte hassas bilgilerin güvenilmeyen ortamlarda iletiminin yaygınlaşması sonucu yalnızca organizasyonlar için değil bireyler için de yaygın olarak kullanılan bir uygulama haline gelmiş, şifreleme ve şifre çözme eylemlerinden çok daha fazlasını ifade etmeye başlamıştır. Zaman içerisinde hassas bilgilerin korunmasının yanı sıra mesajın, göndericisinin ve alıcısının kimlik doğrulamasının gerçekleştirilmesinde, mesaj bütünlüğünün korunmasında ve mesaj iletiminin inkâr edilemezliğinin sağlanmasında da kullanılmaya başlanmış hem saklanan hem de aktarılan bilginin korunmasında kullanılan teknikleri ve uygulamaları ifade eder hale gelmiştir.

1.2. Kriptografinin Tarihçesi

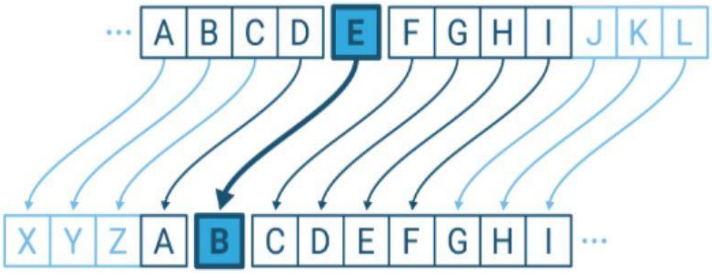
Tarih boyunca yaşanılan dönemin imkanları çerçevesinde kriptografik yöntemler geliştirilmiş olup yazının icadı, matematik ve bilişim teknolojilerinin gelişimi ile birlikte şifreleme yöntemleri ile aygıtlardaki değişim hızlanarak kullanım yaygınlaşmıştır.

Kriptoloji tarihinin milattan önce 1900 yıllarına dayandığı düşünülmekle birlikte bir kâtibin Mısır'daki efendisinin hayatını anlatmak için standart dışı hiyeroglif sembolleri kullanarak yazdığı yazıtlar bilinen en eski şifreleme girişimi olarak kabul edilmektedir. Milattan önce 1500'den kalma ve çömlek yapımının sırlarını anlatan

şifrelenmiş bir Babil çivi yazısı tableti ise şifrelemenin Mezopotamya bölgesinde oluşmuş olabileceğini göstermektedir (Tattersall, 1999).

Kriptografinin ilk önemli kullanımının ise Roma imparatoru Jül Sezar'ın komutanlarıyla iletişim kurmak için geliştirmiş olduğu ve "Sezar Şifrelemesi" olarak da bilinen yer değiştirme algoritmasının olduğu düşünülmektedir. Şekil 1.1'de gösterilen bu şifreleme yönteminde iletilmek istenen mesajdaki harfler, mesajda belirtilen anahtar sayı kadar ileri götürülmekte ve bulunan harf ile yer değiştirilerek şifreleme işlemi gerçekleştirilmektedir (Cohen, 1995). Bu şifreleme yöntemi Büyük Roma Ordusu tarafından yüzlerce yıl boyunca kullanılmış olup filozof ve matematikçi olan El-Kindi'nin bulduğu "alfabe frekans analizi" ile kırılmıştır (Al-Ehwany, 1961).

Şekil 1.1. Sezar Şifrelemesi



Kaynak: (IBM, 2024)

Milattan önce 5 inci yüzyılda ise yer değiştirme algoritması Spartalılar tarafından geliştirilen farklı bir sistem ile kullanılmıştır. Şekil 1.2'de gösterilen bu sistemde, belirli bir kalınlıktaki ahşap silindir etrafına sarılan papirüs veya deri bant üzerine gizli mesaj yazılmakta ve ardından çözülerek alıcıya iletilmekte; kullanılan silindirin çapı ise metnin şifrelenmesi ve çözülmesi için bir anahtar görevi görmekteydi (Sahinaslan, 2019).

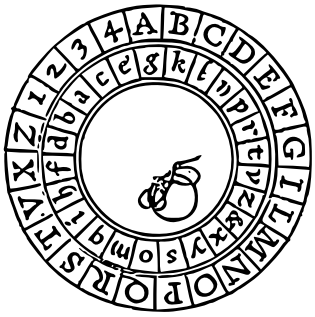
Şekil 1.2. Spartalılar Tarafından Kullanılan Scytale

Kaynak: (Wikipedia, Scytale, 2024)

Milattan sonra 600'lü yıllarda ise şifrelenmiş metnin çözümünü bulmayı hedefleyen kriptanaliz çalışmaları yoğunluk kazanmış; Abdurrahman el-Halil İbn-i Ahmed'in Bizans imparatoru tarafından gönderilen Yunanca bir şifreli mektubun çözümünü veren "Kitab-ül Muamma" adlı eseri ile ilk kriptanaliz tekniklerini açıklayan "Kriptografik Mesajların Şifresini Çözmek İçin El Yazması" adlı bir kitap yazan El-Kindi tarafından keşfedilen frekans analizi yöntemi ile birlikte, kriptanalizinde istatistiksel olarak anlamlı sonuçlar elde edilebilen şifreleme yöntemlerinin tamamı kolaylıkla kırılabilir hale gelmiştir (Singh S. , 2000).

1467'de Leon Battista Alberti tarafından şekil 1.3'te gösterilen iç içe geçmiş iki diskten ve yirmi dört hücreden oluşan bir kriptografik cihaz geliştirilerek tek alfabeli şifreleme sistemlerinden çok alfabeli şifreleme sistemlerine geçiş sağlanmıştır (Babaoğlu, 2009).

Şekil 1.3.Alberti Diski



Kaynak: (Wikipedia, 2024)

16 ncı yüzyılda Blaise de Vigenere tarafından bir anahtar kelime kullanılarak düz metnin karakterlerini farklı miktarlarda kaydıran ve bu yönüyle Sezar şifrelemesinin bir üst modeli olarak kabul edilen şekil 1.4'te yer verilen "vigenere karesi" yöntemi geliştirilerek frekans analizi yöntemi ile iletilmek istenen mesajın deşifre edilmesini zorlaştıran ve uzun yıllar boyunca kırılması imkansız olarak görülen bir yöntem geliştirilmiştir (Raggo & Hosmer, 2013).

Şekil 1.4. Vigenere Karesi

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

Kaynak: (Wikipedia, 2024)

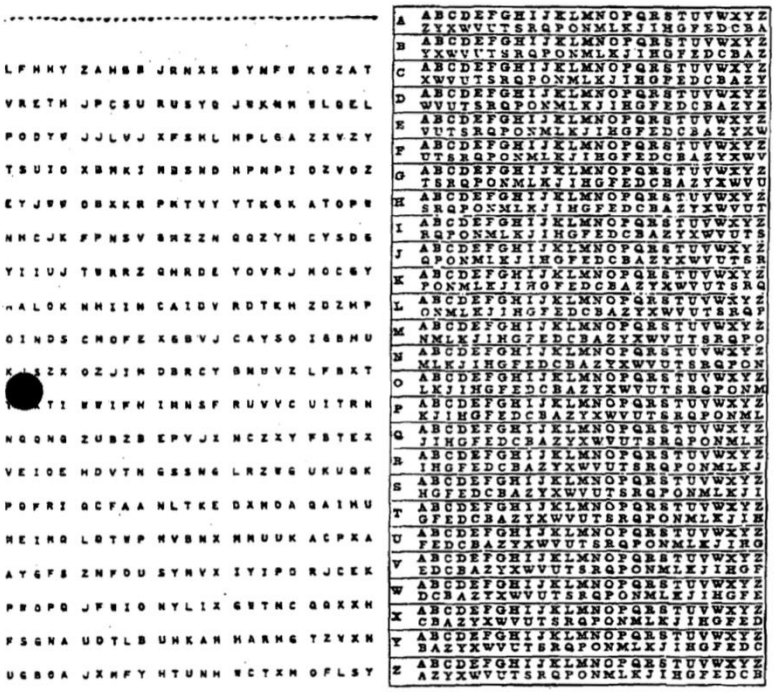
1854 yılında Charles Wheatstone, harflerin çiftler halinde kodlandığı (digraphic) ve sonucun her iki harfe bağlı olduğu; bu sebeple tek alfabeli istatistiksel analiz yöntemlerinin uygulanamadığı ve monoalfabetik bir şifrelemeye kıyasla çözülmesini zorlaştıran bir teknik geliştirmiştir (Britannica, Playfair Cipher, 2023).

1863 yılında ise Friedrich Kasiski, Vigenere şifreleme metodunun kriptanalizi için bir yöntem geliştirmiştir. Kasiski testi olarak da bilinen bu yöntem ile şifreli metinde sık tekrarlanan heceler arasındaki mesafeden yola çıkılarak anahtar uzunluğu tahmin edilmektedir (Sahinaslan, 2019).

1917 yılında Gilbert Vernam, Vernam şifrelemesi veya tek kullanımlık şerit olarak da ifade edilen, Amerikan Ulusal Güvenlik Ajansı (National Security Agency- NSA) tarafından kriptolojideki en büyük buluşlardan biri olarak nitelendirilen ve dünyanın ilk kırılmaz şifresi olarak bilinen bir şifreleme yöntemi geliştirmiştir. Vernam

şifrelemesinde; anahtar, şifrelenecek metin ile aynı boyutta olmalı ve rastgele sayı üretecinden yararlanılarak yalnızca tek seferlik üretilip kullanılarak şifreleme işlemi gerçekleştirilmelidir. Bu şifreleri kırmak imkansız olsa da benzersiz bir anahtar oluşturabilmek için gerekli olan rastgele sayı üretiminin zorluğu ve güvenli anahtar dağıtım problemi sebebiyle kullanım alanı yaygınlık kazanmamıştır (Dubrawsky, 2007). Şekil 1.5'te sağ tarafında bulunan tablonun sol tarafında bulunan karakterleri anahtar olarak kullanarak düz metin ve şifreli metin arasında dönüşüm işleminin gerçekleştirilebildiği bir tek kullanımlık şerit formatının örneğine yer verilmektedir.

Şekil 1.5. Tek Kullanımlık Şerit Formatı



Kaynak: (Wikipedia, 2024)

Alman mühendis Arthur Scherbius tarafından tasarlanan ve "muamma, bilmece" anlamına gelen kripto cihazı Enigma, İkinci Dünya Savaşı sırasında Alman ordusunun en yaygın kullandığı şifreleme cihazı olmuştur. Şekil 1.6'da yer verilen daktilo benzeri, rotorlu, elektromekanik bir şifreleme cihazı olan Enigma, 26 elemanlı bir alfabede permütasyona dayalı bir şifreleme işlemi gerçekleştirmekteydi. İngiliz kriptanalist Alan Turing tarafından geliştirilen, rotorların oluşturduğu permütasyonları olası adaylar arasından eleme yoluyla bulan ve aynı anda altı Enigma cihazını taklit

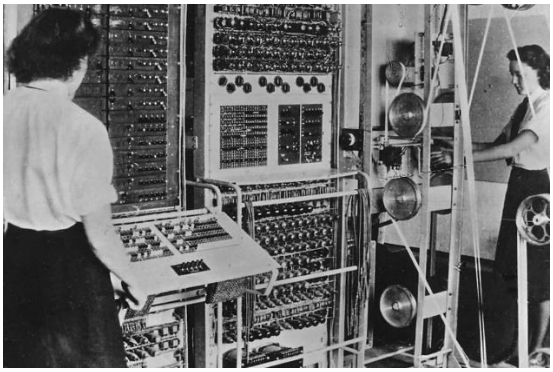
edebilen “Bombe” isimli cihaz ise savaşın seyrini değiştiren ve bilinen ilk kriptanaliz cihazıdır (Kara, 2009).

Şekil 1.6. Enigma Cihazı

Kaynak: (Britannica, 2024)

Enigma kodlarının yanı sıra yüksek rütbeli Alman askerlerinin ve kurmayların kullandığı 12 rotorlu Lorenz SZ-40 Schlüsselzuzatz ile gönderilen mesajların çözümü için ise şekil 1.7’de yer verilen delikli şerit kağıtlar yardımıyla programlanabilen ve dünyanın ilk dijital elektronik bilgisayarı olan “Colossus” İngilizler tarafından üretilmiş olup söz konusu kriptanaliz cihazları sayesinde savaşın en az iki yıl kısaldığı birçok tarihçi tarafından kabul görmektedir (Kara, 2009).

Şekil 1.7. İlk Dijital Bilgisayar Colossus



Kaynak: (Britannica, 2024)

1929'da Lester Hill tarafından yayınlanan, klasik bir simetrik anahtar şifreleme yöntemi olan Hill Şifreleme metodunda ise düz metin bir tamsayı değerleri vektörü olarak temsil edilmekte ve bu vektör şifreleme anahtarı olan kare anahtar matrisi ile çarpılarak şifreleme işlemi gerçekleştirilmektedir (Stallings, 2011).

Dijital bilgisayar kullanımı ile daha karmaşık şifreleme işlemleri gerçekleştirilmeye başlanmış, anahtar dağıtım problemi sürecin en zayıf halkası haline gelmiştir. Kriptografide çığır açan buluş ise 1975 yılında, Whitfield Diffie tarafından günümüzde açık anahtarlı kriptografi olarak bilinen metodun geliştirilmesi olmuştur. Diffie'nin meslektaşı olan Martin Hellman ile birlikte tarafların güvenli olmayan bir hat üzerinde güvenli bir şekilde iletişim kurmalarına ve iletişimlerini şifrelemek için simetrik bir anahtar üzerinde anlaşmalarına izin veren bir algoritma geliştirmişlerdir (Grindlay, 2003).

1977 yılında ise Massachusetts Teknoloji Enstitüsünden üç araştırmacı, kullanıcıya gönderilen mesajın alıcının açık anahtarı ile şifrelendiği, alıcının gizli anahtarını kullanarak mesaj şifresini çözdüğü Rivest, Shamir ve Adleman (RSA) isimli asimetrik şifreleme yöntemi üzerine ilk makalelerini yayımlamıştır. RSA şifrelemesi ile birlikte ilk kez gönderici ve alıcının önceden paylaşılan bir gizli anahtar oluşturmasına ihtiyaç duyulmadan güvenli olmayan bir hat üzerinde iletişim kurabilmesi sağlanmıştır (Grindlay, 2003).

Asimetrik şifrelemenin keşfinden sonra ise, özellikle e-posta şifrelemesinde ve mesaj kimliğinin doğrulanmasında kullanılan PGP (Pretty Good Pivacy-PGP), hem donanım hem de yazılım açısından verimli olacak şekilde tasarlanan AES gibi birçok modern kriptografik algoritma geliştirilmiş olup günümüzde yeni yöntemler ve çözümlerle birlikte gelişimi devam etmektedir (Grindlay, 2003)

1.3. Kriptografi ve Bilgi Güvenliği

Kriptografi, hem iletişim hem de depolama sürecinde; bilginin yalnızca yetkili kişilerce okunmasına imkan sağlayan **gizlilik**, yalnızca yetkili kişilerce veri eklenmesi,

silinmesi ve değiştirilmesine imkan sağlayan **bütünlük**, iletişimi kuran tarafların kimliğinin belirlenmesini ve doğrulamasını sağlayarak gerçekleştirilen işlemin gizliliği ile bütünlüğü için güvence sağlayan **kimlik doğrulama** ve işlemde yer alan tarafın işleme katılımını inkar etmesini engelleyen **inkar edilemezlik** özelliklerinin korunması hedeflerine ulaşılmasını amaçlamaktadır (Caceres, Robichaux, & D., 2009). Bu doğrultuda veri güvenliğini sağlayabilmek amacıyla kriptografik işlemler vasıtasıyla gerçekleştirilen çeşitli güvenlik hizmetleri kullanıma sunulmuştur.

- **Veri Gizliliği:** Verinin gizli kalmasını sağlayan ve yetkisiz kişilerce okunmasını engelleyen bu güvenlik hizmetinde, verilerin bir şifreleme algoritması aracılığıyla şifreli metne dönüştürülmesi amacıyla dosya düzeyinde, oturum katmanında veya bağlantı düzeyinde şifreleme işlemi gerçekleştirilebilmektedir.
- **Veri Bütünlüğü, Doğruluğu ve İnkâr Edilemezliği:** İletilen verinin şifrelenmiş olması, söz konusu verinin silme veya değiştirme gibi işlemlere maruz kalarak manipüle edilmediğini ispatlamamaktadır. Bu sebeple güvenilirliğin sağlanabilmesi amacıyla yetkili bir kaynaktan geldiklerinin ve değiştirilmediklerinin kanıtlanması gerekmektedir. Bu doğrultuda aşağıda kısaca açıklanan ek kriptografik işlemler gerçekleştirilmektedir.
    - Mesaj Özetleme (Hash/ Message Digest): Kimlik doğrulama için kullanışlı olan bu kriptografik yöntem, var olan bir özetin daha sonraki tarihte yeni oluşturulmuş bir özet ile karşılaştırılmasını ve özetlerin aynı olması halinde verilerin değiştirilmemiş olduğunun anlaşılmasında kullanılmaktadır.
    - Mesaj Doğrulama Kodu (Message Authentication Code): Bu yöntemde mesajın iletildikten sonra değiştirilmediğinden emin olabilmek için gizli bir anahtar ile şifreleme algoritması kullanılarak mesaj doğrulama kodu üretilmekte; iletilen mesajın sonuna eklenen mesaj doğrulama kodunun alıcının gönderici ile aynı algoritmayı kullanarak ürettiği kod ile eşleşmesi halinde mesajın değiştirilmediği ispatlanmış olmaktadır.
    - Özet Tabanlı Mesaj Doğrulama Kodu (Hash Message Authentication Code): Mesaj doğrulama kodu yöntemi ile aynı şekilde kullanılan bu kriptografik yöntemde farklı olarak şifreleme algoritması yerine mesaj özetleme algoritmaları kullanılmaktadır.
    - İmzalama/Doğrulama:

- İmzalama işleminde elektronik imza[1] adı verilen kimlik doğrulama değeri gönderici ve alıcının iki farklı anahtara sahip olduğu asimetrik anahtarlı şifreleme algoritması ile üretilerek aşağıda yer alan aşamalar sırasıyla gerçekleştirilir.
  - İletilmek istenen verinin bütünlüğü ile doğruluğunun sağlandığının kanıtlanabilmesi amacıyla gönderici tarafından anahtarsız algoritmalar kullanılarak imzalanacak veriye ait bir özet değer oluşturulur.
  - Göndericiye ait özel anahtar kullanılarak oluşturulan özet şifrelenir ve elektronik imza oluşturulur.
- Doğrulama işlemi ise aşağıdaki aşamalarda gerçekleşir:
  - Elektronik imzanın şifresi göndericiye ait açık anahtar kullanılarak çözülür ve gönderici tarafından şifrelenen birinci mesaj özeti değerine ulaşılır.
  - Gönderici tarafından iletilen veriler alıcı tarafından aynı anahtarsız algoritma kullanılarak yeniden özetlenir ve ikinci bir özet değerine ulaşılır.
  - İki özetin eşleşmesi halinde imza geçerli olur.

- **Anahtar ve Rastgele Sayı Üreteçleri:** Güvenlikle ilgili birçok işlevde olduğu gibi kriptografik anahtar üretimi de rastgele sayı üretimine dayanmakta ve oluşturulan rastgele sayıların kriptografik olarak yeterince güçlü olmaması halinde işlev saldırıya açık hale gelmektedir.
- **Finansal Kişisel Kimlik Numaraları (Personal Identification Number-PIN):** Kişisel Kimlik numarası (PIN) oluşturma ve işleme de kriptografik işlem olarak kabul edilmektedir. PIN, bir kuruluş tarafından bir bireye atanan benzersiz bir numara olup genellikle finansal kuruluşlar tarafından müşterilere atanarak müşteriyle ilişkili verilerin karşılaştırılmasında kimlik kanıtı sağlaması için kullanılmaktadır.
- **Anahtar Yönetimi:** Kriptografik anahtarların güvenli ortam dışına gönderilmeden veya saklanmadan önce şifrelenmesini sağlayan anahtar şifreleme, anahtarın güvenli bir şekilde iletimini sağlayan anahtar dağıtım

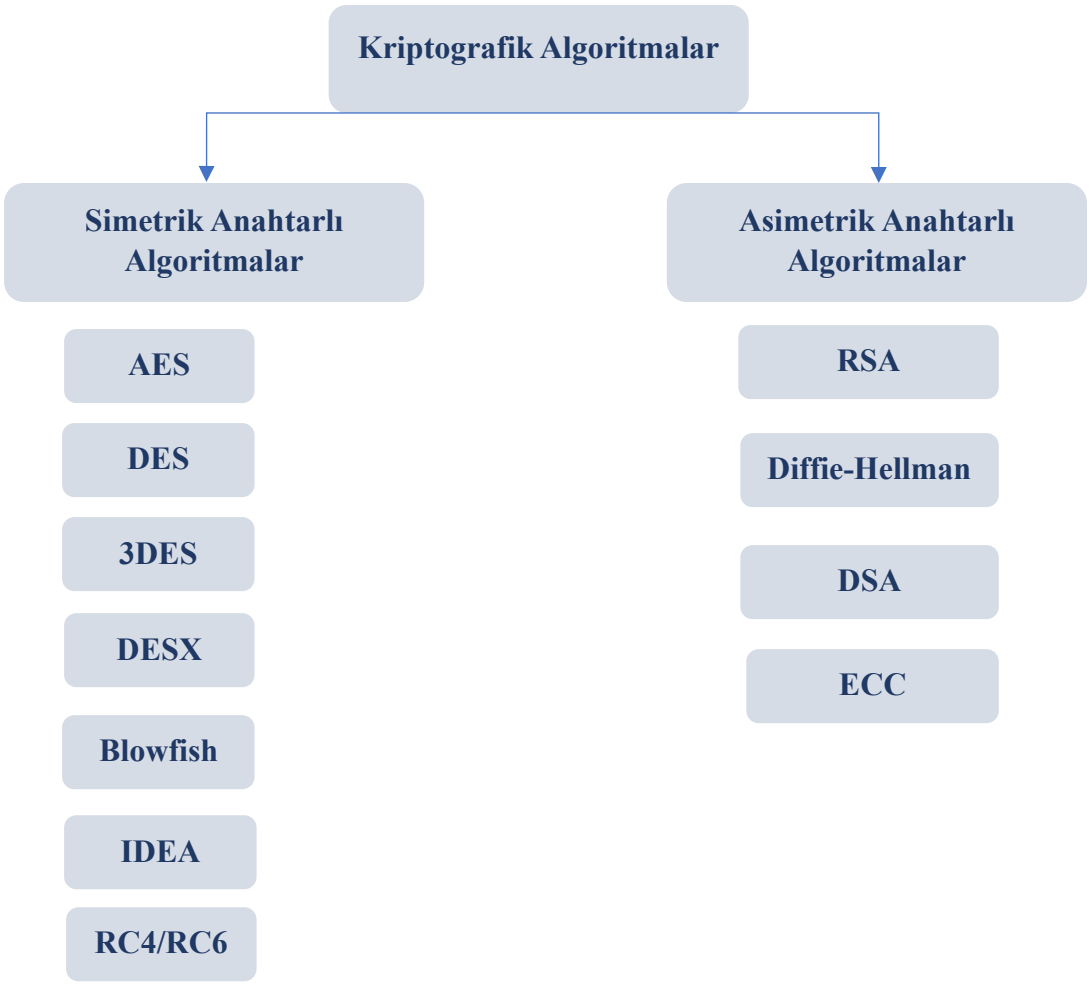
[1] Bu tez çalışmasında yabancı dilde yazılan kaynaklarda "digital signature" veya birebir Türkçe ifadeyle "dijital imza" olarak belirtilen terim yerine ülkemizde yürürlükte olan mevzuatta tanımlandığı şekliyle "elektronik imza" ifadesi kullanılmıştır.

protokolleri (simetrik ve asimetrik anahtar dağıtım protokolleri) ve kriptografik anahtarların güvenli bir şekilde saklanmasını ve işlenmesini sağlayan (key-encrypting keys-anahtar şifreleme anahtarı vb.) yöntemler bütünüdür (IBM, 2023).

1.4. Modern Kriptografik Teknikler

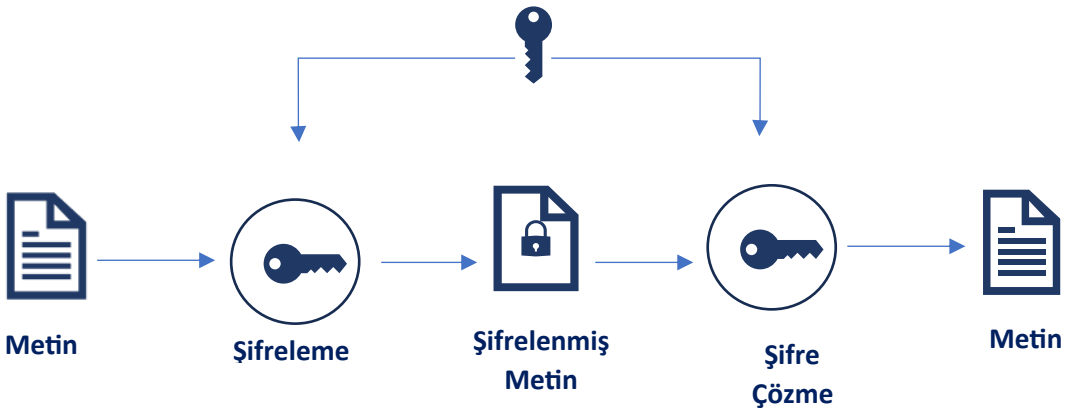
Şifreleme işlemleri için kullanılan anahtarın özellikleri ve çeşidine bağlı olarak simetrik ve asimetrik kriptografi olmak üzere iki çeşit şifreleme algoritması bulunmaktadır. Simetrik kriptografide, gönderici ve alıcı arasında hem şifreleme hem de şifre çözme için gizli ve tek bir anahtar kullanılırken; açık anahtarlı şifreleme olarak da bilinen asimetrik kriptografide şifreleme ve şifre çözme işlemi gönderici ile alıcı arasında anahtar paylaşımı olmaksızın açık anahtar ve özel anahtarın birlikte kullanımı ile gerçekleştirilir.

Şekil 1.8. Kriptografik Algoritmalar



1.4.1. Simetrik Şifreleme Algoritmaları

Şekil 1.9. Simetrik Anahtarlı Şifreleme



Şekil 1.9'da genel işleyişine yer verilen ve gizli anahtarlı şifreleme olarak da bilinen simetrik şifreleme algoritmaları, aynı gizli anahtarın hem gönderici hem de alıcı tarafından paylaşıldığı, güvenli olmayan bir kanal üzerinde veri gizliliğini sağlamak için göndericinin veriyi şifreleyerek alıcıya ilettiği, alıcının da aynı anahtarı kullanarak şifrelenmiş metni çözebildiği şifreleme sistemleridir. Bu algoritmalar ile büyük miktarda verinin kısa sürede şifrelenmesi ve güçlü bir anahtar ile kırılması zor veriler oluşturulması mümkün olmasına rağmen iki tarafın güvenli bir şekilde iletişim kurabilmesi için gizli anahtarın güvenli bir şekilde paylaşılması zorunluluğunun bulunması sistemin en büyük dezavantajı olarak görülmektedir (Settia, 2010).

Simetrik anahtarlı şifreleme algoritmaları blok şifreleme ve dizi (akan) şifreleme algoritmaları olmak üzere ikiye ayrılmaktadır. Blok şifreleme algoritması ile şifrelenmemiş metindeki veriler sabit boyuttaki bloklar halinde işlenerek şifrelenmektedir. Genellikle 64 bitlik bloklar kullanılmakla birlikte seçilen algoritmaya bağlı olarak daha büyük veya daha küçük bloklar tanımlanabilmektedir. Dizi şifreleme algoritmasında ise açık metinde yer alan her bir karakter 1 bit olarak kabul edilerek şifreleme işlemi gerçekleştirilmektedir (Andres, 2014).

Kullanımda olan şifreleme algoritmalarının büyük çoğunluğunda, dizi şifreleme algoritmalarından daha yavaş olmalarına rağmen aynı anda mesajın daha büyük

bloklarında çalışabilmeleri ve daha verimli olmaları sebebiyle blok şifreleme algoritmaları kullanılmaktadır. Genel olarak, blok şifreleme algoritmalarının dosya şifrelemesi veya protokol başlığında mesaj boyutunun bildirildiği durumlarda olduğu gibi mesaj boyutunun sabit olduğu veya önceden bildirildiği durumlarda; dizi şifreleme algoritmalarının ise boyutu bilinmeyen bir veriye sahip olunduğu veya verilerin bir akış içerisinde olduğu durumlarda kullanımı tercih edilmektedir (Andres, 2014).

AES (Advanced Encryption Standard-AES), DES (Data Encryption Standard-DES), 3DES (Triple-DES-3DES), Blowfish, IDEA (International Data Encryption Algorithm-IDEA), Rivest Ciphers (RC2, RC4, RC6) şifreleme ve şifre çözme işleminin hızlıca gerçekleştirilebildiği, büyük hacimli verilerin şifrelenme sürecinde günümüzde yaygın olarak kullanılan simetrik şifreleme algoritmalarına birer örnektir (Kessler, 2015).

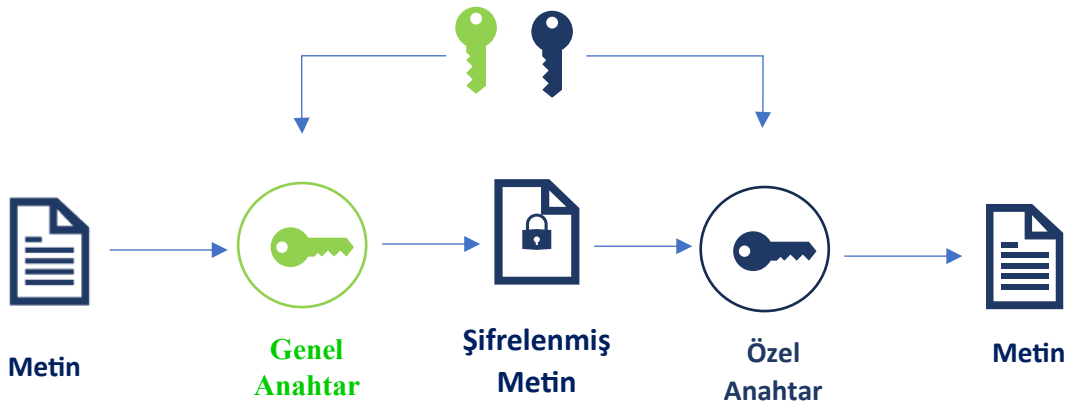
Tablo 1.1. Simetrik Anahtarlı Algoritmaların Karşılaştırması

Algoritma	Anahtar Uzunluğu	Blok Boyutu	Özellikleri
AES	128,192,256 Bit	128 Bit	Yüksek Güvenlik DES algoritmasının ikamesi Hızlı Şifreleme
DES	64 Bit	64 Bit	Yeterince Güçlü Değil Yavaş Şifreleme
3DES	112, 118 Bit		Yeterli Güvenlik Seviyesi Oldukça Yavaş Şifreleme
IDEA	128 Bit	64 Bit	Donanım ve Yazılım Üzerinde Uygulanması Kolay Yüksek Hızlı Şifreleme Yüksek Güvenlik
Blowfish	32-448 Bit	64 Bit	Yüksek Güvenlikli Hızlı Şifreleme
RC4	Değişken	20-2048 Bit	SSL Kullanımı İçin Hızlı Şifreleme Özelliği
RC6	128-256 Bit	128 Bit	Yüksek Güvenlik

Kaynak: (Singh & Patro, 2019), (Princy, 2015), (Yang, Piao, & Zhang, 2007)

1.4.2. Asimetrik Şifreleme Algoritmaları

Şekil 1.10. Asimetrik Anahtarlı Şifreleme



1976 yılında Stanford Üniversitesi profesörü Martin Hellman ile öğrencisi Whitfield Diffie tarafından yayımlanan makalede[2]; şekil 1.10'da yer verilen ve gönderici ile alıcı arasında gizli bir anahtar paylaşımı olmadan, güvenli olmayan bir iletişim kanalı üzerinden güvenli iletişim kurulabilmesine olanak sağlayan iki anahtarlı bir kripto sistemi tanımlanmıştır. Söz konusu makalede tanımlanan ve açık anahtarlı şifreleme algoritmaları olarak da adlandırılan asimetrik şifreleme algoritmalarında, anahtarlardan biri genel anahtar olarak belirlenerek şifrelenmemiş metni şifrelemek için kullanılmakta ve bir ağda mesaj şifreleme için güvenlik kimlik bilgilerini ve genel anahtarları yayımlama görevi bulunan sertifika yetkilileri aracılığıyla veya başka gruplardaki üyelerle dosya paylaşmak için kullanılabilen dizin sunucular (public directory) aracılığıyla kullanıcılara duyurulabilmekte (S. F. Al-Janabi, 2012); ikinci anahtar ise özel anahtar olarak belirlenerek şifrelenmiş metnin şifresinin çözülmesi amacıyla kullanılmakta ve başka bir tarafa açıklanmasına izin verilmemektedir. Diğer bir deyişle, göndericinin alıcıya ilettiği veriler genel anahtar ile şifrelenirken iletilen şifrelenmiş verinin şifresinin çözülebilmesi için alıcının özel anahtarı kullanılmakta; şifreleme ve şifre çözme eylemleri için farklı anahtarlar kullanılması sebebiyle asimetrik şifreleme algoritmalarında anahtarın gizli bir şekilde dağıtılmasına ihtiyaç

[2] Whitfield Diffie ve Martin E. Hellman, "New Directions in Cryptography", *IEEE Transactions on Information Theory*, Cilt 22, No 6, 1976

duyulmamakta ve bu sayede simetrik şifreleme algoritmalarının en büyük dezavantajı olarak görülen anahtar dağıtım problemi ortadan kaldırılmaktadır (Kessler, 2015).
Asimetrik anahtar altyapısı, kullanıcıların ağ üzerindeki iletişimlerinin ve işlemlerinin güvenliğini sağlamak için kullanılan yazılım, şifreleme teknolojileri ve hizmetlerin birleşimi olup asimetrik anahtarlı kriptografinin, sertifika yetkililerinin ve elektronik sertifikaların kusursuz bir ağ güvenlik mimarisine entegrasyonundan oluşmaktadır (NIST, 2021). Asimetrik anahtar altyapısında yer alan roller ve bileşenlerden:

- **Son kullanıcılar:** Sistemi kullanan, sertifika yetkilisinden sertifika talebinde bulunan ve sertifikalı anahtarları ile sertifikaları asimetrik anahtar altyapısına sahip uygulama hizmetlerinde kullanan tarafları,
- **Kayıt yetkilisi**: Son kullanıcının kimliğini doğrulamak ve genel anahtar sertifikası almaya yetkili olup olmadığını belirlemekle görevli bileşeni,
- **Sertifika yetkilisi**: Bir ağda, mesaj şifreleme için güvenlik kimlik bilgilerini ve genel anahtarları yayınlayan ve yöneten, elektronik sertifika talebinde bulunan kişi tarafından sağlanan bilgileri doğrulamak için kayıt yetkilisini kontrol eden, kayıt yetkilisinin bilgileri doğrulaması halinde başvuru sahibine sahibinin adını, genel anahtarını, sertifikanın son kullanma tarihini ve genel anahtar sahibi hakkındaki diğer bilgileri içeren elektronik sertifikaları veren, aynı zamanda bu sertifikaların dağıtımından ve iptalinden sorumlu güvenilir üçüncü tarafları,
- **Elektronik sertifikalar:** Kullanıcısına kimlik kanıtı sunan, kullanıcının imza doğrulama verisini ve kimlik bilgilerini birbirine bağlayan elektronik kayıtları,
- **Bilgi deposu:** Sertifikaların, sertifika iptal durum kayıtlarının ve diğer sertifika işlemleri ile ilgili bilgilerin yayımlandığı web sunucular, dizin sunucular gibi veri saklama ortamlarını,

ifade etmektedir (S. F. Al-Janabi, 2012).

Asimetrik anahtar altyapısı, sisteminde yer alan sertifika yetkilisinin hem göndericiyi hem de alıcıyı tanımlaması ve genel anahtarlarının orijinal olduğunu onaylaması sayesinde kullanıcıların birbirini tanımasına veya birbirine güvenmesine gerek kalmaksızın iletişim kurmasını mümkün kılmaktadır. Sertifika yetkililerince sağlanan elektronik sertifikalar ile kullanıcıların kimlik doğrulamasının gerçekleştirilebilmesinin yanı sıra asimetrik anahtarlı şifrelemenin temelini oluşturan

ve göndericiye ait genel anahtar ile şifrelenen verinin yalnızca alıcıya ait özel anahtar ile deşifre edilebilir olması hem kimlik doğrulama hem de işleme katılımın inkar edilemezliği özelliklerini sunarak güvenli iletişimin kurulmasına olanak sağlamaktadır (NIST, Digital Signature Standard (DSS), 2023).

Asimetrik şifreleme algoritmalarının güvenliği, büyük asal sayıları çarpanlarına ayırmanın zorluğu ile ayrık logaritma problemi gibi tek yönde hesaplanması basitken ters yönde hesaplamanın çok zor olduğu "tek yönlü fonksiyon" olarak adlandırılan algoritmalar üzerine inşa edilmiştir. Dolayısıyla, asimetrik şifreleme algoritmaları son derece güvenli olarak kabul edilmekle birlikte büyük verilerin şifrelenmesi ve şifrelerinin çözülmesi işlemlerinde oluşan hesaplama ek yükü nedeniyle sistemin yavaş çalışmasına sebep olabilmektedir (Mohamed, 2020).

Birçok yazılım ürününün yanı sıra güvenli anahtar değişimi, kimlik doğrulama ve elektronik imza algoritmalarında kullanılan, RSA algoritması, Diffie-Hellman algoritması, ElGamal algoritması, elektronik imza algoritması (Digital Signature Algorithm-DSA) ile RSA ve DSA'nın sağladığı güvenliği daha kısa parametreler ve dolayısıyla daha kısa sürelerde sağlayan eliptik eğri algoritmaları (Eliptic-curve cryptography-ECC) günümüzde yaygın olarak kullanılan asimetrik şifreleme algoritmalarına birer örnektir (Kessler, 2015).

Tablo 1.2. Asimetrik Anahtarlı Algoritmaların Karşılaştırması

Kriptografik Algoritma	**Anahtar Uzunluğu (Bit)**	**Güçlü Yanları**	**Zayıf Yanları**
RSA	1024 2048 3072 4096	Kısa hesaplama süresi	Şifreleme ve imzalama işlemleri için aynı anahtarın kullanımı Farklı kullanıcılar için aynı/ortak bileşenlerin kullanımı
Diffie-Hellman	1024 3072	Zorlu ayrık logaritma problemlerini çözebilir Bilgi transferinde değil anahtar oluşturma ve paylaşımında kullanılır	Üstel işlem zorluğu Kimlik doğrulama eksikliği

Tablo 1.2. Asimetrik Anahtarlı Algoritmaların Karşılaştırması (devamı)

DSA	512 ile 1024 arasında 64'ün katları	Kimlik doğrulama, veri bütünlüğü, inkar edilmezlik sağlar	Oluşturulan imza değerinin gizliliği ve eşsizliği kritik öneme sahiptir
ECC	160,224,256	Daha küçük anahtar boyutu, Depolama maliyeti küçük, İletim süresi kısa, RSA'dan 15 kat daha hızlı, Daha az güç tüketimi	Şifrelenmiş metnin boyutunu artırır, Algoritmanın karmaşıklığını artıran çok zor denklemlere dayanmaktadır
ElGamal	1024 2048	Yüksek performans Düşük güç tüketimi Yazılım ve donanım entegrasyonunda hızlı ve verimli	Şifrelenmiş metnin boyutunu artırır, Algoritmanın güvenliği yalnızca tek bir rastgele sayının kullanımına bağlıdır

Kaynak: (Singh & Chauhan, 2017), (F. Mallouli, 2019)

1.4.3. Anahtarsız Algoritmalar

Tek yönlü fonksiyonlar olarak da adlandırılan anahtarsız algoritmalar, şifreleme işleminde girdi olarak anahtar yerine rastgele uzunluktaki metinleri alarak orijinal mesaja dayalı sabit uzunlukta bir özet değer oluşturan, tek başına kullanımının amaçlanan güvenliği sağlamada yetersiz kalması sebebiyle diğer algoritmalara yardımcı olarak kullanılan algoritmalardır (Andres, 2014).

Uygulamalar, şifrelenmemiş metin mesajları veya işletim sistemi dosyaları üzerinde kullanılabilen bu algoritmalar orijinal mesajın içeriğini veya diğer özelliklerini görebilmek için değil, iletilen mesajın değiştirilip değiştirilmediğini belirlemek için kullanılmaktadır. Bu sebeple anahtarsız algoritmalar veri gizliliğini sağlarken veri bütünlüğünü garanti etmemektedir. Mesaj özetinin iletilen mesaj ile birlikte gönderildiği durumlarda ise, alıcı, aynı algoritmayı kullanarak mesajı tekrar

özetlemekte, gönderilen özet ile kendi özetini karşılaştırmakta ve özetlerin eşleşmesi halinde mesajın değiştirilmediği ile veri bütünlüğünün sağlandığı sonucuna ulaşabilmektedir (Andres, 2014).

Mesaj Özeti Algoritmaları (Message Digest Algorithms- MDA) ile Ulusal Standartlar ve Teknoloji Enstitüsü (National Istitute of Standards and Technology-NIST) tarafından yayımlanan Güvenli Özet Algoritması (Secure Hash Algorithm- SHA) en yaygın anahtarsız algoritmalar olup asimetrik şifreleme yöntemi ile birlikte kullanılan ve güvenilir zaman damgası mekanizmalarıyla da birleştirilerek gizlilik, kimlik doğrulama, veri bütünlüğü ile inkar edilemezlik özelliklerini sağlayan elektronik imzanın temel unsurları arasında yer almaktadır (Andres, 2014).

1.5. Kriptografinin Kullanım Alanları

Bilgi güvenliğini sağlamak, veri gizliliğini korumak ve kimlik doğrulamanın gerçekleştirilebilmesi amaçlarıyla birçok farklı sektörde ve uygulamada kriptografik protokoller kullanılmaktadır. Bu bölümde kriptografinin temel alınarak bilgi güvenliğinin sağlandığı bazı uygulamalara yer verilmiştir.

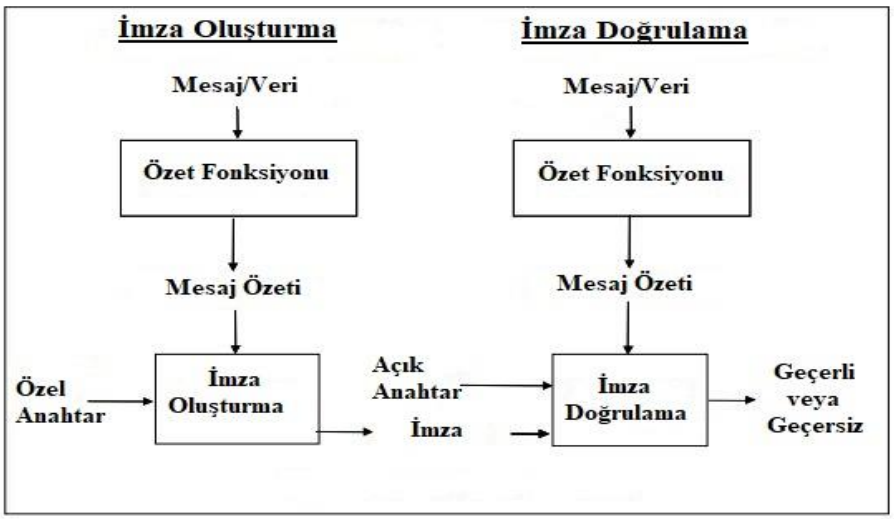
1.5.1. Elektronik İmzalar

Elektronik imza, imza sahibinin mesajı imzaladığına dair güvence sunan, imzalanan mesajın iletimi aşamasında bütünlüğünün ve içeriğinin değiştirilmediğini garanti eden, çeşitli kriterleri sağladığı takdirde ıslak imza ile eşdeğer hukuki sonucu doğuran ve şifreleme işleminin gerçekleştiren algoritmalar vasıtasıyla oluşturulan bir elektronik güvenlik öğesidir.

Elektronik imza algoritmaları, şekil 1.11'de yer verildiği gibi imza oluşturma ve imza doğrulama olmak üzere iki aşamada gerçekleştirilmektedir. Asimetrik şifreleme altyapısının kullanımı sonucu hem göndericinin hem de alıcının özel ve genel olmak üzere iki farklı anahtarı bulunmaktadır. İlk aşama olan imza oluşturma sürecinde; gönderici tarafından iletilmek istenen mesaj oluşturulduktan sonra verinin içeriğinin

ve bütünlüğünün değiştirilmediğinin tespitini sağlayan mesaj özeti algoritmaları uygulanmakta ve göndericinin özel anahtarı kullanılarak elektronik imza oluşturulmaktadır. Sonrasında ise göndericinin metin ile birlikte ilettiği elektronik imza, alıcı tarafından göndericinin genel anahtarı ile deşifre edilerek mesaj özeti değerine ulaşılmakta, elektronik imzanın doğrulanması amacıyla iletilen şifrelenmemiş metin üzerinden mesaj özeti yeniden oluşturulmakta ve elde edilen iki mesaj özeti değeri kıyaslanarak iletilen mesajın doğruluğunun ve bütünlüğünün korunduğu tespit edilmektedir (NIST, 2023).

Şekil 1.11. Elektronik imza oluşturma ve doğrulama süreci



Kaynak: NIST, 2023

Elektronik imzada asimetrik anahtar altyapısı kullanılmakta olup mesajı imzalayan kişinin kimliğinin tespiti için bir sertifika ve bu sertifikayı düzenleyen üçüncü bir kişiye ihtiyaç duyulmaktadır. Sertifika yetkilisi, varlığın kimliğini ve diğer özniteliklerini bir genel anahtarla ilişkilendiren elektronik sertifikalar yayınlayarak farklı varlıklar arasında güvenilir üçüncü taraf hizmeti sağlamada kritik bir rol sahibi olmasının yanı sıra sertifikanın güvenilirliğini kaybetmesi veya tehlikeye girmesi durumunda da bilgilendirme yapmak ve sertifika iptal verilerini imzalamaktan da sorumlu tutulmaktadır (NIST, 2023).

1.5.2. İnternet Güvenliği

Kriptografinin diğer bir kullanım alanı ise internet üzerinde güvenli iletişimin sağlanmasıdır. İnternet trafiğinin şifrelenmesi ve verinin güvenli bir şekilde aktarımının sağlanabilmesi amacıyla 1994 yılında web tarayıcıları ve sunucular arasındaki http bağlantılarını güvence altına alan Güvenli Soket Katmanı (Secure Sockets Layer-SSL) protokolü yayınlanmış ve zaman içerisinde gelişerek ve daha güvenli hale gelerek Taşıma Katmanı Güvenliği (Transport Layer Security-TLS) isimli internet standardına dönüşmüştür. TLS, sertifika tabanlı kimlik doğrulama yöntemini kullanarak sunucu ile istemci arasında güvenli iletişimin gerçekleştirilmesine olanak sağlamakta ve temel olarak kayıt ile yönetim protokollerinden oluşmaktadır (Das & Samdaria, 2014).

Hiper-Metin Transfer Protokolü (Hypertext Transfer Protocol-HTTP), web tarayıcıları ile sunucu arasındaki veri alışverişini sağlayan bir protokoldür. Ancak HTTP'nin verileri şifrelememesi sebebiyle veri iletimi sırasında büyük bir güvenlik riski oluşturmaktadır. Bu sebeple SSL/TLS protokolü istemci ve sunucu arasında HTTP yoluyla gönderilen verileri korumak için uygulamaya entegre edilerek kullanılmakta, TLS protokolünün HTTP ile birleşmesi ile oluşan Güvenli Hiper Metin Aktarım İletişim Protokolü (Hypertext Transfer Protocol Secure-HTTPS) protokolü ile güvenli iletişim kurulabilmektedir (Das & Samdaria, 2014).

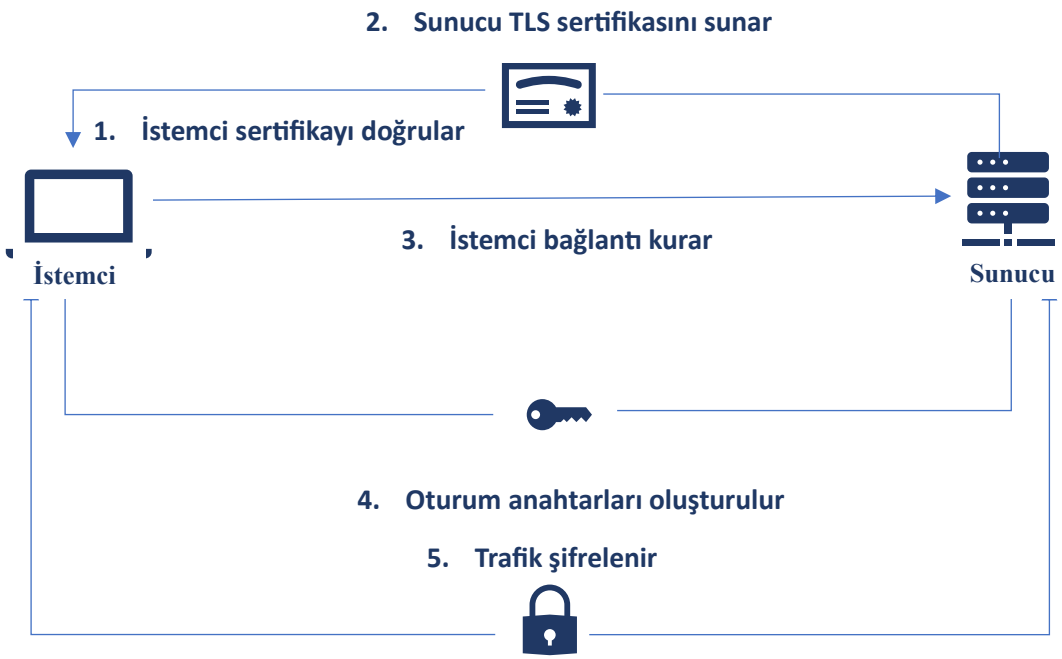
Şekil 1.12'de genel işleyişine yer verilen SSL/TLS özellikli bir uygulamada, istemci öncelikle sunucuya bir merhaba mesajı göndermekte, ardından sunucu anlaşılan parametreleri onayladıktan sonra sunucunun merhaba mesajını sunucunun elektronik sertifikasıyla birlikte istemciye iletmektedir. Sunucunun elektronik sertifikası, sunucunun genel anahtarı, sertifika geçerlilik süresi, sertifika sağlayıcı ve sahibine ilişkin hususlar hakkında bilgi sunmaktadır. İstemci, sunucunun sertifikasını kullanarak sunucu kimliğini doğruladıktan sonra, istemci ve sunucu, SSL/TLS oturumu sırasında değiş tokuş edilen bilgileri şifrelemek/şifresini çözmek ve mesaj bütünlüğünü doğrulamak için kullanılan simetrik şifreleme altyapısındaki oturum anahtarlarını oluşturmaktadır. Sonuç olarak, SSL/TLS özellikli bir uygulama, standart bir simetrik anahtar şifreleme (örn. AES) algoritması kullanarak elektronik sertifika

tabanlı sunucu kimlik doğrulaması, ortak anahtar tabanlı anahtar değişimi ve oturum anahtarı tabanlı veri gizliliği sağlamanın yanı sıra mesaj kimlik doğrulama kodlarının kullanılması yolu ile mesaj bütünlüğü kontrolünü sağlayabilmektedir (Das & Samdaria, 2014).

TLS protokolü, dört farklı alt protokole sahiptir, bu alt protokoller güvenli iletişimin farklı yönlerini ele almaktadır.

- El Sıkışma Protokolü (Handshake Protocol), sunucu ve istemci arasında kimlik doğrulama yöntemlerinin ve şifreleme algoritmalarının belirlenerek güvenli bir iletişim kanalının oluşturulması için kullanılmaktadır.
- Şifre Değişim Özelliği Protokolü (Change Cipher Spec Protocol): El sıkışma aşamasının tamamlandığını ve iletişimin güvenli hale getirildiğinin bildirilmesi amacıyla kullanılmaktadır.
- Kayıt Protokolü (Record Protocol): El sıkışma alt protokolünde hesaplanan anahtarları kullanarak geçerli oturumdaki uygulama verilerinin korunmasından sorumludur.
- Uyarı Protokolü (Alert Protocol): Diğer alt protokoller çalıştırılırken ortaya çıkan hataları ve uyarıları iletmek için kullanılmaktadır (Das & Samdaria, 2014).

Şekil 1.12. TLS Protokolü



Kaynak: (CSA, 2024)

1.5.3. Kablosuz Ağ Güvenliği

Kablosuz ağ güvenliği, kablosuz bir ortamda ağın ve birbirine bağlı cihazların korunmasını ifade etmektedir. Dizüstü bilgisayarlardan cep telefonlarına, video oyun konsollarından buzdolaplarına kadar birçok cihaz, verileri radyo dalgaları aracılığıyla ileten kablosuz ağ bağlantısını yaygın olarak kullanmakla birlikte, verinin okul, kütüphane, otel gibi halka açık ve güvenli olmayan ağlar aracılığıyla iletilmesi güvenlik riski oluşturmaktadır. Kablosuz ağ güvenliği olmadan, kablosuz erişim noktası veya yönlendirici gibi bir ağ cihazına, yönlendiricinin kablosuz sinyalinin menzili içinde bilgisayar veya mobil cihaz kullanan herkes erişebilmekte; kablosuz ağ sisteminde herhangi bir güvenlik önleminin uygulanmaması saldırganın ağa bağlanarak trafiği yakalamasına veya kendi kötü niyetli trafiğini enjekte etmesine neden olabilmektedir (Moissinac, Ramos, Elleithy, & Rendon, 2021)

Kablosuz ağ bağlantılarındaki güvenlik protokolleri de kriptografik algoritmalara dayanmakta olup 1997 yılından 2018 yılına kadar Kabloluya Eşdeğer Gizlilik (Wired Equivalent Privacy-WEP), Wi-Fi Korumalı Erişim (Wi-Fi Protected Access-WPA), WPA2 ve WPA3 standartları yayımlanarak gizlilik, bütünlük ve kimlik doğrulamayı sağlayan güvenlik protokolleri geliştirilmiştir (Kohlios & Hayajneh, 2018).

Tablo 1.3. Kablosuz Ağ Bağlantı Güvenlik Protokolleri

Protokol	**WEP**	**WPA**	**WPA2**	**WPA3**
Yayımlanma Tarihi	1997	2003	2004	2018
Altyapısında Kullanılan Kriptografik Algoritma	RC4	RC4	AES	AES
Anahtar Boyutu (Bit)	64, 128	128	128	128, 256
Şifreleme	Dizi	Dizi	Blok	Blok

Kaynak: (Wang, Yang, & Wan, 2020)

1.5.4. Bulut Güvenliği

Bulut bilişim; sunucu, ağ, depolama, uygulama ve yazılım gibi bilgi işlem kaynaklarının kullanım başına ödeme esasına göre internet üzerinden bir dış hizmet olarak talep edilebildiği, uygulamalara ve verilere her yerden ve her zaman ulaşabilme imkanı sunan sistemlerdir.

Bulut sisteminde; veri gizliliği, veri bütünlüğü, yetkisiz erişimin engellenmesi gibi kritik güvenlik gereksinimleri kriptografik teknikler kullanılarak karşılanmaktadır. Bununla birlikte, büyük miktarda veri içeren bu sistemlerde geleneksel kriptografik tekniklerin kullanılması sebebiyle, şifrelenmiş bir verinin aranması veya üzerinde işlem yapılması işlemleri, şifrelenmemiş metne ulaşılmadan gerçekleştirilememekte, bu durum yüksek işlem gücü gerektirmesinin yanı sıra daha uzun sürelerde gerçekleştirilmektedir. Bulut sistemlerde yaşanan bu problemlerin çözümü için şifreli veriler üzerinde işlem gerçekleştirilmesine olanak sağlayan homomorfik şifreleme[3] ve aranabilir şifreleme[4] (searchable encryption) yöntemlerinin bulut sistemlerine uygulanmasına yönelik çalışmalar devam etmekle birlikte söz konusu sistemlerin uygulanmasıyla hassas verilerin şifreli ve güvenli bir şekilde bulutta işlenebilir hale gelmesi beklenmektedir (Kaaniche & Laurent, 2017).

1.5.5. Nesnelerin İnterneti Güvenliği

Nesnelerin interneti (Internet of Things- IoT), çeşitli sensörler içeren ve internete bağlanabilen cihazların birbirleriyle veri alışverişi yapmalarına ve çeşitli görevleri bağımsız olarak gerçekleştirmelerine imkan tanıyan cihaz ağıdır.

[3]Homomorfik şifreleme, şifreli metin üzerinde belirli hesaplama türlerinin gerçekleştirilmesine ve şifrelenmemiş metin üzerinde gerçekleştirilen işlemlerin sonucuyla eşleşen şifreli bir sonuç üretilmesine olanak tanıyan bir şifreleme yöntemidir (Yi, Paulet, & Bertino, 2014).

[4]Aranabilir şifreleme, veritabanında bulunan şifreli metin üzerinde işlem gerçekleştirmek isteyen kullanıcıların, aranan anahtar kelime ile ilişkili bir arama belirteci oluşturması aracılığıyla aranan anahtar kelimeyi içeren şifrelenmiş içeriğe ulaşmasına ve şifreli metin üzerinde sorgular gerçekleştirilmesine imkan tanıyan bir şifreleme yöntemidir (AWS, 2023).

Küçük boyutlu, az enerji kullanan, az yer kaplayan IoT cihazları (RFID etiketleri, sensörler, temassız akıllı kartlar vb.); cihazların fazlalığı, kaynak kullanımının kısıtlı olması nedeniyle gelişmiş güvenlik yazılımlarının uygulanamaması, yazılım güncellemelerinin zamanında gerçekleştirilememesi, sağlık uygulamaları ile ev otomasyonları gibi son kullanıcıya yönelik cihazların büyük oranda kişisel veri içermesi gibi sebeplerle saldırganların hedefi haline gelmektedir. Söz konusu problemin çözümü içinse daha etkin olarak kullanılabilecek kısıtlı kaynakların (alan, güç tüketimi, enerji tüketimi) kullanıldığı ve blok şifreleme algoritması temelli hafif sıklet kriptografi (Lightweight Cryptography) adı altında yeni bir şifreleme alanı doğmuştur (Aslan, 2020).

1.5.6. Blokzinciri Güvenliği

Blokzinciri, güven eksikliğinin bulunduğu ortamlarda verilerin merkezi olmayan bir veri kayıt defterine kaydedilerek anonim katılımcıların kaydedilen verileri okumasına, doğrulamasına ve kopyalamasına olanak tanıyan ancak silme ve değişiklik yapılmasına izin verilmediği bir veritabanı mekanizmasıdır (Guo & Yu, 2022). Her biri bir önceki bloğun kriptografik özetini, zaman damgasını ve işlem kayıtlarını içeren birbirine bağlı bir dizi bloktan oluşan bu dijital kayıt sisteminde üçüncü bir taraf olmadan güvenli işlem gerçekleştirebilmek ve bloklarda verilerin dürüstçe kayıt altına alınabilmesi için ise her katılımcının takip etmesi gereken belirli (konsensus) algoritmalar kullanılmaktadır (Zhang, He, Lai, Hou, & Zhao, 2023).

Blokzinciri, güvenilmez taraflar arasında güvenilir kayıtların ve işlemlerin gerçekleşmesine olanak tanımak ve merkezi bir kurumun aracı rolünü üstlenme gerekliliğini ortadan kaldırabilmek için kriptografik teknikler kullanmaktadır. Blokzinciri sisteminde; bir işlemin doğru kişi tarafından oluşturulduğunu kanıtlamak için elektronik imza algoritmaları, kullanıcının anonim kimliğini koruyarak gerçekleştirilmesi istenen eylemin doğrulanabilmesi için Sıfır Bilgi Kanıtları (Zero-Knowledge Proofs), mesajın değiştirilmediğinin ve veri bütünlüğünün sağlandığının tespitinde ise özetleme algoritmaları kullanılmaktadır. Böylelikle blokzincirinde yer alan herhangi bir bloktaki bilginin veya işlemin değiştirilmesi halinde blok ile

sonrasında gelen bloklar arasındaki bağlantı bozularak, değiştirilemeyen ve son derece güvenilir bir dağıtık veritabanı oluşturulmaktadır (Guo & Yu, 2022).

1.5.7. IPSec Protokolü

"Internet Protokolü (IP) Güvenliği" veya "IP Güvenlik Protokolü" olarak da bilinen IPSec, internet üzerinde iletişimde bulunan cihazların güvenliğini sağlamak için kullanılan bir güvenlik protokolüdür. IPSec, internet protokollerini kullanarak veri güvenliği ve şifrelemesi için çeşitli güvenlik hizmetleri sunmakta; alınan paketin paket başlığında kaynak olarak tanımlanan taraf tarafından iletildiğini ve aktarım sırasında değiştirilmediğini garanti eden kimlik doğrulama mekanizması, iletişim kuran tarafların üçüncü kişilerce dinlenilmesini engellemek amacıyla mesajları şifrelemesine olanak tanıyan gizlilik özelliği ve güvenli anahtar değişimi için gerekli protokoller söz konusu hizmetler arasında yer almaktadır. IPSec ile internet üzerinden, güvenli sanal özel ağ oluşturma, güvenli uzaktan erişim kurma, intranet ile ekstranet bağlantılarını kurma gibi uygulamalar, tüm trafiğin IP düzeyinde şifrelenebilmesi/doğrulanabilmesi sayesinde güvence altına alınabilmektedir (Camilo, Couto, & Costa, 2017).

2. KUANTUM MEKANİĞİ

Latince miktar veya ne kadar anlamına gelen “quantus” kelimesinden gelen kuantum terimi, fizik biliminde tanımlanan varlığın en küçük ve bölünemeyen birimini ifade etmektedir. Kuantum mekaniği ise atom ve atom altı ölçekte madde ve ışığın özelliklerini, etkileşimlerini ve eylemlerini inceleyen bilim dalıdır (LibreTexts, 2023).

Maddenin yapı taşlarının atom adı verilen görünmez derecede küçük parçacıklar olduğu düşüncesinin kökeni milattan önce 5 inci yüzyıldaki Yunan filozofları Miletoslu Leucippus ve Abderalı Demokritos'a kadar uzanmaktadır. 19 uncu yüzyılın ilk yıllarında ise İngiliz kimyager John Dalton “Yeni Kimya Felsefesi Sistemi” isimli kitabıyla atomun varlığına ilişkin ikna edici bir fenomenolojik kanıt sunmuştur. Kelime anlamı bölünmez anlamına gelen atomun maddenin nihai parçacığı olmadığı ise Michael Faraday’ın çalışmaları ile öne sürülmüş, atomlardan alfa, beta ve gama parçacıklarının yayıldığı radyoaktif bozunmanın keşfiyle 1896 yılında Henri Becquerel tarafından, elektronun tüm atomların evrensel bir bileşeni olduğu ve “-e” olarak adlandırılan negatif bir elektrik yükü taşıdığı Joseph John Thomson tarafından ortaya çıkarılarak maddenin elektriksel doğası ve atom altı parçacıkların varlığı kanıtlanmıştır. 1911 yılında ise Ernest Rutherford tarafından gerçekleştirilen deneylerle atomun merkezinde proton isimli pozitif bir yükün varlığı tespit edilmiş, 1932 yılında Chadwick’in nötronu keşfetmesiyle atom çekirdeğinin yapısı netleşmiştir (LibreTexts, 2023).

Diğer yandan, 19. yüzyılda James Clerk Maxwell tarafından elektrik, manyetizma ve optik olgular birleştirilerek elektromanyetik dalgaların, elektrik yüklerinin hızlandırılmasıyla üretildiği deneysel olarak gösterilmiş; gama ışınları, X ışınları, ultraviyole, görünür ışık, kızılötesi, mikrodalgalar ve radyo dalgaları dahil olmak üzere çok geniş bir dalga boyu aralığında elektromanyetik radyasyonun var olduğu ortaya çıkmıştır. Ancak, 1900 yılında Max Planck, siyah cisim ışınımının ispatını yaparak elektromanyetik ışımanın Maxwell’in teorisinde ifade edildiği gibi sürekli olmadığını, aslında “kuantum” adını verdiği ayrı demetlerden oluştuğunu ifade etmiştir (LibreTexts, 2023).

Doğadaki tüm cisimlerin mutlak sıfırın üstündeki her sıcaklıkta ışıma yaptığının anlaşılabilmesi ve tanımlanabilmesi için siyah cisim tanımına ihtiyaç duyulmuştur. Siyah cisim, üzerine düşen tüm dalga boylarındaki ışınımı yutmakta ve belirli bir sıcaklıkta tüm dalga boylarında yayınım gerçekleştirmektedir. Bu yayınıma siyah cisim ışınımı adı verilmektedir. Siyah cisim teorik olarak ortaya ilk defa 1862 yılında Kirchhoff tarafından ortaya atılmış olup Planck tarafından formüle edilerek ışınımın sürekli bir şekilde değil, bir enerji seviyesinden diğer bir enerji seviyesine geçişte belirli ve kesikli değerler şeklinde yapılabildiğine yönelik bir hipotez kurulmuştur (LibreTexts, 2023).

Planck, ışığın kuantum cinsinden soğurulması ve yayılması kuralının yalnızca siyah cisim radyasyonuna uygulandığına ve radyasyondan ziyade atomların bir özelliği olduğuna inanmasına rağmen, 1905 yılında Albert Einstein, Planck'ın hipotezini elektromanyetik radyasyonun bir özelliği olarak görmüş ve ışık ışınlarının foton adı verilen enerji paketlerinden oluştuğu ile bir metalden bir elektron koparabilmek için fotonun enerjisinin belirli bir eşik değerinin üzerinde olması gerektiğini öne sürmüştür (LibreTexts, 2023).

1913 yılında Niels Bohr, bir proton ve bir elektrondan oluşan hidrojen atomunun klasik elektromanyetik teorinin yasalarına uygun bir şekilde; elektronun yörüngeye doğru hızlanarak spiral çizmesi ve enerjiyi elektromanyetik dalga şeklinde yayması sonucu neden kendi kendini yok etmediğini anlamak amacıyla Einstein'ın fikirlerinden yararlanmış, elektronların çekirdek etrafında dönerken belirli bir yörünge üzerinde yer aldığını ve enerji seviyeleri arasında sıçrayarak enerji soğurma ve yayım süreçlerini gerçekleştirdiğini ileri sürmüştür (Kleppner & Jackiw, 2000).

1924 yılında ise Luis De Broglie, elektromanyetik ışınımın dalga-parçacık ikili doğasından esinlenerek elektron, proton nötron gibi durgun kütleli atom-altı parçacıklarının da dalga özelliğine sahip olabileceklerini öne sürmüştür. Tüm maddelerin yalnızca kütlesi olan bir parçacık gibi değil, aynı zamanda enerji transferi yapabilen bir dalga olduğunu gösteren bu teorem "Dalga Parçacık İkilemi" olarak bilinmektedir (Kleppner & Jackiw, 2000).

Atomun bir parçacık mı yoksa bir dalga mı olduğuna ilişkin olarak bilim insanları tarafından birçok deney gerçekleştirilmiş, deneyler sonucu kuantum fiziğinin bilimsel olarak açıklaması mümkün olmayan çeşitli sonuçlarıyla karşılaşılmıştır.

Bilim insanları yüksek yoğunluklu lazer ışınlarını bir veya iki yarıklı bir engelden geçirerek ve ardından arka planda nereye düştüklerini kontrol ederek dalga parçacık ikiliğini göstermiştir. Söz konusu deney düzeneğinde tek yarık kullanılması halinde fotonun bir parçacık gibi davranarak arka planda birbirlerine oldukça yakın yerlerde konumlandığı, çift yarık kullanıldığında ise bir dalga özelliği göstererek arka planda bir girişim deseni oluşturduğu gözlemlenmiş ve fotonun bir dalga olarak ilerlediği ancak parçacık olarak yere düştüğü sonucuna varılmıştır (Grimes, 2020).

Bilim insanlarının fotonun hareketini detaylı olarak inceleyebilmek ve hangi yarıktan geçerek girişim deseni oluşturduğunu gözlemleyebilmek amacıyla yarıklara foton dedektörü yerleştirmesinin ve çift yarık deneyini tekrarlamasının akabinde ise açıklanamayan bir sebeple fotonun parçacık olarak hareket ettiği ve girişim deseni oluşturmadığı gözlemlenmiştir. Hatta fotonların yarıktan geçene kadar dedektörleri açmadıkları ve dedektörleri açtıkları anda fotonun parçacık olarak hareket ettiğinin gözlemlendiği, fotonun geçmişteki ilk davranışını gelecekteki bir algılamanın başlatılmasına bağlı olarak geriye dönük olarak ayarlayabildiğinin gözlemlendiği deneyler gerçekleştirilmiştir. Bu durum açıklaması yapılamayan kuantum mekaniği özelliklerinden yalnızca biri olup gözlemci etkisi olarak adlandırılmaktadır. Aşağıda kuantum mekaniğinin temelini oluşturan özellikler kısaca özetlenmektedir (Grimes, 2020).

- **Olasılık İlkesi:** Atomun çekirdeğinde proton ve nötronun bulunduğu, elektronların ise elektromanyetik çekim nedeniyle çekirdeğin yörüngesinde döndüğü bilinmekteydi ancak kuantum mekaniği, elektronun herhangi bir zaman diliminde yörüngenin hangi konumunda bulunacağının tahmin edilemeyeceğini, yalnızca belirli atomik yörünge alanlarında bulunma olasılığının tahmin edilebileceğini göstermiştir. Olasılık ilkesi yalnızca elektronlar için değil, bir kuantum parçacığın herhangi bir özelliği için de

uygulanabilmektedir. Söz konusu rastlantısallık tesadüfi olmayıp kuantum mekaniğinin temeli ve doğası gereği oluşmaktadır. Başka bir deyişle kuantum mekaniği, matematiği, nesneleri ve nasıl etkileştiklerini ne kadar iyi bilirsek bilelim, tek bir deneyin veya kuantum sonucunun belirli cevabını asla tahmin edemeyeceğinizi söylemektedir.

- **Belirsizlik İlkesi:** Werner Heisenberg tarafından ortaya atılan belirsizlik ilkesi, bir kuantum parçacığının hem konumunu hem de momentumunu aynı anda tam olarak ölçemeyeceğinizi ve bir niceliği daha hassas bir şekilde ölçmeye çalıştıkça, bağımlı çiftin diğer tarafının daha az doğru hale geldiğini ifade etmektedir. Bu durum, ölçümde gerçekleştirilen bir kusur sebebiyle değil, dalga-parçacık ikiliği ile olasılık ilkesinden kaynaklanan kuantum mekaniğinin doğal bir sonucu olarak gerçekleşmektedir.
- **Kuantum Tünelleme:** Kuantum parçacıklarının engellerden geçmesine imkan tanıyan ve nasıl çalıştığının ya da bir atomaltı parçacığın öncesinde gerçekleştirdiği başarısız denemelerine kıyasla ne zaman başarılı olacağının bilinmediği bir kuantum mekaniği özelliği olup güneşin termonükleer füzyon kullanarak ısı ve ışık üretme yönteminin, bir radyoaktif elementin bozunmasının ve fotosentezin temelini oluşturmaktadır.
- **Süperpozisyon:** Bir parçacığın tek bir cevap vermek üzere gözlemlenip ölçülene kadar tüm olası durumlarda var olabileceğini söyleyen bir kuantum özelliğidir. Örneğin, cevabını bilmediğimiz belirli bir matematik probleminin cevabının A veya B olabileceğini varsayarsak süperpozisyon, cevabın gözlemlenmeden veya ölçülmeden önce kuantum durumundayken, aynı anda hem A hem de B olduğunu söylemektedir.

  Erwin Schrödinger'in kuantum kedi bilmecesi süperpozisyonu en iyi açıklayan düşünce deneyi olarak bilinmektedir. Schrödinger, bir kedinin, içinde ölümcül zehir bulunan kapaklı bir şişe, radyoaktif bir element ve bir "Geiger sayacı"nın[1] bulunduğu kapalı bir kutuya yerleştirildiği bir senaryo yaratmıştır. Radyoaktif elementin bozunabilir ya da bozunmayabilir durumda olması bir kuantum olayıdır ve elementin herhangi bir atomunun bozunmaya karar verdiği an rastgele bir olaydır. Geiger sayacının radyoaktif bozunmadan kaynaklanan

[1] İyonlaştırıcı radyasyonu tespit etmeye ve ölçmeye yarayan bir cihaz

radyasyonu tespit etmesi halinde, zehir içeren şişenin kırılmasını tetiklenecek ve bu da kediyi öldürecektir.

Süperpozisyon ilkesi radyoaktif elementin hem bozunduğunu hem de bozunmadığını belirttiğinden kutuyu açmadan ve kediyi gözlemlemeden önce kedi hem canlı hem de ölü olarak kabul edilmekte, makroskobik dünyada anlamsız görünen bu durum kuantum düzeyinde mutlak gerçeklik olarak kabul edilmektedir.

- **Gözlemci Etkisi:** Bilim insanlarının onlarca yıl boyunca gerçekleştirdiği deneyler sonucu doğruluğu kanıtlanan ancak nedeni ve nasıl gerçekleştiği anlaşılamayan bu özelliğe göre bir kuantum sistemini gözlemlemek sistemin değişmesine sebep olmaktadır. Kuantum mekaniğinin gelişiminde bahsedildiği üzere, gerçekleştirilen her çift yarık deneyinde bir fotonun hangi yarıktan geçeceğinin tespit edilebilmesi amacıyla bir dedektör yerleştirildiğinde fotonun parçacık gibi davrandığı, dedektörün olmadığı durumlarda ise dalga özelliği gösterdiği gözlemlenmiştir. Bu durum birçok farklı yorumlamaya sebebiyet vermiş olup en bilinenleri Kopenhag yorumu ile Çoklu Dünyalar yorumudur.

  Kopenhag yorumu, kuantum mekaniğinin süperpozisyon özelliğinden de yola çıkarak, birçok olasılıktan oluşan kuantum dalga fonksiyonunun ölçülüp gözlemlendiğinde dalga fonksiyonunun parçalanarak (dalga fonksiyonu çökmesi olarak da bilinmektedir) nihai bir duruma dönüştüğünü, çöküşü yaratan eylemin ise gözlem girişimi olduğunu söylemektedir. Kuantum senaryosunu ölçme eylemi tüm durumları ya da cevapları tek bir nihai cevaba indirgediğinden Kopenhag yorumu, bir şeyi gözlemlemenin onu neden değiştirdiğini açıklamak için kuantum dünyasında en büyük desteği alan yorum olmuştur.

  Çoklu dünyalar yorumu ise dalga fonksiyonu çöküşünden önceki tüm olası cevapların başka bir evrende olduğunu ve her kuantum çöküşünün, çöküşten önceki olasılıksal dalga fonksiyonundaki tüm olası cevaplara eşit sayıda yeni evren yarattığını söylemektedir.

- **Klonlanamazlık İlkesi:** Bir kuantum sisteminin ölçülmesinin veya gözlemlenmesinin sistemi değiştirdiğini belirten gözlemci etkisinden yola

çıkan klonlanamazlık ilkesi, kuantum durumların doğrudan kopyalanamayacağını belirtmektedir. Söz konusu kopyalama eyleminin dolaylı olarak gerçekleştirilmesi mümkün olmakla birlikte kuantum işlemlerinin tamamlanması gerekmektedir. Bu durum bir kuantum bilgisayarda kopyalama veya hata düzeltme işlemlerini zorlaştırırken kuantum kriptografi için birçok gizli dinleme senaryosunu önlemekte ve iletişimin güvenliğini garanti etmektedir.

- **Dolanıklık İlkesi:** Einstein'ın uzaktan ürkütücü eylem olarak nitelendirdiği dolanıklık ilkesi, birbirine dolanık iki kuantum parçacığından bir parçacıkta gerçekleşen özellik değişiminin, ne kadar uzak mesafelerde olursa olsunlar diğer parçacık çiftinde de tahmin edilebilir bir değişime sebep olduğunu ortaya koymaktadır. Dolanıklık özelliğinden yararlanılırken ölçüm işlemi gerçekleştirilememekte, istenen yeni bir durumun elde edilebilmesi için dolanık parçacıkların manipüle edilmesi halinde kuantum durum ve dolayısıyla parçacıklar arasındaki dolanıklık bozulmaktadır.

  Doğada doğal bir süreç olarak işleyen dolanıklık eylemi, bir kuantum parçacığının başka bir kuantum parçacığıyla etkileşime girmesi ile gerçekleşmekte, her karşılaşılan parçacık ile birlikte büyüyebilmekte, bu sayede saniyenin milyonda biri kadar bir süre içerisinde milyarlarca kuantum parçacık birbirine bağımlı çok parçacıklı bir varlık oluşturabilmektedir.

  Bilim insanları, dolanık kuantum parçacıklar elde etme ve dolanıklık özelliklerinin araştırılmasına yönelik birçok deneysel çalışma gerçekleştirmiştir. Gerçekleştirilen çeşitli çalışmalar ile dolanık kuantum parçacıklar oluşturulabilmiş, birbirinden çok uzakta bulunan kuantum parçacıkların dolanık hale getirilmesi henüz mümkün olmasa da dolanık parçacıkların birbirinden çok uzak mesafelere taşınması durumunda da özelliklerini koruyabildiği keşfedilebilmiştir.

  Dolanıklık ilkesinin, fiziksel olayların öncelikli olarak yakın çevreden etkilendiğini belirten yerellik ilkesine aykırı olması ve ışık hızından hızlı mesaj iletiminin gerçekleştiği sanrısı Albert Einstein, Boris Podolsky ve Nathan Rosen'in 'Fiziksel gerçekliğin kuantum mekaniksel açıklaması tam olarak düşünülebilir mi?' adlı makaleyi yayımlamasına sebep olmuş, EPR (Einstein,

Podolsky, Rosen) Paradoksu olarak da adlandırılan makalede; parçacıklardan birine yapılan ölçümün uzaktaki diğer parçanın durumunu anlık olarak etkilemesinin yerellik ilkesini ihlal ettiği, kuantum teorisinin eksik olduğu ve teorinin tamamlanması için parçacıklar arasındaki bu etkiye sebep olan yerel gizli değişkenlerin bulunması gerektiği ifade edilmiştir.

John Bell 1964 yılında "Einstein Podolsky Rosen Paradoksu Üzerine" başlıklı makalesini yayımlayarak Bell Eşitsizliğini formüle etmiş ve hiçbir gizli değişken teorisinin kuantum mekaniğinin tüm sonuçlarını yeniden üretemeyeceğini matematiksel olarak göstermiştir (Aspect, 2015).

1969 yılında ise John Clauser, Michael Horne, Abner Shimony ve Richard Holt tarafından Bell teoremi gerçekleştirilebilir deneylere uygulanacak şekilde genelleştirilmiş (Clauser, Shimony, Holt, & Horne, 1969), 1972 yılında ise deney gerçekleştirilerek gizli değişkenlerin dolanıklığın etkilerini açıklayamayacağını göstermiştir (Freedman & Clauser, 1972).

Ancak, Clauser-Freedman deneyi Bell'in bir parçacığın bir gözlemci tarafından ölçülmesinin diğer parçacığın ölçümünü etkilemeyeceği yönündeki varsayımını test etmemiştir. Alain Aspect, bu sorunun cevabını aramış ve Bell'in bir polarizördeki ölçümün sonucunun diğerinin yönüne bağlı olmadığına yönelik varsayımını yine Bell'in önerdiği şekilde; her bir polarizörün yöneliminin fotonların uçuş halindeyken seçilmesi halinde nedenselliğin (hiçbir etkinin ışıktan daha hızlı hareket edemeyeceğini belirtir) polarizörün değişim anında diğerinin yönelimini bilmesini engelleyeceğini belirterek yerellik boşluğunun kapatılabileceğini ifade ettiği uygulamasını deney ortamına aktarmış ve kuantum mekaniği yasaları ile uyumlu bir sonuç ortaya koymuştur (Aspect, 2015).

Anton Zeilinger, bir parçacığın kuantum durumunu başka bir parçacığa aktarmanın kuantum ışınlanma ve dönüşümü sırasında durum hakkında herhangi bir bilgi edinilmemesi koşuluyla mümkün olduğunu belirterek kuantum mekaniğinin temel özelliği olan kuantum dolanıklıktan da yararlanılarak gerçekleştirilebileceğini ifade etmiş ve gerçekleştirdiği deney ile parçacığın yeniden yapılandırılabilmesi için taranan bilgilerini uzak bir

mesafeden ileterek parçacığın kuantum durumunu başka bir parçacığa aktarmayı başarmıştır (Bouwmeester, Mattle, & Zeilinger, 1997).

Fransız fizikçi Alain Aspect, Amerikalı teorik ve deneysel fizikçi John F. Clauser ve Avusturyalı kuantum fizikçisi Anton Zeilinger, dolanık fotonlarla ilgili deneyler, Bell eşitsizliklerinin bozulduğunun gösterilmesi ve kuantum enformasyon biliminde öncülük etmeleri sebebiyle 2022 Nobel Fizik Ödülü'nü kazanmışlardır.

- **Dekoherans (Eşevresizlik):** Bir kuantum parçacığının takip edilmesi ve gözlemlenmesi mümkün kuantum durumları içerisinde yer alması söz konusu parçacığın tutarlı olduğunu, diğer bir deyişle dekoherans durumunda bulunmadığını ifade etmektedir. Kuantum bilgi biliminde sonuç olarak adlandırılabilecek bir kuantum cevabına ulaşılabilmesi için kuantum parçacıklarından oluşan sistemin kuantum durumunun matematiksel bir temsili olan dalga fonksiyonu ile tanımlanması ve çeşitli kuantum etkilerini açıklamak içinse dalga fonksiyonunun olasılıksal bir yorumunun kullanılması gerekmekte, farklı durumlar arasında kesin bir faz farkının olması sistemin tutarlı olduğunu göstermektedir.

  Diğer yandan, bir kuantum sisteminde çevre izolasyonunun sağlanmadığı durumlarda kuantum parçacıklarının mikrosaniyeler içerisinde milyarlarca kuantum parçacığı ile etkileşime girerek dolanık parçacıklar oluşturabilme yeteneği, bir parçacığın veya kuantum özelliğinin takip edilmesini zorlaştırarak arzu edilmeyen karmaşık sonuçlarla karşılaşılmasına sebep olmaktadır. Bu durum kuantum deneylerinin gerçekleştirilmesinde kullanılan cihazların ve kuantum bilgisayarların iç yapılarının dış dünyadan izole edilmesini zorunlu kılmakta, aksi takdirde orijinal parçacık veya kuantum özelliğinin takip edilememesi ya da ulaşılmak istenen sonucun anlaşılamaması kuantum parçacığının veya sisteminin uyumsuzlaşmasına diğer bir deyişle dekoherans durumunun meydana gelmesine sebep olmaktadır. Bu nedenle, kuantum bilgi bilimlerindeki en büyük mücadelelerden biri, istenen ölçüm gerçekleştirilinceye kadar sistemin dekoherans durumuna geçmesinden korumaktır.

2.1. Kuantum Teknolojiler

Son yirmi yılda kuantum teknolojileri muazzam bir ilerleme kaydetmiş ve kuantum dolanıklık ile süperpozisyon gibi kuantum durumlarından yararlanan yeni teknolojiler geliştirilmiştir. Kuantum teknolojiler; dolanık parçacıkların verilerin güvenli iletiminde kullanıldığı kuantum iletişim, kontrol edilebilen kuantum sistemlerinin daha az ulaşılabilir olan kuantum sistemlerinin davranışını yeniden üretmek için kullanılan kuantum simülasyonu, çarpanlara ayırma gibi belirli hesaplamaları önemli ölçüde hızlandırmak için kullanılan kuantum hesaplama ve tutarlı kuantum sistemlerinin dış etkenlere karşı yüksek hassasiyetinin fiziksel büyüklüklerin ölçüm performansını arttırmak için kullanıldığı kuantum algılama ve metroloji olmak üzere dört temel alanda gruplandırılmaktadır.

2.1.1. Kuantum Simülasyon

Karmaşık kuantum sistemlerini anlamlandırabilmek amacıyla kuantum mekaniğinin klasik bilgisayarlar ile simüle edilmesinin mümkün olmadığının ortaya çıktığı 1982 yılında, kuantum sisteminin kuantum mekaniği prensipleriyle çalışan başka bir kuantum simülatör ile simüle edilmesinin daha verimli olacağı düşüncesiyle Richard Feynman tarafından "kuantum mekaniği yasalarına göre çalışan" kuantum bilgisayarlar önerilmiştir (Georgescu, Ashhab, & Nori, 2014).

Kuantum simülatörler, çok düşük sıcaklıklarda kuantum durumlarının gözlemlenebilir hale gelmesiyle olağanüstü özelliklerin yeniden üretilebildiği ve bu sayede klasik bilgisayarlarla çözülmesi mümkün olmayan hesaplamaların gerçekleştirilebildiği kuantum bilgisayarların belirli uygulamalar için tasarlanarak optimize edildiği kuantum cihazlarıdır. Kuantum simülatörlerin kuantum bilgisayarlara kıyasla daha az kübit kullanımı gerektirmesi sebebiyle daha kolay inşa edilebilir olması öngörülmekte; kimya, nükleer fizik, malzeme bilimleri, akışkanlar mekaniği, lojistik ve daha genel olarak optimizasyon gibi çok çeşitli alanlarda uygulama alanı bulması beklenmektedir (AvrupaKomisyonu, 2023).

2.1.2. Kuantum Algılama

Kuantum algılama teknolojileri, kuantum parçacıklarının çevresine karşı geliştirdiği olağanüstü duyarlılıktan yararlanarak klasik ölçüm cihazlarına kıyasla sıcaklık, basınç, frekans, ivme, dönüş, manyetik ve elektrik alan gibi çeşitli fiziksel özellikleri daha hassas ve kesin bir şekilde ölçmemize yarayan gelişmiş bir sensör teknolojisidir. Analiz edilen verilerin atomik özelliklerin kullanılarak ölçülmesi; cihazların daha doğru, kapsamlı ve verimli hale getirilmesine olanak tanırken klasik ölçüm cihazlarında olduğu gibi fiziksel kısıtlamalara tabi olmamaları sebebiyle ışık ve ses tabanlı veri sensörlerinde meydana gelen sinyal sıkışması ve elektromanyetik girişim gibi durumlara karşı koruma sağlayarak güvenilirliği artırmaktadır (BAE, 2023).

Kuantum algılama teknolojisinin gelecekte;

- Uyduya bağımlı küresel konumlandırma sistemi cihazlarıyla daha hızlı, doğru ve güvenilir coğrafi konum belirlenmesinde,
- Moleküler analiz ve tıbbi görüntüleme alanlarında daha kolay tespit ve daha az olası yan etkiyle ayrıntılı ve doğru tıbbi teşhislerde bulunulmasında,
- Uzayda, su altında ve radyo frekansı sinyallerinden etkilenen bölgelerde kullanılan füze, uydu, roket, uçak, helikopter, gemi gibi araçların bir konumdan başka bir konuma ulaşması için kullanılan güdüm sistemlerinin daha doğru ve daha duyarlı hale getirilmesinde,
- Transit tüneller, kanalizasyonlar ve madenler gibi yer altı ortamlarının daha doğru tespiti, görüntülenmesi ve haritalandırılmasında,
- Çığ, deprem, volkanik patlama, tsunami gibi kütleçekimsel etkilerin etkin bir şekilde algılanarak uyarı sistemlerinin oluşturulmasında

kullanılması beklenmektedir (BAE, 2023).

2.1.3. Kuantum Hesaplama

Kuantum hesaplama, klasik bilgisayarlar ile çözülmesi mümkün olmayan; polinom zaman algoritması ile çözülemeyen veya üstel işlem zamanı gerektiren problemleri,

kuantum mekaniği ilkelerinden yararlanarak hızla çözebilmeyi hedefleyen, kuantum bilgisayarlara odaklanan ve henüz gelişim aşamasında olan teknolojilerdir (Yang, Zolanvari, & Jain, 2023). Kuantum hesaplama alanı, Amerikalı teorik fizikçi Feynman'ın hesaplamalar için kuantum durumlarının kullanılmasını önermiş olduğu "Fiziği Bilgisayarla Simüle Etmek"[2] adlı makalesinin yayınlanmasının ardından ilgi görmeye başlamış olup dünya genelinde yeterli sayıda kübite[3] hata toleransına sahip bir kuantum bilgisayarı ile kuantum teknolojilerinde üstünlük elde edilmesi hedeflenmektedir. Bu konudaki en etkileyici örnek 1994 yılında Peter Shor'un kuantum bilgisayarların sayıları etkili bir şekilde çarpanlara ayırabildiğini göstermesidir (Shor P. W., 1994). Bu durumun kriptografik işlemlerde kullanılan ve güvenliği tam sayıları çarpanlarına ayırmanın zorluğuna dayandırılan asimetrik anahtarlı şifrelemeler için ciddi bir tehdit unsuru olduğu düşünülmektedir.

Klasik bilgisayarlar verileri depolamak, aktarmak ve işlemek için devre anahtarının açık veya kapalı olması ile ilişkili olarak 0 veya 1 değerini alabilen ve bit adı verilen bilgi birimlerini kullanmaktadır. Kuantum hesaplama ise kuantum teorisini kullanan yeni bir paradigma olup klasik bilgisayarlarda kullanılan bit bilgi birimi yerine kuantum mekaniğinin süperpozisyon, dolanıklık ve girişim gibi temel özelliklerini kullanarak olağanüstü bir hesaplama avantajı sunan kuantum biti veya kübit olarak adlandırılan bilgi biriminin kullanıldığı ve kuantum bilgisayarlarında algoritmaları gerçekleştirebilmek için kübitlerin durumunun kontrollü bir şekilde manipüle edilerek işlemlerin gerçekleştirildiği uygulamadır (Grimes, 2020).

Bir kübit, klasik bilgisayarlarda olduğu gibi 0 ve 1'den oluşan iki durumlu bir sistemi ifade etmektedir. Örneğin bir fotonun yatay ve dikey pozisyonu sırasıyla 0 ve 1'i temsil edebilmektedir. Bir kübit ile klasik bir bit arasındaki fark ise; bir kuantum parçacığının aynı anda tüm olası durumlarda bulunabilmesine imkan tanıyan süperpozisyon ilkesi gereğince bir kübitin aynı anda 0 ve 1 değerini alabilmesidir (Wang Y. , 2020).

[2] Feynman, R. P. (1982). Simulating physics with computers. *Int. j. Theor. phys*, 21, 467-488, https://doi.org/10.1007/BF02650179

[3] Bir kübit, klasik bilgisayarlarda olduğu gibi 0 ve 1'den oluşan iki durumlu bir sistemi ifade etmektedir

Süperpozisyon durumunda bulunan ve dolanık kübitlerden oluşan bir ortamda sistemin ölçümünün sonuçlarını gösteren olasılık dalgaları meydana gelmekte, bu dalgalar girişim oluşturarak birbirini kuvvetlendirebilmekte ya da sönümlendirebilmektedir. Kuantum bilgisayarı üzerinde gerçekleştirilen bir hesaplama, olası tüm hesaplama durumlarının bir süperpozisyonunun hazırlanması ve bir algoritmaya göre süperpozisyonunun bileşenleri üzerinde seçici girişimin kullanılması yolu ile çalışmaktadır. Bu sayede birçok olası sonuç girişim yoluyla iptal edilirken güçlendirilmiş sonuçlar hesaplamanın çözümlerini oluşturmaktadır (IBM, 2023).

Süperpozisyon durumundaki bir kübit üzerinde gerçekleştirilen bir işlemin aynı anda her iki değer üzerinde de etkili olması ve dolanıklık özelliğinin de kullanılarak kübitlerin birbirinden bağımsız olarak değil, farklı durumları temsil edebilen tek bir nesne olarak tanımlanabilmesi kuantum bilgisayarların çok sayıda olasılık üzerinde eş zamanlı paralel hesaplamalar gerçekleştirebilmesini sağlamaktadır. Genel olarak n klasik bit bir seferde 2^n olası durumdan yalnızca birini kodlayabiliyorken, n kübitlik bir kuantum bilgisayar 2^n işlemi paralel olarak işleyebilmekte; dolayısıyla, kuantum bilgisayarların aritmetik ve mantıksal işlemleri gerçekleştirme kapasitesinde üstel oranda artan bir durum iyileştirmesi sunmaktadır (Vasileios, 2018). Bu sebeple ilk kuantum bilgisayarının geliştirildiği 1998 yılından itibaren kübit sayısı artırılmaya çalışılarak kuantum bilgisayarların işlem gücü artırılmaya çalışılmıştır. Ancak kübit sayısının artmasıyla birlikte bir kuantum bilgisayarın gücünü ve hızını artıran etmenin yalnızca kübit sayısına bağlı olmadığı, kübitler ve diğer bileşenler arasındaki bağlantı ve tutarlılık süresi, geçit ve ölçüm hataları, iletilen sinyalin başka bir devre veya kanalda istenmeyen bir etki yarattığı çapraz konuşma (Crosstalk) ile devre yazılımı derleyici verimliliği gibi çeşitli faktörlerin de hesaba katılması gerektiği anlaşılmıştır (Grimes, 2020).

Kuantum bilgisayarların klasik bilgisayarların çözemediği bir sorunu çözebilir duruma eriştiği nokta kuantum üstünlüğü olarak adlandırılmaktadır. Kuantum üstünlüğüne ulaşılabilmesi için bir kuantum bilgisayarda kaç kübit kullanılması gerektiği henüz bilinmemekle birlikte bu üstünlüğe ulaşabilmek için bilim insanları kübit sayısını artırmanın yanı sıra mükemmel kübitleri oluşturabilmenin önündeki engelleri kaldırmanın yolunu araştırmaktadır (Grimes, 2020).

Mükemmel kübiti oluşturmanın önündeki en büyük zorluklardan biri kuantum dekoheransıdır. Dekoherans, bir kuantum parçacığının süperpozisyon durumunu ve dolanıklığını kaybetmesine ve klasik duruma geçmesine sebep olarak ulaşılmak istenen sonucun anlaşılamamasına sebep olmaktadır. Kuantum üstünlüğünün gerçekleştirileceği kuantum bilgisayarlarda dekoheransın bir cevaba ihtiyaç duyulması ve ölçümün gerçekleşmesinin akabinde oluşması amaçlanmaktadır. Bu sebeple çoğu kuantum bilgisayar üreticisi kübit yapısı, ısı, radyasyon, gürültü, titreşim, hatalı geçitler, hatalı ölçümler gibi çeşitli nedenlerle meydana gelebilen dekoheransın gelişme süresini, kuantum bileşenlerinin dış dünyadan izole edilmesi, süper soğutmanın kullanılması, kontrol kübitlerinin kullanılması, hata düzeltimi için kuantum dolanıklığının kullanılması gibi yöntemler ile ulaşılmak istenen sonuç için gerekli hesaplama süresinden daha uzun olacak şekilde iyileştirebilmek için çalışmaktadır (Grimes, 2020).

2.1.3.1. Kuantum Bilgisayar Çeşitleri

Günümüzde geliştirme aşamasında olan ve farklı uygulamalar için tasarlanmış birçok farklı türde kuantum bilgisayarı, teorik modeli, mimarisi ve uygulaması bulunmakta olup aşağıda bazı kuantum bilgisayar çeşitleri ile avantaj ve dezavantajlarına yer verilmiştir.

2.1.3.2. Süperiletken Kuantum Bilgisayarlar

Var olan tüm maddeler kuantum mekaniği yasalarına tabiidir. Mutlak sıfır noktasında madde alışılmadık bir aşamaya geçerek beklenmedik davranışlar sergilemekte ve normal şartlar altında mikro ölçekli dünyada işleyen kuantum mekaniği gözlemlenebilir hale gelmektedir. Bu nedenle, kuantum işlemcilerinin kuantum davranışı sergileyebilmesi ve dekoherans durumuna geçişinin engellenebilmesi amacıyla mutlak sıfırın (-273,15 °C) yüzde biri kadar üzerinde bir sıcaklık gerekmekte, bu sıcaklık derecesine ulaşabilmek içinse ultrasoğuk süperakışkanlar kullanılmaktadır. Ultra düşük sıcaklıklarda bazı maddeler büyük ölçüde kuantum mekaniği durumuna

uyan özellikler sergileyerek elektronların direnç göstermeden hareket etmesine izin veren süperiletken özellikleri göstermektedir (IBM, 2023).

Elektronlar süperiletkenlerden geçerken eşleşerek Cooper[4] çiftlerini oluşturmakta ve kuantum tünelleme olarak bilinen bir süreçle bariyerler veya yalıtkanlar boyunca yük taşıyabilmektedir. Bir yalıtkanın iki tarafına yerleştirilen iki süperiletken bir Josephson bağlantısı[5] oluşturmakta, kuantum bilgisayarlar ise bu bağlantıları süperiletken kübit olarak kullanmaktadır. Bu kübitlere mikrodalga fotonları gönderilerek davranışları kontrol edilebilmekte ve kuantum bilgi birimlerini tutmalarını, okumalarını ve değiştirmeleri sağlanabilmektedir (IBM, 2023).

Diğer kuantum sistemlerine kıyasla süperiletken kübitler aşağıdaki avantajlara sahiptir:

1. Yüksek Tasarlanabilirlik: Yük kübitleri, akı kübitleri, faz kübitleri gibi farklı kübit türleri tasarlanabilmekle birlikte kübitin enerji seviyesi ve bağlantı gücü gibi farklı parametrelerinin de değiştirilmesi mümkündür.
2. Ölçeklenebilirlik: Süperiletken kübitlerin hazırlanması yarı iletken mikrofabrikasyon sürecine dayanmakta olup üretim ve ölçeklenebilirlik açısından gelişmiş çip üretim teknolojisinden yararlanılarak yüksek kaliteli cihazlar üretilebilmektedir.

[4] Temel parçacıklar fermiyon ve bozon olmak üzere ikiye ayırılmaktadır. İki özdeş fermiyon aynı kuantum durumunda bulunamazken sınırsız sayıda özdeş bozon aynı kuantum durumunda bulanabilmektedir. John Bardeen, Leon Cooper ve John Robert Schrieffer BCS kuramı ile süperiletkenliğin nasıl ortaya çıktığının kuramsal açıklamasını yapmış ve fermiyon özelliği taşıyan bir çift elektronun bozon oluşturabileceğini ortaya çıkarmıştır. Cooper çifti olarak anılan bu elektronlar, hızları zıt olan dönüşleri baştan sona birbirine bağlı iki elektrondan oluşmaktadır. Dolayısıyla Cooper çiftleri aynı kuantum durumunda bulunabilmekte, aynı kuantum durumunda bulunan çok sayıda Cooper çiftinin bir araya gelmesiyle bir süperakışkan ortaya çıkabilmekte, bir süperakışkanın çevresiyle hiç etkileşmeden akabilmesi sayesinde elektriksel direnç sıfır olabilmektedir. Süperiletkenliğin düşük sıcaklıklarda ortaya çıkmasının nedeni ise Cooper çiftlerini bir arada tutan bağın zayıf olmasıdır. Sıcaklık arttığında Cooper çiftleri kolayca dağılmakta ve malzeme yeniden elektrik akımına direnç göstermeye başlamaktadır. (Dr. Mahir E. Ocak, Bilim ve Teknik, Mart 2023,s:54)

[5] Belirli koşullar altında Cooper çiftleri, ince yalıtım katmanı boyunca bir süper iletkenden diğerine hareket edebilmektedir. Elektron çiftlerinin bu hareketi Josephson bağlantısını oluşturur ve çiftlerin yalıtkan tabakayı geçme sürecine Josephson tünelleme adı verilir. (Britannica, Josephson effect https://www.britannica.com/science/Josephson-effect#ref51197)

3. Birleştirilebilirlik: Süperiletken kübit sisteminin devre yapısı, birden fazla kübitin birbirine bağlanmasını kolaylaştırmaktadır.
4. Kontrol Edilebilirlik: Süperiletken kübitlerin çalışması ve ölçümü, mikrodalga atımları ile kontrol edilebilmektedir. Bu sayede, ticari mikrodalga cihazları ve ekipmanları süperiletken kuantum hesaplama deneylerinde kullanılabilmektedir. (He-Liang Huang, 2020)

2.1.3.3. Tavlama (Analog) Kuantum Bilgisayarlar

Tavlama kavramı genel olarak camın veya metalin başka bir şekle dönüştürülmesine olanak sağlamak için ısıtılması ve mukavemetinin veya saflığının artırılması için yavaşça soğumasına izin verilmesi işlemini tanımlamaktadır. Kuantum tavlama bilgisayarlarında tavlama işlemi ise süperpozisyon durumunda olan kübitlere elektromanyetik bağlayıcı adı verilen bir mekanizmanın uygulanması ile gerçekleşmektedir. Bağlayıcı ile eşit olan olasılık durumu eşit olmayan olasılık ile değiştirilerek kübitlerin sahip olduğu belirli durumların olasılığı artırılmakta, kuantum durumları enerjilerini mümkün olan en düşük enerji durumuna indirmekte ve gözlemlenen en düşük enerji durumunun nihai cevap olma olasılığı en yüksek olduğu durum olarak belirlenebilmektedir. (Grimes, 2020, s. 45)

Kuantum hesaplama alanında özel bir hesaplama yaklaşımı olan kuantum tavlama, matematiksel modelleme ile problem boyutunun büyüdüğü ve problem çözümünün uzun zaman aldığı optimizasyon problemlerinin çözümünde kullanılmakta; kuantum hesaplama alanında faaliyet gösteren Kanada merkezli D-Wave Systems firmasının finans, lojistik, ilaç keşfi ve makine öğrenmesi gibi alanlarda çeşitli optimizasyon problemlerini çözebilen 2000 kübitlik kuantum tavlama bilgisayarları ürettiği belirtilmektedir. (Salva, 2023)

Dış ortam gürültüsüne karşı dirençli, ölçeklenebilirliği kolay ve mutlak sıfır noktasına yakın değerlerde çalıştırılmanın zorunlu olmaması gibi avantajlara sahip olan kuantum tavlama bilgisayarları, günümüzde yalnızca optimizasyon problemlerinin çözümünde kullanılabilmekte, uzun vadede klasik bilgisayarlardan daha iyi performans gösterip

göstermeyeceği ya da çeşitli alışılmadık sorunların üstesinden gelip gelemeyeceği bilinmemektedir. (Grimes, 2020, s. 47)

2.1.3.4. Topolojik Kuantum Bilgisayarlar

Topoloji, yüzey özelliklerini inceleyen ve bir nesne gerildiğinde, büküldüğünde veya deforme edildiğinde bozulmayan özellikleri tanımlayan matematiksel bir terimdir. Kübitlerin çevresel etkilerden kolaylıkla etkilenmesi ve kuantum durumlarının çökerek istenen hesaplamaların tamamlanamaması sebebiyle Microsoft, topolojik özellikleri kuantum hesaplamaya uygulayarak kübitin bilgiyi korumasına yardımcı olan bir koruma düzeyi eklemeyi hedeflemektedir. Topolojik kübitler bu ekstra koruma düzeyini elektron bölünmesi yöntemi ile kuantum bilginin her iki yarıda da depolanarak veri yedekliliğine benzer şekilde davranması ve elektronun bir yarısı enterferansa maruz kalsa bile elektronun diğer yarısında hesaplamanın devam etmesine imkan tanıyacak şekilde bilgi depolanması ya da temel durum dejenerasyonu olarak bilinen kübitlerin iki temel duruma sahip olacak şekilde tasarlanması yolu ile gerçekleştirebilmektedir. Topolojik kübitlerin iki ayrı noktada bulunan değerleri sayesinde gürültü koruması sağlayarak kuantum bilgisayarları dış müdahalelere karşı daha dayanıklı olması ve daha uzun, karmaşık hesaplamaları tamamlamasına yardımcı olması beklenmektedir. (Microsoft, 2018)

Topolojik kuantum bilgisayarlar henüz gelişim aşamasında olduğundan diğer kuantum bilgisayar türlerine kıyasla daha düşük sayıda kübite sahiptir. Ancak daha fazla topolojik kübitin oluşturulabilmesi halinde kuantum sisteminin dayanıklılığı ile daha az kübite ihtiyaç duyulacak olması gibi sebeplerle potansiyel faydasının çok büyük olması beklenmektedir. (Grimes, 2020, s. 50)

2.1.3.5. Tuzaklanmış İyon Kuantum Bilgisayarları

İyon, eşit olmayan sayıda proton ve elektrona sahip atomdur; bu nedenle net pozitif veya negatif elektrik yüküne sahiptir. Uzun koherans süresine sahip olan ve bu sayede daha uzun ve karmaşık hesaplama işlemlerini gerçekleştirmeye imkan sağlayan

tuzaklanmış iyon kuantum bilgisayarlarında kullanılan iyonları oluşturabilmek içinse; bir vakum içerisinde yer alan atomların lazer ışınları aracılığıyla çok yüksek sıcaklıklara kadar ısıtılması ve bu ısıtılmış atomlara elektron fırlatılarak bir elektron kaybettirilmesi, dolayısıyla pozitif yük elde etmesinin sağlanması gerekmektedir. Oluşturulan iyonu oda sıcaklığındaki bir silikon çipin üzerinde tutabilmek içinse bir vakum sistemi ile elektromanyetik alan kullanılmakta, hareketleri ve dolanık kübitler oluşturup oluşturmadığı lazer ışınları ile kontrol edilebilmekte, iyonların veya dolanık çiftlerin hareketi ile kuantum bilgi aktarımı gerçekleştirilebilmektedir. (Grimes, 2020, s. 51)

Tuzaklanmış iyon kuantum bilgisayarları oda sıcaklığında çalışabilmekte, on dakika gibi uzun bir süre dekoherans durumuna geçmeden hesaplama işlemine devam edebilmekte, yüksek doğrulukla dolanıklık özelliği gösterebilmekte ve çok daha hassas ölçümler gerçekleştirebilmektedir. Ancak eşzamanlı hapsedilen iyonların sayısının artarken her birini ayrı ayrı kontrol etmenin ve yüksek doğrulukla ölçmenin zorlaşması bu kuantum bilgisayar türünün temel problemini oluşturmaktadır. Bununla birlikte, uzun bir süre dekoherans durumuna geçmeden hesaplama işlemine devam edebilmesi en büyük avantajı olarak görülse de daha uzun yürütme süresine sahip olması diğer kuantum bilgisayar türlerine kıyasla daha yavaş olmasına sebebiyet vermektedir. (Grimes, 2020, s. 52)

2.1.4. Kuantum Hesaplamanın Kriptografiye Etkisi

Veri iletimi ve depolanmasında gizlilik, bütünlük, doğrulanabilirlik ve inkar edilemezlik özelliklerinin sağlanmasında kullanılan asimetrik şifreleme yöntemlerinin, 1982 yılında Richard Feynman tarafından ortaya atılan kuantum hesaplama yöntemleri ile büyük oranda işlevsiz hale geleceği, simetrik şifreleme yöntemlerinin ise daha büyük anahtar yapılarının kullanılmaması halinde belirli kuantum algoritmalarına karşı direnç gösteremeyeceği öngörülmektedir.

Gönderici ile alıcının genel ve özel olmak üzere iki anahtara sahip olduğu, iletilmek istenen mesajın genel anahtar ile şifrelendiği; iletilen şifrelenmiş verinin şifresinin

alıcının özel anahtarının kullanılması yolu ile çözülebildiği ve elektronik imza altyapısının da temelini oluşturan asimetrik şifreleme algoritmalarının güvenliği, RSA algoritmasında kullanılan büyük asal sayıları çarpanlarına ayırmanın zorluğu ve Diffi-Hellman ile Eliptik Eğri algoritmalarında kullanılan ayrık logaritma problemi gibi hesaplama problemlerine dayanmaktadır. Ancak, 1994 yılında Peter Shor tarafından yayımlanan makale ile; büyük tam sayıları çarpanlara ayırmanın kuantum bilgisayarlar ile mümkün olduğu kanıtlanmış (Shor P. W., 1994), Vazirani tarafından ise Shor algoritmasının metodolojisi ayrıntılı olarak incelenerek ayrık logaritma problemlerinde de kullanılabileceği ortaya konmuştur (Vazirani, 1998).

Lov Grover tarafından ise sıralanmamış veritabanlarını aramak için kuantum bilgisayarları kullanan bir algoritma oluşturmuş ve simetrik şifreleme algoritmalarının çözülebilmesi amacıyla olası uygulamalar üzerine çalışmalar gerçekleştirilmiştir (Grover, 1996) (Vasileios, 2018). Bu çalışmalar sonucunda kuantum hesaplama yöntemlerinin simetrik algoritmaları tamamen geçersiz kılmadığı ancak klasik kaba kuvvet algoritmalarına göre karekök hızlandırma sunan Grover algoritması nedeniyle daha büyük anahtar boyutlarına ihtiyaç duyulabileceği değerlendirmesi yapılmıştır (Vasileios, 2018). Klasik saldırılara karşı güvenliği sağlamak için NIST, 80 bit veya daha altı güvenlik seviyesinde yer alan şifreleme sistemlerinden 112 veya 128 bit güvenlik sağlayan anahtar boyutlarına ve algoritmalara geçişi tavsiye etmiş (NIST 800-131A, 2015), AES şifreleme algoritmasının 192 veya 256 bitlik anahtar boyutlarıyla kullanılması halinde kuantum hesaplamalarına dayanıklı olduğu kabul edilmiştir. Girdi olarak anahtar yerine orijinal mesaja dayalı, sabit uzunlukta bir özet değer oluşturarak kullanılan anahtarsız şifreleme algoritmalarının güvenliği de simetrik şifreleme algoritmalarına benzer şekilde boyutu ile ilişkili olup SHA-2 ve SHA-3 şifreleme algoritmaları haricinde kuantum hesaplama yöntemlerine karşı dirençli olmadığı değerlendirilmektedir. (Vasileios, 2018)

Bu sebeple kuantum üstünlüğüne ulaşmış bir kuantum bilgisayarın anahtar değişimi, şifreleme ve elektronik kimlik doğrulama gibi birçok güvenli iletişim yöntemini tehdit etmektedir. Kuantum hesaplamanın yaygın olarak kullanılan kriptografik algoritmalar üzerindeki etkisi Tablo 2.1'de, yaygın olarak kullanılan kriptografik algoritmaların klasik ve kuantum güvenlik seviyesi karşılaştırması ise Tablo 2.2'de gösterilmektedir.

Tablo 2.1 ile Tablo 2.2'de yer verilen algoritmalarda; RSA, ECC, DSA gibi asimetrik anahtarlı algoritmaların kuantum bilgisayarlarda Shor algoritmasının uygulanması ile savunmasız kalması sebebiyle anahtar boyutundan bağımsız olarak güvensiz olduğu kabul edilirken AES gibi simetrik anahtarlı algoritmalar ile anahtarsız algoritmaların kuantum bilgisayarlarda Grover algoritmasının uygulanması ve klasik kaba kuvvet algoritmalarına göre karekök hızlandırma sağlanması sebebiyle anahtar boyutlarının güvenlik seviyesinin bit cinsinden yarıya düşmesi sebebiyle 192 bit altındaki anahtar boyutlarının güvensiz olduğu kabul edilmektedir.

Tablo 2.1. Kriptografik algoritmalar üzerindeki kuantum hesaplama etki analizi

Kriptografik Algoritma	**Tür**	**Amaç**	**Kuantum Hesaplamanın Algoritmaya Etkisi**
AES-256	Simetrik Algoritma	Şifreleme	Güvenli
SHA-256, SHA-3	Anahtarsız Algoritma	Özetleme Fonksiyonları	Güvenli
RSA	Asimetrik Algoritma	İmzalama, Anahtar Oluşturma	Güvenli Değil
ECDSA, ECDH (Eliptik Eğri Kriptografisi)	Asimetrik Algoritma	İmzalama, Anahtar Değişimi	Güvenli Değil
DSA (Dijital İmza Algoritması)	Asimetrik Algoritma	İmzalama, Anahtar Değişimi	Güvenli Değil

Kaynak: NIST,2015, Vasileios, 2018

Tablo 2.2. Yaygın olarak kullanılan kriptografik algoritmalar için klasik ve kuantum güvenlik seviyelerinin karşılaştırılması

Şifreleme Algoritması	**Anahtar Boyutu**	**Etkin Anahtar Gücü (Bit Cinsinden)/Güvenlik Seviyesi**	
		Klasik Hesaplama	**Kuantum Hesaplama**
RSA-1024	1024	80	0 (Güvenli Değil)
RSA-2048	2048	112	0 (Güvenli Değil)
ECC-256	256	128	0 (Güvenli Değil)
ECC-384	384	256	0 (Güvenli Değil)
AES-128	128	128	64 (Güvenli Değil)
AES-256	256	256	128 (Güvenli)

Kaynak: Vasileios, 2018

2.1.5. Kuantum İletişim

Kuantum iletişim, kuantum mekaniği yasalarının kullanılarak; bilginin ve kuantum kaynaklarının güvenli bir şekilde iletilebilmesi amacıyla kuantum bilgisayarların, simülatörlerin ve sensörlerin birbirine bağlandığı bir iletişim ağını ifade etmektedir. Kuantum iletişimin gerçekleştirilerek uzun vadede ulaşılmak istenen hedef, hataya dayanıklı kuantum bilgisayarlar geliştirmek, aynı zamanda bu bilgisayarları birbirine bağlamak ve aralarında kuantum bilgi alışverişi yapmak; aslında hem kuantum hesaplama hem de kuantum iletişim yeteneklerinden yararlanarak bir 'kuantum interneti' geliştirmektir (AvrupaKomisyonu, 2023).

Kuantum iletişim ağ yapısı, klasik ağ yapısında olduğu gibi iletişim bağlantıları ve ağ düğümlerinden oluşmakta; iletim mesafesini uzatmak için kullanılan tekrarlayıcılar ve ağları birbirine bağlamak ile en uygun yolu belirlemek için kullanılan yönlendiriciler aracılığıyla optimize edilebilmekte, iletişim bağlantıları fiber optik kablolar veya serbest-uzay iletim ortamı olabilmektedir. Klasik ağ yapısından tek farkı ise tüm bu bileşenlerin kuantum mekaniği yasaları uyarınca yeniden tasarlanmış olmasıdır.

Kuantum iletişimi gerçekleştirmede karşılaşılan en büyük zorluklardan biri veri gürültüsüne ve kaybına neden olan kuantum dekoheransıdır. Bu sebeple iletim bağlantıları kuantum ağları için büyük önem taşımaktadır. Kablolu kuantum iletiminde günümüzde kullanılan fiber optik kablolar ve foton tabanlı kübitler kullanılabilmekle birlikte daha uzak mesafelere ve daha yüksek veri iletim kalitesine (uzun mesafe, yüksek veri iletim hızı ve düşük hata oranı) ulaşabilmek için çalışmalar gerçekleştirilmektedir. Diğer bir iletim ortamı olan serbest-uzay ortamında ise düşük foton emiliminin olması ve atmosferik katmanın aşılması ile birlikte kuantum dekoheransının ihmal edilebilir seviyelere indirgenmesi sebebiyle uydu tabanlı kuantum ağları, fiber optik kablolara kıyasla çok daha geniş bir iletişim menzili sunmakta; ancak kablosuz ağların doğal koşullardan, atmosferik türbülanstan ve gün ışığında yoğun arka plan ışık gürültüsünden kaynaklanan girişimlerden etkilenebilmesi sebebiyle düşük veri iletim hızı ve yüksek gecikmeye yol açabilmektedir. Kablosuz kuantum ağlarının performansı; optik kaynaklar, kuantum işlemciler ve yönlendirme protokolleri gibi kuantum hesaplama donanım ve yazılım

gelişimine bağlı olup ağ performansını artırmak, gürültüyü en aza indirgemek ve yüksek iletim hızlarını korumak için yeni donanım ve yazılım paradigmaları (yeni malzemeler ve hesaplama modelleri gibi) geliştirilmektedir. Fiber optik kablo bağlantıları ile uydu tabanlı iletim bağlantılarının birlikte kullanımı ise kuantum internetinin inşa edilmesinde önemli bir fırsat sunmaktadır. (A. Singh K. D., 2021)

Kuantum iletim ağlarında veri kaybının ve dekoherans durumuna geçişin uzun mesafeli iletişimi zorlaştırması sebebiyle; yol boyunca bitişik düğümler arasındaki dolanıklığı yeniden üreterek gönderici ve alıcı arasında uçtan uca dolanıklık oluşturulmasını sağlayan kuantum tekrarlayıcılar kullanılmaktadır. Bitişik düğümler arasındaki kuantum iletişimi genellikle dolanıklık aracılığıyla gerçekleştirilmektedir. Ancak, iki taraf arasındaki dolanıklık iletişimin gerçekleşmesinin akabinde çökmekte ve durumlarının aynı kuantum sisteminde olmaması halinde (bağlı/ilişkili değilse) dolanıklık yeniden oluşturulamamaktadır. Bu nedenle, doğrudan bağlı olmayan taraflar arasında dolanıklığı yeniden oluşturabilmek için tekrarlayıcılara ihtiyaç duyulmaktadır. Gerektiğinde, kuantum tekrarlayıcılar bilgiyi ışınlamak ve kendi belleğindeki durum ile komşu düğümün belleğindeki durum arasında dolanıklığı yeniden oluşturabilmek için kuantum bellekleri de kullanabilmektedir. (A. Singh K. D., 2021)

Klasik ağlarda olduğu gibi kuantum ağlarında da kaynak ve hedef arasındaki en iyi yolu belirlemek için yönlendiriciler kullanılmaktadır. Ancak kuantum yönlendiriciler, klasik yönlendiricilerden; iletişim bağlantılarının her kullanımdan sonra yeniden kurulmasının gerekmesi sebebiyle farklılaşmaktadır. Bir kuantum bağlantısının oluşturulabilmesi için farklı yerlerde bulunan iki kübitin dolanık hale getirilmesi gerekmektedir. Fakat oluşturulan dolanıklığın iletimin gerçekleşmesi akabinde çökmesi nedeniyle bir sonraki iletim için yeniden oluşturulması gerekmektedir. Yeniden oluşturulan bağlantıların başarılı veya başarısız olma olasılığı bulunduğundan yönlendirme stratejilerinde bağlantı kararlılığının dikkate alınması gerekmekte; seçilen bir yolun kullanılamaz hale gelmesi durumunda ise alternatif bir yolun belirlenmesi gerekmektedir. Bu sebeple kuantum yönlendiriciler kullanılarak verinin kuantum tekrarlayıcılar aracılığıyla iletilmesi sağlanmaktadır. (Z. Yang, 2023)

Kuantum anahtar dağıtımı protokolleri de kuantum iletişim kanalını kullanarak gizli anahtar oluşturulmasına imkan tanımakta, yetkisiz erişimi tespit edebilmek ve engelleyebilmek amacıyla dolanıklık ile klonlanamazlık teoremi gibi kuantum özelliklerinden yararlanmaktadır.

2.2. Kuantum Teknolojilerinin Sektörler Üzerindeki Etkisi

Kuantum teknolojilerinin, günümüzde yaygın olarak kullanılan ve güvenli olarak kabul edilen kriptografik algoritmaları kolaylıkla savunmasız hale getirecek olması mevcut iletişim sistemlerini ve veri güvenliğini tehdit etmesine rağmen daha yüksek bilgi işlem gücü ile birçok alanda gün geçtikçe daha da önem kazanmakta, var olan teknolojik gelişmeleri hızlandırarak insanlığın yaşam kalitesini artırması beklenmektedir. Bu bölümde kuantum teknolojilerinin etki edebileceği bazı sektörler incelenmiştir.

- **Tıp, Biyoloji ve Genetik Üzerine Etkisi:** Kuantum teknolojilerinin daha verimli klinik ilaç keşfine imkan tanıması, karmaşık hastalıkların mekanizmalarının aydınlatılmasına yardımcı olması, canlıların biyolojisinin ve genomunun daha fazla aydınlatılmasına katkıda bulunması beklenmektedir. Günümüzde kullanılan klasik bilgisayarlar ile basit bir moleküler sistemin dinamiklerini simüle etmenin imkansız olması nedeniyle ilaç geliştirme süreci, keşif, klinik öncesi ve klinik fazları gibi hayvanlar ve insanlar üzerinde yıllarca süren klinik testlerin gerçekleştirilmesinin akabinde tamamlanmaktadır. Ancak kuantum simülasyon ve kuantum hesaplama teknolojilerinin sayesinde ilaç etkileşimleri gibi mikroskobik süreçler simüle edilirken ele alınan hesaplama probleminin zorluğu üstel zaman yerine polinom zamanda çözümlenebilir hale geldiğinden ilaç tasarımında dönüm noktası niteliğinde bir sıçrama yaşanması, mevcut biyomedikal teknolojisi ile ulaşılması mümkün olmayan yeni teknik ve süreçlere zemin hazırlaması beklenmektedir. Bunun yanı sıra, canlı hücre dinamiği üzerine hassas çalışmalar ve ölçümler yapılmasını mümkün kılan kuantum optiği teknolojisi ile canlı organizmaların moleküler düzeyde tahrip/manipüle ve kontrol edilmesine de olanak tanıyarak uygulanacak

tedaviye yönelik etkin kararlar alınmasında kullanılması öngörülmektedir (IDB, 2019).

- **Ekonomi ve Finans Üzerindeki Etkisi:** Kuantum teknolojilerinin ekonomi ve finans alanında da köklü değişikliklere sebep olacağı öngörülmektedir. Kuantum bilgisayarlar ile simülatörlerin karmaşık sorunları çözme ve çok sayıda olasılığı hızlı ve etkili bir şekilde işleme kapasitesinin kuantum algoritmaların kullanılmasına imkan tanıyarak finansal modeller oluşturulmasına, simüle edilmesine ve geliştirilmesine yardımcı olması; kuantum bilgisayarlar ile paralel işlem gerçekleştirilebilmesi sayesinde çeşitli seçeneklerin sırayla değil eşzamanlı olarak değerlendirilmesi ve böylelikle kaynakların çok daha verimli şekilde kullanılması beklenmektedir (IDB, 2019).
- **Sürdürülebilir Enerji ve Tarım Üzerindeki Etkisi:** Gübre üretimi için gerekli olan amonyak bileşiğinin elde edilmesi için aşırı basınç ve sıcaklık koşulları altında azot atomunun ayrıştırılması gerekmekte olup bu süreç dünya enerjisinin %2'sini tüketmektedir. Kuantum bilgisayarlar sayesinde amonyak sentezi sürecinin moleküler düzeyde simüle edilerek nitrojenaz enziminin kullanılması yöntemi ile oda sıcaklığında amonyak elde edileceği, benzer veri işleme yöntemlerinden enerji sektöründe de yararlanılacağı ve kaynakların çok daha verimli bir şekilde kullanılacağı öngörülmektedir (IDB, 2019).
- **Siber Güvenlik Üzerindeki Etkisi:** Günümüzde yaygın olarak kullanılan kriptografik algoritmaların kuantum hesaplama teknolojilerine karşı savunmasız olması siber güvenliği tehdit ederken bahse konu teknolojilerin makine öğrenmesi, derin öğrenme ve yapay sinir ağları gibi yapay zeka uygulamaları ile birlikte kullanımı siber risklerin etkin yönetiminde umut vadetmektedir. Kriptografik algoritma güvenliğinin kuantum çağında da sağlanabilmesi amacıyla güvenliği kuantum mekaniği yasalarınca garanti edilen kuantum anahtar dağıtım yöntemleri ile hem klasik hem de kuantum bilgisayarlar tarafından çözülmesi mümkün olmayan matematiksel tekniklerin kullanılmasıyla oluşturulan kuantum güvenli kriptografik algoritmalara yönelik çalışmalar devam etmekte; ülkelerin bilgi güvenliğinin korunmaya devam edebilmesi amacıyla yeterli bilgi işlem kapasitesine ulaşmış bir kuantum bilgisayarın inşasından önce anılan yöntemleri bilgi sistemlerine entegre etmesi beklenmektedir. Diğer yandan kuantum hesaplama

teknolojilerinin sahip olduğu olağanüstü hesaplama yeteneğinin mevcut yapay zeka uygulamaları ile birlikte kullanılmasıyla birlikte örüntü tanıma, veri analizi ve problem çözme kapasitesinde artış sağlanarak:

- Anomali tespitinin başarılı bir şekilde gerçekleştirilerek gerçek zamanlı kötü amaçlı yazılımların tespit edilmesinde, potansiyel tehditlerin daha doğru bir şekilde tanımlanmasında, sistemlerin dayanıklılığının artırılarak siber saldırılara karşı temel bir savunma aracı olarak kullanılmasında,
- Kurum ve kuruluşların internet altyapısı üzerinden gerçekleştirdiği trafiğin siber saldırılara karşı korunmasında kullanılan izinsiz giriş önleme sistemlerine uygulanmasında,
- Ağ güvenliği protokollerinin çeşitli potansiyel güvenlik tehditlerini tanıyabilen ve elimine edebilen teknikleri uygulayabilecek şekilde geliştirilmesinde,
- Kriptografik protokollerin zayıflıklarının belirlenebilmesinde ve optimize edilmesinde,

kullanılması beklenmektedir (Bikku, Praveen, & Sirisha, 2024) (Shara, 2023).

- **Diğer Uygulamalar:** Navigasyon uygulamalarının gerçek zamanlı olarak topladığı büyük miktardaki verinin analizi ile araçların ve insanların hareketinin mevcut verilere dayanarak simüle edilmesi, matematiksel modellerin optimizasyonu ile optimum rotaların daha yüksek doğrulukla önerilmesi, acil durum araçlarına rota oluşturabilmek için trafik ışıklarının da koordinasyonunun sağlanması beklenmektedir. Bunun yanı sıra, molekül simülasyonuna olanak sağlaması sayesinde yeni maddelerin sentezinde, atmosferik olayları anlamlandırma kapasitesindeki artış ile daha doğru meteorolojik tahminlerde bulunulmasında, olgular arasındaki korelasyonun tespiti ile kantitatif ticaret stratejilerinin geliştirilmesinde, uydu, füze, roket, uçak ve gemi gibi araçların varmaya programlandığı konuma ulaşabilmesini sağlayan güdüm sistemlerinin daha duyarlı hale getirilmesinde, çığ, deprem, volkanik patlama ve tsunami gibi kütleçekimsel etkilerin etkin bir şekilde algılanarak uyarı sistemlerinin oluşturulmasında kullanılması öngörülmektedir (IDB, 2019) (BAE, 2023).

3. KUANTUM BİLİMİNDE YAŞANAN GELİŞMELER SONRASI KRİPTOGRAFİ

Kuantum bilgisayarların her ne kadar insanlık için yeni ve büyük fırsatlar sunması beklense de günümüzde yaygın olarak kullanılan AES, 3DES, RSA, Diffie Hellman ve ECC gibi kriptografik algoritmalarının; kuantum üstünlüğüne ulaşmış bir kuantum bilgisayarın kullanılması ve Grover'ın arama algoritması ile Shor'un çarpanlara ayırma algoritmasının uygulanması yöntemi ile makul zaman aralıklarında çözümlenebilir hale gelerek savunmasız kalacak olması ülkelerin ulusal bilgi güvenliğini tehdit etmektedir. Bu sebeple yaşanacak kuantum devriminin olumsuz etkilerinden korunabilmek için kuantum sonrası kriptografi uygulamaları üzerine araştırmalar şimdiden başlatılmıştır.

Kuantum sonrası kriptografi temel olarak iki güvenli haberleşme protokolünü temsil etmektedir. Birincisi kuantum güvenli kriptografi olarak adlandırılan ve klasik kriptografik algoritmalarda olduğu gibi matematiksel problemlerin çözümünün zorluğuna dayandırılan ancak yalnızca klasik bilgisayarların değil, kuantum bilgisayarların da saldırılarına dirençli matematiksel tekniklerin üzerine inşa edilen yeni kriptografik yöntemlerdir. İkincisi ise temeli kuantum mekaniği ilkelerine dayanan ve kuantum iletişim kanallarının kullanılarak gizli anahtar dağıtımına imkan tanıyan kuantum anahtar dağıtımı protokolleridir.

3.1. Kuantum Güvenli Kriptografi

Kuantum güvenli kriptografi, günümüz klasik bilgisayarları tarafından da kullanılabilen aynı zamanda kuantum bilgisayarlara karşı güvenlik sağlayan şifreleme algoritmalarının geliştirildiği kriptografi alanıdır. Asimetrik kriptografi algoritmalarının güvenliğini sağlayabilmek için matematikçiler ve kriptograflar tarafından geliştirilmeye çalışılan yeni sayı teorisi problemleri yerini kuantum bilgisayarlar tarafından kolayca çözümlenemeyecek matematiksel problemlerin geliştirilmesine bırakmıştır. Bu çerçevede, 2016 yılında NIST tarafından başlatılan kuantum güvenli kriptografi standardizasyon süreci ile güçlü kuantum bilgisayarlar oluşturulmadan önce yerine yenilerini koymak üzere yeni elektronik imza şemaları,

anahtar üretimi ve değişimi için kullanılan anahtar kapsülleme mekanizmaları ve asimetrik anahtar şifreleme şemaları aranmaya başlanmıştır. Bu yarışma ile kuantum güvenli kriptografik algoritmaların uygulamalarda daha etkin bir şekilde yer alması ve klasik açık anahtarlı sistemlerin yerine uygulanabilir alternatif çözümler sunması beklenmektedir.

Kuantum güvenli kriptografi aşağıdaki ana yaklaşımları içermektedir;

- Kod Tabanlı Kriptografi (Code-based Cryptography)
- Özet Tabanlı Kriptografi (Hash-based Cryptography)
- Kafes Tabanlı Kriptografi (Lattice-based Cryptography)
- İzojeni Tabanlı Kriptografi (Isogeny-based Cryptography)
- Çok Değişkenli Polinomlar Tabanlı Kriptografi (Multivariate-System Based Cryptography)

3.1.1. Kod Tabanlı Kriptografi

Cebirsel kodlama veya hata düzeltme kodları olarak da bilinen kod tabanlı kriptografi, orijinal içeriği şifreleyecek/gizleyecek şekilde düz metin içeriğinde kasıtlı olarak "hata" (yani şifreleme) oluşturan matematiksel algoritmalara dayanan, saldırılara karşı dirençli ve uzun zamandır bilinen bir şifreleme yöntemidir. Örneğin, gönderici tarafından şifrelenecek düz metnin *"1111"* olduğunu varsayarsak kod tabanlı kriptografi yöntemi ile içeriğe kasıtlı olarak hatalar eklenerek iletilmek istenen mesaj alıcıya hatalı olarak *"011101"* şeklinde iletilmektedir. Sonrasında alıcı tarafındaki hata düzeltme işlemi ile hatalar ortadan kaldırılarak orijinal *"1111"* içeriği güvenilir bir şekilde yeniden üretilmektedir. (Grimes, 2020)

Kod tabanlı kriptografi, hata düzeltici kodlar teorisini dayanak aldığından ilgili anahtarı bilmeden hataları çözmek çok zordur. 1970 yıllarında Rus matematikçi Valery Denisovich Goppa, geometrik şekilleri ve kombinasyonlarını hata düzeltici kodlara eklemiş ve günümüzde Goppa kodları olarak bilinen kodları üretmiştir. Goppa kodları, çoğu kod tabanlı kriptografik yöntemin dayandırıldığı ve NIST'in düzenlemiş olduğu

kuantum güvenli kriptografi yarışmasında en başarılı kod tabanlı şifreleme yöntemlerinden biri olan klasik McEliece'in temelini oluşturmaktadır. (ENISA, 2021)

3.1.2. Özet Tabanlı Kriptografi

Değişken uzunluktaki dizeleri sabit uzunluktaki dizelerle eşleyerek içeriği benzersiz bir temsili bit kümesine dönüştüren ve tek yönlü bir işlev olan özet fonksiyonlarına dayandırılarak uygulanan özet tabanlı kriptografik yöntemler, elektronik imza şemalarında sıklıkla kullanılmaktadır. Özet tabanlı kriptografinin, aynı tek seferlik anahtarı iki farklı giriş için tekrarlamasının saldırganlara özel anahtar hakkında güçlü bir fikir verebilecek olması nedeniyle benzersiz özet çıktılarının alınabilmesi amacıyla ya elektronik imzanın boyutu artırılmakta (bu durum performans ve depolama sorunlarına yol açabilmektedir) ya da kullanılan her gizli anahtarın izini sürerek tekrar kullanılmasını engelleyen durum bilgili özetler kullanılmaktadır. NIST, durum bilgisi bulunan imza şemalarını standartlaştıran raporunu halihazırda yayınlamış olmakla birlikte düzenlemiş olduğu yarışmada durum bilgisi içermeyen özet tabanlı elektronik imza şeması SPHINCS+ kuantum dirençli şifreleme yöntemleri arasında yer almıştır. (ENISA, 2021)

3.1.3. Kafes Tabanlı Kriptografi

Kafes tabanlı kriptografi, çok boyutlu bir uzayda geometrik yapılar oluşturan kafeslerin matematiksel özelliklerine dayandırılan bir kriptografik şema türü olmakla birlikte güvenliklerinin temeli, girdi olarak verilen bir kafeste sıfırdan farklı en kısa kafes vektörünün bulunmasının amaçlandığı En Kısa Vektör Problemlerinin (Shortest Vector Problems- SVP) hesaplama zorluğuna dayanmaktadır. Algoritmaların uygulanmasında nispeten verimli ve en kötü durumda kanıtlanabilir güvenlik seviyesine sahip olan kafes tabanlı kriptografinin kuantum güvenli kriptografi algoritmaları içerisinde potansiyel vadeden bir çözüm sunması beklenmektedir. (Kumar, 2022)

NIST tarafından düzenlenen yarışmanın üçüncü turunda en fazla kafes tabanlı kriptografi algoritmalarına yer verilmiş ve anahtar kapsülleme mekanizmaları için CRYSTALS-KYBER, NTRU ve SABER olmak üzere üç algoritma; elektronik imzalar içinse CRYSTALS-DILITHIUM ve FALCON olmak üzere iki algoritma finalist olarak ilan edilmiştir. FrodoKEM ve NTRU Prime ise Anahtar Kapsülleme Mekanizmaları için alternatif adaylar olarak ilan edilmiştir.

3.1.4. İzojeni Tabanlı Kriptografi

İzojeni tabanlı kriptografi, eliptik eğrilerin özellikleri ve aynı sayıda noktaya sahip iki eğri arasında izojeni oluşturmanın zorluğuna dayanan ve diğer kuantum güvenli protokollere kıyasla çok daha küçük bir anahtar boyutuna gereksinim duyan kriptosistemlerdir. (Kumar, 2022)

2005 yılında tanıtılan ve kuantum güvenli algoritmalar arasında en yeni üyesi olan izojeni tabanlı kriptografi protokollerinden Süpersingüler İzojen Tabanlı Anahtar Değişimi (Supersingular Isogeny Key Exchange- SIKE), NIST tarafından düzenlenen yarışmanın üçüncü turunda yer alabilen izojeni tabanlı tek algoritma olmakla birlikte finalist değil alternatif aday olarak ilan edilmiştir. (ENISA, 2021)

3.1.5. Çok Değişkenli Polinomlar Tabanlı Kriptografi

Çok değişkenli polinomlar tabanlı kriptografi, sonlu bir alan üzerinde bulunan çok değişkenli denklem tabanlı bir genel anahtar şifreleme sistemi olup güvenliği, çok değişkenli polinom denkleminin çözümünün zor denklem sınıfında yer aldığının kanıtlanmış olmasına dayanmaktadır. NIST tarafından düzenlenen yarışmanın üçüncü turunda bu şifreleme sistemi üyelerinden Rainbow finalist, GeMSS ise yedek olarak açıklanmıştır. Ancak Rainbow'un üçüncü tur esnasında önemli saldırılara maruz kalması ve güvenlik zafiyetinin oluşması nedeniyle güvenliğinden emin olunamamış ve standardizasyon için seçilmemiştir. (NIST, 2022)

3.2. NIST Kuantum Sonrası Kriptografi Standardizasyon Süreci

Kuantum bilgisayarların yapımına yönelik istikrarlı bir ilerleme kaydedilmesi ve bu ilerlemenin yaygın olarak kullanılan birçok asimetrik anahtarlı kripto sistemin; özellikle çarpanlara ayırma, ayrık logaritma ve eliptik eğri kriptografisine dayanan anahtar oluşturma şemaları ile elektronik imza güvenliğini tehdit etmesi sebebiyle hem kuantum hem de klasik bilgisayarlarda koruma sağlayabilecek asimetrik anahtarlı kripto sistemler bulmaya yönelik araştırmalar yoğunlaşmıştır. Aynı amaca yönelik olarak NIST, kuantum bilgisayara dirençli asimetrik anahtarlı kriptografik algoritmaları seçebilmek için kamuya açık, yarışma benzeri bir süreç başlatmış ve bu süreci "NIST Kuantum Sonrası Kriptografi Standardizasyon Süreci" olarak adlandırmıştır.

Söz konusu standardizasyon süreci ile kuantum bilgisayarların ortaya çıkmasından sonrası da dahil olmak üzere, öngörülebilir gelecekte ABD'nin ulusal bilgi güvenliğini koruyabilmesi hedeflenmekle birlikte daha önce yayınlanmış olan Dijital İmza Standardı[1], Ayrık Logaritma Kriptografisi Kullanarak Çift Yönlü Anahtar Oluşturma Şemaları için Tavsiye[2] ve Tamsayı Çarpanlarına Ayırma Kriptografisi Kullanarak Çift Yönlü Anahtar Oluşturma için Tavsiye[3] gibi standartların güçlendirilmesi amaçlanmaktadır.

NIST, Aralık 2016'da Kuantum Sonrası Kriptografi Standardizasyon Sürecine başvurular için halka açık bir çağrı yayımlamış[4], Kasım 2017'deki son başvuru

---

[1] National Institute of Standards and Technology (2013) Digital signature standard (DSS) (U.S. Department of Commerce, Washington, D.C.), Federal Information Processing Standards (FIPS) Publication 186-4. https://doi.org/10.6028/NIST.FIP S.186-4

[2] Barker EB, Chen L, Roginsky AL, Vassilev A, Davis R (2018) Recommendation for pair-wise key-establishment schemes using discrete logarithm cryptography (U.S. Department of Commerce, Washington, D.C.), Special Publication 800-56A Revision 3. https://doi.org/10.6028/NIST.SP.800-56Ar3

[3] Barker EB, Chen L, Roginsky AL, Vassilev A, Davis R, Simon S (2019) Recommendation for pair-wise key-establishment using integer factorization cryptography (U.S. Department of Commerce, Washington, D.C.), Special Publication 800-56B Revision 2. https://doi.org/10.6028/NIST.SP.800-56Br2

[4] National Institute of Standards and Technology (2016) Announcing request for nominations for public-key post-quantum cryptographic algorithms. Federal Register 81(244):92787–92788. https://federalregister.gov/a/2016-30615.

tarihinden önce 82 aday algoritma sunulmuş; hem başvuru koşullarını hem de minimum kabul edilebilirlik kriterlerini karşılayan 69 aday standardizasyon sürecinin ilk turuna kabul edilmiştir. Adayların bir yıl süren inceleme sürecinin ardından Ocak 2019'da ikinci değerlendirme turuna geçmek üzere hem iç analiz hem de kamuoyu görüşü göz önünde bulundurularak 26 algoritma seçilmiş, ilk tura kıyasla daha geniş bir topluluk ile yapılan değerlendirmeler sonucunda Temmuz 2020'de üçüncü tura geçmek üzere 7 finalist ve 8 yedek algoritma seçilmiş[5], üçüncü turun sonunda finalistlerin; dördüncü tur sonunda ise alternatif adayların standartlaştırılması hedeflenmiştir.

Üçüncü tur Temmuz 2020'de başlamış ve yaklaşık 18 ay sürmüştür. Bu turda; aday algoritmaların güvenli olduğunu doğrulayabilmek amacıyla kullanılan teorik ve ampirik kanıtların kapsamlı analizi yapılmış, çeşitli yazılım ve donanım platformlarında optimize edilmiş uygulamalar kullanılarak performansları değerlendirilmiş ve Kuantum Sonrası Kriptografi Standardizasyon Süreci sonucunda standartlaştırılacak olan ilk algoritmalar seçilmiştir. Bu kapsamda; açık anahtar kapsülleme mekanizması olarak CRYSTALS-KYBER, elektronik imza algoritmalarında CRYSTALS-Dilithium (uygulanacak birincil algoritma olarak önerilmiştir), FALCON ve SPHINCS$^+$ finalist olarak seçilmiştir. Bununla birlikte açık anahtar kapsülleme mekanizmalarından BIKE, Klasik McEliece, HQC ve SIKE alternatif aday olarak belirlenmiş olup dördüncü turun sonunda standardizasyon için değerlendirileceği ifade edilmiştir.

NIST tarafından standardizasyon ve dördüncü turda değerlendirilmek üzere alternatif aday olarak belirlenen anahtar kapsülleme mekanizmaları algoritmalarının listesine Tablo 3.1'de, üçüncü tur sonuçlarına göre standardizasyon için seçilen elektronik imza algoritmalarına ise Tablo 3.2'de yer verilmektedir.

[5] Alagic G, Alperin-Sheriff J, Apon D, Cooper D, Dang Q, Kelsey J, Liu YK, Miller C, Moody D, Peralta R, Perlner R, Robinson A, Smith-Tone D (2020) Status report on the second round of the NIST post-quantum cryptography standardization process (National Institute of Standards and Technology, Gaithersburg, MD), NIST Interagency or Internal Report (IR) 8309. https://doi.org/10.6028/NIST.IR.8309

Tablo 3.1. NIST tarafından standardizasyon ve dördüncü turda değerlendirilmek üzere alternatif aday olarak belirlenen Anahtar Kapsülleme Mekanizmaları Algoritmalarının listesi

Algoritma Adı	Güvenlik	Verimlilik	Genel Değerlendirme	Sonuç
CRYSTALS-KYBER	Kafes tabanlı kriptografiye dayalı güçlü teorik güvenlik temeli sunar.	Birçok farklı uygulamadaki performansı yeterli düzeydedir.	Yazılım, donanım ve hibrit ayarlardaki genel performansı mükemmeldir.	Üçüncü turda finalist olarak belirlenmiştir.
BIKE	Kod çözme problemlerini çözmenin zorluğuna bağlıdır	Performansı çoğu uygulama için uygun olacaktır.	Genel performansına ilişkin değerlendirmeler devam etmektedir.	Alternatif aday olarak belirlenmiş olup dördüncü turun sonunda standardizasyon için değerlendirilecektir.
Klasik McEliece	Rastgele kodların kodunu çözmenin ve ayrıca karıştırılmış Goppa kodlarını rastgele kodlardan ayırmanın zorluğuna dayanır.	NIST standardizasyon süreci adayları arasında en küçük şifreli metne sahiptir	Güvenliğinden emin olunsa da yeterli sayıda uygulama için en iyi seçeneği temsil edip etmediği belirsizdir.	Alternatif aday olarak belirlenmiş olup dördüncü turun sonunda standardizasyon için değerlendirilecektir.
HQC	Eşlik uyuşmazlığı sorunu ile ilişkili kod çözme problemi zorluğuna dayanır.	Şifreli metin ve açık anahtarları BIKE şifreli metin ve açık anahtarlarının 1.5-2.9 kat daha büyüktür. Ancak performans olarak en iyi anahtar kapsülleme mekanizması alternatiflerinden biridir.	Genel performansı ideal olmasa da kabul edilebilir düzeydedir.	Alternatif aday olarak belirlenmiş olup dördüncü turun sonunda standardizasyon için değerlendirilecektir.
SIKE	Eliptik eğrilerin özellikleri ve aynı sayıda noktaya sahip iki eğri arasında izojeni oluşturmanın zorluğuna dayanmaktadır.	Nispeten düşük iletişim maliyetleri vardır. Ancak, tek bir anahtar kapsülleme/dekapsülasyon gerçekleştirme süresi nedeniyle yerleşik cihazlardaki performans sorun olabilmektedir.	Kuantum güvenli algoritmalar arasında henüz çok yeni olması sebebiyle üzerinde daha fazla çalışılması gerekmektedir.	Alternatif aday olarak belirlenmiş olup dördüncü turun sonunda standardizasyon için değerlendirilecektir.

Kaynak: NIST, 2022

Tablo 3.2. Üçüncü tur sonuçlarına göre standardizasyon için seçilen elektronik imza algoritmaları

Algoritma Adı	Güvenlik	Verimlilik	Genel Değerlendirme	Sonuç
CRYSTALS-Dilithium	Genel anahtarın gizli anahtar hakkında herhangi bir bilgiyi sızdırmadığını göstermek için yeterli olduğu bilinen Modüller üzerinde Tanımlı Hatalar ile Öğrenme (MLWE) varsayımına dayanmaktadır.	Performansı artırmak için sözde rastgelelik ve kesikli depolama tekniklerini kullanır.	Genel performansının oldukça verimli, uygulanmasının nispeten basit olduğu değerlendirmesi yapılmıştır.	Üçüncü turda finalist olarak belirlenmiş ve standardizasyon için seçilmiş olup uygulanabilecek algoritmalar arasında birincil algoritma olarak önerilmiştir
FALCON	Teorik güvenlik, NTRU kafesleri üzerinde SIS Probleminin zorluğuna dayanan QROM'da taklit edilemezlik kanıtına dayanmaktadır	Doğrulama süreci hızlı olmakla birlikte düşük bant genişliği gerektirmektedir.	Güvenliğinden emin olunan algoritma, düşük bant genişliği sayesinde belirli uygulamalar için tercih edilebilecek bir seçim olarak görülmektedir.	Üçüncü turda finalist olarak belirlenmiş ve standardizasyon için seçilmiştir.
SPHINCS$^+$	SPHINCS+'ın güvenliği, kullanılan özet fonksiyonlarının güvenliğine dayanır.	Anahtar oluşturma ve doğrulama, imzalamaktan çok daha hızlıdır	Güvenliği oldukça sağlam görünen ve standartlaştırılacak diğer imza şemalarımızdan tamamen farklı varsayımlara dayanan uygulanabilir bir imza şeması sunmaktadır.	Üçüncü turda finalist olarak belirlenmiş ve standardizasyon için seçilmiştir.

Kaynak: NIST, 2022

Bununla birlikte NIST, "Getting Ready for Post-Quantum Cryptography: Exploring Challenges Associated with Adopting and Using Post-Quantum Cryptographic Algorithms" adlı belgesini yayımlayarak;

- Birçok bilgi sistemi altyapısının kriptografik çeviklikten yoksun olması sebebiyle var olan kriptografik algoritmaların yenileriyle değiştirilmesinin zor ve uzun bir süreç gerektireceğini, sistemin altyapısında önemli değişikliklerin yapılmadan yeni kriptografik algoritmaların uygulanmasının hızlı bir şekilde gerçekleştirilmesinin mümkün olmayacağını,

- İletişimde birlikte çalışabilirliğin gerekli olması sebebiyle, kriptografik algoritmaların sistemdeki tüm bileşenlerin değişimi uygulayabilir hale gelinceye dek değiştirilemeyeceğini, bu sebeple algoritma değişiminin son derece zor olduğu ile kullanılan protokollerde, şemalarda ve altyapılarda güncellemelerin tamamlanmasının on yıllar alabileceğini,
- Kuantum hesaplama teknolojilerinin bilgisayar korsanlarının kullanımına sunulmasının, asimetrik anahtarlı kriptografik sistemlerin neredeyse tamamının savunmasız hale gelmesine sebebiyet vereceğini ve bu ihtimalin kayıt altına alınan tüm iletişimin ve depolanmış verilerin güvenliğini etkileyeceğini, böyle bir senaryonun gerçekleşmesi halinde ise depolanan verilerin korunabilmesi için kuantum güvenli kriptografik algoritma ile şifrelenmesinin ve eski kopyaların silinmesinin ya da fiziksel olarak güvence altına alınmasının gerekeceğini, kuantum güvenli şifreleme öncesinde üçüncü kişiler tarafından depolanmış olan şifreli materyalin gizliliğinin korunabilmesi içinse gerçekleştirilebilecek hiçbir işlemin olmayacağını,
- NIST'in kuantum güvenli kriptografi sürecine ilişkin başlattığı standartlaştırma sürecinin 2024 yılı içerisinde tamamlanmasının hedeflendiği, söz konusu sürecin tamamlanmasının akabinde ise standartlar ile uygulama kılavuzları üzerindeki çalışmaların hızla devam edeceğinin ancak kriptografik standartların yayımlansa dahi uygulamaya geçirilmesinin en iyi ihtimalle 5 ila 15 yıl arası veya daha fazla süre gerektireceği,
- Kurum ve kuruluşların açık anahtarlı algoritmaları yoğun bir şekilde kullanmasına rağmen söz konusu algoritmaların nerelerde kullanıldığına ilişkin bir envantere sahip olmadığı, bu durumun kuantum güvenli algoritmaların nerede kullanılması gerektiğinin belirlenmesinde ve uygulamaların önceliklendirilmesinde zorluk oluşturacağını, benzer şekilde standart geliştiren kuruluşların etkilenen standartları belirlemesinin ve kritik uygulamaların ve protokollerin tanımlamasının geçiş yol haritalarının oluşturulmasında kilit rol oynayacağı

ifade edilmiştir (NIST, 2021).

3.3. Kuantum Anahtar Dağıtımı

Kuantum hesaplama yöntemlerinin simetrik algoritmaları tamamen geçersiz kılmadığı ancak klasik kaba kuvvet algoritmalarına göre karekök hızlandırma sunan Grover algoritması nedeniyle daha büyük anahtar boyutlarına ihtiyaç duyulabileceği; klasik saldırılara karşı güvenliği sağlamak için NIST'in, 80 bit veya daha altı güvenlik seviyesinde yer alan şifreleme sistemlerinden 112 veya 128 bit güvenlik sağlayan anahtar boyutlarına ve algoritmalara geçişi tavsiye ettiği, AES şifreleme algoritmasının ise 192 veya 256 bitlik anahtar boyutlarıyla kullanılması halinde kuantum hesaplamalarına dayanıklı olduğunun kabul edildiği; girdi olarak anahtar yerine orijinal mesaja dayalı, sabit uzunlukta bir özet değer oluşturarak kullanılan anahtarsız şifreleme algoritmalarının güvenliğinin de simetrik şifreleme algoritmalarına benzer şekilde boyut ile ilişkili olduğu ve SHA-2 ile SHA-3 şifreleme algoritmaları haricinde kuantum hesaplama yöntemlerine karşı dirençli olmadıklarına bir önceki bölümde detaylarıyla yer verilmiştir.

Gerekli anahtar boyutuna sahip simetrik anahtarlı algoritmaların kuantum saldırılarına karşı dirençli olacağı bilinse dahi; güvenli olmayan bir ortamda gizli bir şekilde paylaşılması gereken simetrik anahtarın güvenli iletiminin kuantum bilgisayar tehdidi altında olan açık anahtarlı kriptografik algoritmalar aracılığıyla gerçekleştirilmesi, simetrik anahtar algoritmalarının kuantum bilgisayarlara karşı temel güvenlik açığını oluşturmaktadır. AES gibi kuantuma dirençli simetrik şifreleme algoritmalarının güvenli anahtar dağıtımına yönelik güvenlik açığının giderilebilmesi amacıyla, kuantum bilgisayar tehdidine dirençli asimetrik anahtarlı kriptografik algoritmaların oluşturulmasının yanı sıra "Kuantum Anahtar Dağıtımı" olarak bilinen ve güvenliğinin fizik yasalarınca garanti edildiği bir diğer güvenli anahtar dağıtım yöntemi bulunmaktadır. Kuantum anahtar dağıtımının kuantum saldırıları da dahil olmak üzere tüm saldırı yöntemlerine karşı dirençli olduğu 'teorik' olarak kanıtlanmış olup bu durum, saldırganın sınırsız klasik ve kuantum hesaplama kaynağına sahip olsa dahi kuantum anahtar dağıtımı yönteminin her zaman güvenli olacağını ifade etmektedir. Söz konusu güvenlik unsurları, kuantum mekaniği ilkelerine dayandırılmakta ve bilginin ışığın kuantum durumlarında kodlanmasıyla sağlanmaktadır. Kuantum

anahtar dağıtımının benzersiz güvenlik özelliklerinin temelini oluşturan ve birbiriyle ilişkili olan üç kavram bulunmaktadır:

- Heisenberg belirsizlik ilkesi, bilinmeyen bir kuantum durumunun ölçülmesinin fiziksel bir değişime sebebiyet vereceğini ima etmektedir. Bu durum, kuantum anahtar dağıtımı yöntemi ile gerçekleştirilen veri akışını gözlemleyen bir dinleyicinin bazı bitlerin değerini fiziksel olarak ve tespit edilebilir bir şekilde değiştireceği anlamına gelmektedir.
- Klonlanamazlık teoremi, bilinmeyen bir kuantum durumunun mükemmel bir kopyasını yapmanın fiziksel olarak imkansız olduğunu belirtmektedir. Bu durum, bir saldırganın dinleme faaliyetini gizlemek umuduyla veri akışındaki bitin bir kopyasını oluşturmasının imkansız olduğunu; kuantum durumlarında kodlanmış verilere erişmenin verileri yetkili taraflarca tespit edilebilecek şekilde değiştireceğini ve hataların ortaya çıkacağını ifade etmektedir.
- Kuantum dolanıklık ise yetkisiz erişimin önüne geçen özellikler sunmaktadır. (ETSI, 2015)

Diğer yandan, kuantum anahtar dağıtım yöntemlerinin güvenlik sorununa teorik olarak nihai bir çözüm sunduğu belirtilse de ideal uygulama metotlarının pratikte hayata geçirilmesinin zor olduğu ve ele alınması gereken bazı problemlerin bulunduğu ifade edilmektedir. Kuantum anahtar dağıtım yöntemleri uygulanma yöntemi açısından iki farklı yaklaşım üzerine temellendirilmiş olup teorik güvenliğin kesin bir şekilde sağladığı ifade edilen dolanıklık tabanlı kuantum anahtar dağıtım yönteminin en yüksek düzeyde kuantum güvenliği sağladığı varsayılmakla birlikte uygulanmasının zor ve gizli anahtar üretim hızının (anahtara dönüştüren giriş sinyallerinin oranını ifade etmektedir) düşük olduğu; "hazırla ve ölç" yaklaşımına dayalı kuantum anahtar dağıtım protokollerinin ise daha pratik olduğu ve kabul edilebilir seviyelerdeki gizli anahtar üretim hızına sahip olduğu değerlendirilmesine rağmen güvenliğinin yalnızca kuantum yasalarına değil uygulamanın gerçekleştirildiği cihaza da bağlı olması sebebiyle;

- Donanımsal özelliklerin kötüye kullanılarak kriptografik cihazların ürettiği yan kanal bilgilerinin kullanılması,

- Kodlama cihazları hakkında bilgi almak için gönderici modüle foton enjekte edilmesi yöntemi ile truva atı saldırılarının kuantum versiyonunun gerçekleştirilmesi,
- İdeal kuantum anahtar dağıtım sistemlerinde tek foton kaynağı kullanımının olmasına rağmen söz konusu sistemlerin henüz yaygınlık kazanmaması sebebiyle zayıflatılmış lazer diyotlarının kullanılması sonucu yetkisiz erişime izin veren foton bölme saldırılarının gerçekleştirilme potansiyelinin oluşması,
- Polarize ışığa kodlanan durumların fiziksel ekipmandan kaynaklanan sorun nedeniyle farklı durumlarda iletilmesi ve anahtar üretim oranında beklenenden yüksek bir düşüşe sebebiyet vermesi,
- Kuantum anahtar dağıtım cihazlarında bulunan foton dedektörlerine parlak ışık saldırısı gönderilerek anahtar bitlerinin çalınması,

yöntemleri ile gizli bilgilerin açığa çıkarılmasına yönelik tehditler içerdiği değerlendirilmektedir (ETSI, 2018) (Pirandola, Andersen, & Banchi, 2020).

Kuantum anahtar dağıtımının güvenlik ile ilişkili diğer bir önemli özelliği ise herhangi bir saldırının gerçek zamanlı olarak gerçekleştirilmesi gerektiğidir. Klasik kriptografik algoritmaların aksine kuantum anahtar dağıtımı ile iletilen verinin sonrasında daha güçlü teknolojiler ile deşifre edebilmek amacıyla saklanmasına ilişkin bir yöntem bulunmamaktadır. Bu durum, kuantum anahtar dağıtımına yönelik gerçekleştirilebilecek saldırılara ilişkin olasılıkları klasik kriptografik yöntemlere kıyasla büyük ölçüde azaltmaktadır. (ETSI, 2015)

3.3.1. Kuantum Anahtar Dağıtımının Genel İşleyişi

Kuantum anahtar dağıtımı, gizli bir anahtar oluşturabilmek için kimlik doğrulamasının yapılabildiği klasik bir iletişim kanalı ile kuantum iletişim kanalının birlikte kullanıldığı bir süreçtir. Kuantum anahtar dağıtımının uygulanabilmesi için mevcut tüm protokollerde; ışığın kuantum durumunu gönderebilmek için bir kuantum iletişim kanalı ile gönderici ve alıcının kuantum durumları ile ilgili belirli ölçümleri karşılaştırması ve gizli anahtarı elde edebilmek amacıyla sonraki işlem adımlarını gerçekleştirebilmesi için kimliği doğrulanmış bir klasik iletişim kanalı gerekmektedir.

Kuantum kanalında, gönderici ile alıcı arasındaki foton iletiminin sağlanabilmesi için fiber optik kablolar veya uydu bağlantıları kullanılmaktayken, kuantum kanalının kuantum mekaniği ilkeleri doğrultusunda iletişim kanalının dinlenip dinlenmediğine ilişkin bilgi sağlaması sebebiyle klasik kanal için, güvenlikten ödün vermeksizin gönderici ile alıcının birbirleriyle iletişim kurduğu bir telefon hattı kullanılabilmektedir.

Kuantum anahtar dağıtımı hem göndericinin hem de alıcının kuantum kanalını kurmak için gerekli ekipmana ve birbirleriyle iletişim kurabilecekleri klasik bir kanal erişimine sahip olduğu bir ortamda, göndericinin alıcıya kriptografik anahtarları dağıtmaya karar vermesi ile başlamaktadır. Gönderici, bir ışık kaynağı kullanarak kuantum durumlarını içeren foton akışını (her foton bilgi içeren bir bit olarak düşünülebilir) alıcıya iletmekte, her foton iletiminde gönderici tarafından belirlenen rastgele iki tabandan (taban, fotonun ölçüldüğü perspektif olarak tanımlanabilmektedir) biri seçilmekte ve alıcı tarafından iletilen her foton iki tabandan birinde ölçülerek bulunan değer kaydedilmektedir. Göndericinin foton iletiminde seçtiği taban rastgele olmakla birlikte anahtar üretimi için alıcının göndericinin seçtiği tabana ilişkin bilgi alması gerekmekte; bu bilgi ise klasik kanal üzerinden alıcı ile göndericinin iletişim kurması ile elde edilebilmektedir.

Kuantum anahtar dağıtımının kullanımı yukarıda özetlenmiş olup saldırganın söz konusu süreçte anahtarı elde etmesi;

- Fotonların gözlemlenmesi halinde değişerek gönderici ve alıcı tarafından farkına varılması,
- Klasik iletişim kanalı üzerinde gerçekleştirilen haberleşme eyleminde kuantum durumunun nihai sonucunun açıklanmadan yalnızca ölçüm için hangi tabanın kullanıldığına ilişkin bilgi paylaşımının gerçekleştirilmesi,
- Bilgi paylaşımının gerçekleştirildiği sırada foton ölçümünün tamamlanmış olması sebebiyle paylaşılan tabanın bilinmesinin bir anlam ifade etmemesi

gibi nedenlerle mümkün olmamaktadır. (ETSI, 2015)

3.3.2. Kuantum Anahtar Dağıtımı İletim Ortamı

Kuantum anahtar dağıtımı, klasik iletişim kanalı ile kuantum iletişim kanallarının birlikte kullanımı ile gerçekleştirilmektedir. Kuantum iletim kanalında kuantum durumlarının iletiminin gerçekleştirildiği fotonlar fiber optik kablolar ya da uydu bağlantıları aracılığıyla iletilebilmektedir.

3.3.2.1. Fiber Optik Kablolar Aracılığıyla İletim

Fiber optik kablolar düşük kayıp oranı ve yüksek kararlılığa sahip olduğundan kuantum sinyallerinin iletimi için daha uygun olduğu düşünülmektedir. Son yıllarda, fiber optik kablolar üzerinden kuantum anahtar dağıtımı tasarımı için hem teorik hem de deneysel olarak önemli bir çaba harcanarak ulaşılabilir mesafe ile anahtar iletim oranında önemli ölçüde iyileştirmeler gerçekleştirilmiştir. Deneysel olarak, kuantum anahtar dağıtımının bir fiber optik bağlantısı aracılığıyla 50,5 km üzerinde 1,2 Mbps ve 405 km fiber bağlantı üzerinde 6,5 Mbps gizli anahtar iletim hızına ulaştığı gösterilmiştir (Boaron, 2018). Fiber optik iletimine dayalı kuantum anahtar dağıtımı sistemleri piyasada mevcut olmakla birlikte sahada düşük bir maliyetle fiber altyapısına dayalı olarak dağıtımını gerçekleştirmek mümkündür. Diğer yandan, fiber optik kablo tabanlı kuantum anahtar dağıtımı, kabloların belirli zorlu arazilerden, nehirlerden vb. kolaylıkla geçememesi nedeniyle sınırlanabilmekle birlikte uzun mesafeli iletim sırasında kuantum sinyallerinin emilimi ve gürültüsü nedeniyle ulaşılabilir noktadan noktaya mesafe birkaç yüz kilometre ile sınırlı kalmaktadır. (Y. Cao, 2022)

3.3.2.2. Uydu Haberleşmesi Aracılığıyla İletim

Geniş kapsama alanına sahip uydu bağlantıları üzerinden de gerçekleştirilebilen kuantum anahtar dağıtımında önemli ilerlemeler kaydedilmiştir. Micius adını taşıyan ilk kuantum uydusu Ağustos 2016'da fırlatılmış ve alçak irtifa uydu yörüngeleri (Low Earth Orbit-LEO) ile yer istasyonu arasında 1200 km'lik bir mesafede kuantum anahtar dağıtımının uygulanabilirliğini göstermiştir (Liao, 2017). İletim kaybı daha az olan ve daha uzak mesafelerde iletim gerçekleştirebilen uydu tabanlı kuantum anahtar

dağıtım sistemlerini deney ortamından uygulama alanına taşınması için çalışmalar devam etmektedir. Küresel bir kuantum anahtar dağıtım ağı ile kuantum internetinin geliştirilebilmesi için fiber optik kablolar ile uydu tabanlı kuantum anahtar dağıtım yöntemlerinin entegre edileceği öngörülmektedir (Chen Y.-A. , 2021).

Tablo 3.3. Fiber optik kablo ile uydu tabanlı kuantum anahtar dağıtımı iletiminin karşılaştırması

	Fiber Optik Kablo	**Uydu Haberleşmesi**
Stabilite	Yüksek	Düşük
Esneklik	Düşük	Yüksek
Gelişmişlik Düzeyi	Yüksek	Düşük
Maliyet	Düşük	Yüksek
Ticarileştirme	Mevcut	Mevcut Değil
Aktarma Olmadan Ulaşılabilir Mesafe	605 km	1200 km
Gelecekteki Yönlendirmeler	Küresel bir ağ oluşturabilmek amacıyla entegre bir şekilde kullanılacakları öngörülmektedir.	

Kaynak: Y. Cao, 2022

3.3.3. Kuantum Anahtar Dağıtım Protokolleri

Kuantum anahtar dağıtım protokolleri yetkisiz erişim tespitine bağlı olarak iki kategoriye ayrılmaktadır.

- **Hazırla ve ölç yaklaşımında**, gönderici bilgiyi polarize foton formunda hazırlayarak iletmekte ve ardından alıcı gönderilen fotonları ölçmektedir. Bu yaklaşımda Heisenberg'ün bir sistemdeki kuantum durumunu orijinal kuantum durumunu bozmadan ölçmenin imkansız olduğunu ifade ettiği belirsizlik ilkesi kullanılmakla birlikte klonlanamazlık teorisinde açıklandığı gibi kuantum biti bozulmadan kopyalanması veya yükseltilmesi de mümkün olmamaktadır. Hazırla ve ölç yaklaşımında gönderici ile alıcı, iletişimlerinde karşılaşmayı bekledikleri hata oranı ile gerçekleşen hata oranını kıyaslayarak yetkisiz erişim olup olmadığını tespit etmektedir. Bu yaklaşım, iletilen kuantum durumlarını ele geçiren bir saldırganın, söz konusu kuantum durumunu ölçerek ve bir

tahminde bulunarak alıcıya iletmesi üzerine tanımlanabilir bir hata yüzdesi ortaya çıkarılması varsayımına dayanmaktadır (ETSI, 2015). Bu yaklaşımda kuantum durumları gönderici tarafından hazırlanarak alıcıya iletilmektedir. (Y. Cao, 2022)

- **Dolanıklık tabanlı yaklaşımda** ise gönderici ile alıcı da bulunan kuantum dolanıklığa sahip fotonlara bir saldırgan tarafından herhangi bir müdahalenin veya ölçümün gerçekleştirilmesi halinde dolanıklığın bozularak yetkisiz erişim teşebbüsünün tespit edilebileceği varsayımına dayanmaktadır (ETSI, 2015). Bu yöntem ile dolanık kuantum durumlar gönderici ve alıcıdan bağımsız olarak iletilmekle birlikte ortam koşullarındaki bozulmalara karşı daha dirençli olduğu değerlendirilmektedir. (Y. Cao, 2022)

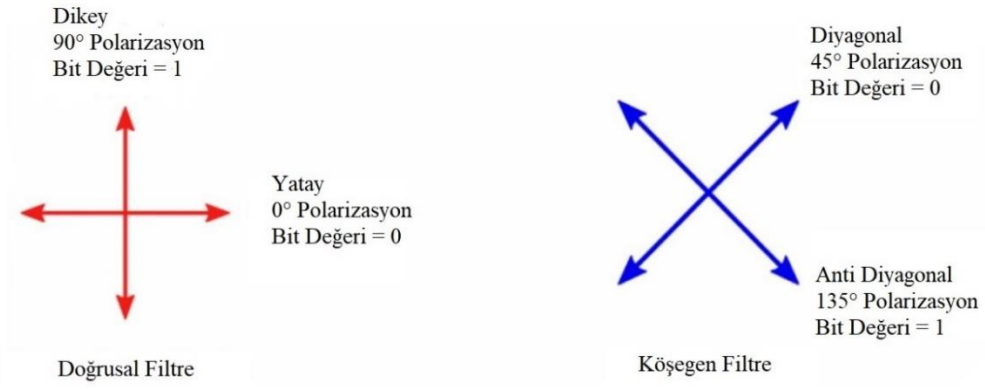
Bu bölümde hazırla ve ölç yaklaşımı ile dolanıklık tabanlı kuantum anahtar dağıtımı protokollerinden birkaçı temel çalışma prensibi göz önünde bulundurularak incelenmiştir.

3.3.3.1. BB84 Protokolü

1984 yılında Bennett ve Brassard isimli iki araştırmacı, anahtar bilgisini bir kuantum iletişim kanalı aracılığıyla iletebilmek amacıyla foton polarizasyon durumunun nasıl kullanılacağını açıklayan ve kuantum mekaniği ilkelerini kullanarak iki taraf arasında anahtar paylaşımına imkan tanıyan ilk kuantum kriptografi protokolünü açıklamıştır (C.H. Bennett, 2014). Bu protokol BB84 protokolü olarak bilinmekte olup hazırla ve ölç tabanlı kuantum anahtar dağıtımı protokolü olarak kategorize edilmektedir.

Bu protokol ile anahtar bitlerini iletmek ve dağıtmak için tek bir foton kullanılmakta olup foton dört polarizasyon durumundan birinde polarize edilerek şekil 3.1'de gösterilen iki eşlenik bazdan/tabandan biri; yani dikey ve yatay polarizasyon için doğrusal taban, diyagonal ve anti diyagonal polarizasyonu için çapraz taban kullanılabilmektedir.

Şekil 3.1. BB84 protokolü için polarizasyon-kübit değeri eşleşmesi



Kaynak: (A. I. Nurhadi, 2018)

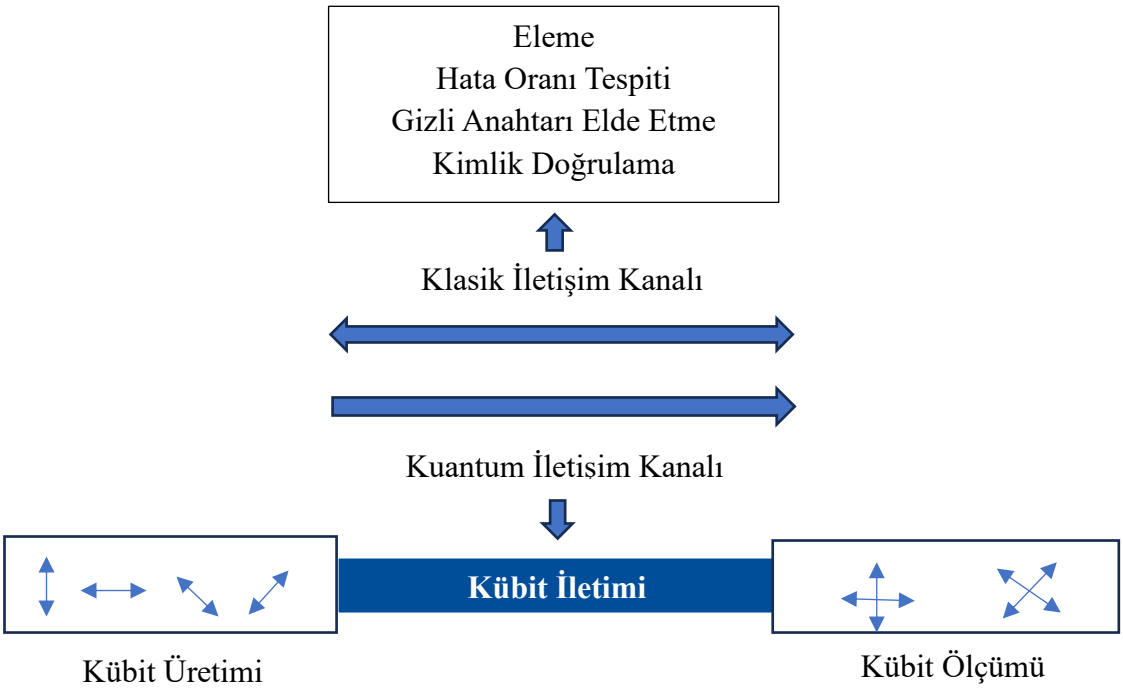
BB84 protokolünde şekil 3.2'de özetlenen ve aşağıda açıklanan beş aşama gerçekleşmektedir.

1. **Kübit hazırlama, iletimi ve ölçümü:** Gönderici tarafından bir dizi klasik bit (ham anahtar olarak adlandırılmaktadır) üretilmekte ve kübiti oluşturabilmek amacıyla her bir fotonun sırasıyla "0", "1", "1" ve "0" klasik bitlerine karşılık gelen yatay, dikey, anti diyagonal ve diyagonal olmak üzere dört polarizasyon durumundan birine sahip olduğu foton akışına kodlanmaktadır. Sonrasında kübitler bir kuantum iletişim kanalı aracılığıyla alıcıya iletilmekte ve alıcı tarafından her bir kübitin ölçümü iki filtreden birine dayandırılarak gerçekleştirilip sonuçlar kaydedilmektedir.
2. **Eleme:** Gönderici ve alıcı klasik bir iletişim kanalı üzerinden kodlama ve ölçüm filtrelerini birbirleriyle paylaşmakta ve gönderim ile alım sırasında aynı tipte filtre kullanılmayan kübitler elenmektedir. Eşleşen filtrelere karşılık gelen kübitlerin kodu bir bit akışına çözümlenerek elenmiş anahtar elde edilmektedir.
3. **Hata Oranı Tespiti:** Kuantum bit hata oranının belirlenen eşik değerinin altında olup olmadığının tespiti amacıyla elenmiş anahtarın bir kısmı kullanılarak kuantum bit hata oranı tahmin edilmektedir. Tahmin edilen kuantum bit oranının eşik değerinin üzerinde olması halinde kuantum kanalındaki gizli dinleme olasılığı göz önünde bulundurularak kuantum

anahtar dağıtım süreci sonlandırılmakta ve ilk aşamadan başlamak üzere yeniden başlatılmaktadır.

4. **Gizli Anahtarı Elde Etme:** Gönderici ile alıcı tarafından klasik bir kanal üzerinden hata düzeltme, doğrulama ve gizlilik yükseltme işlemleri gerçekleştirilerek son güvenli bit dizisi ortaya çıkarılıp gizli anahtar elde edilmektedir.
5. **Kimlik Doğrulama:** Protokolün güvenli bir biçimde çalışabilmesi için göndericinin ve alıcının kiminle iletişim kurduklarından emin olması gerekmektedir. Gerçekleştirilen tüm iletişim gizli bilgileri ele geçirmeye çalışan yetkisiz birisiyle de yapılıyor olabileceğinden gönderici ile alıcının ilk kez iletişim kurmadan önce birbirlerinin kimliklerini doğrulayacak ortak bir anahtara sahip olması gerekmektedir. Daha sonra gerçekleştirilecek iletişimlerden önce yapılacak kimlik doğrulaması ise bir önceki iletişim sırasında kullanılan ve kuantum kriptografi ile elde edilen anahtarın küçük bir kısmı kullanılarak yapılabilmektedir (Y. Cao, 2022).

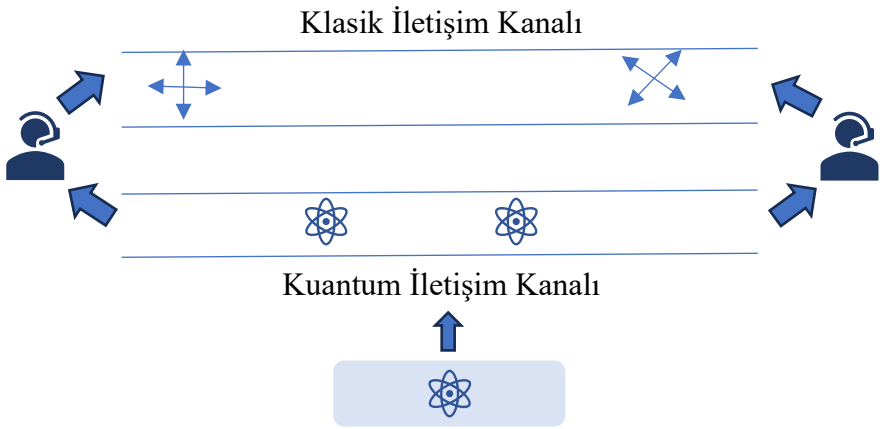
Şekil 3.2. BB84 protokolünde yer alan beş aşama



3.3.3.2. E91 Protokolü

1991 yılında Ekert tarafından dolanık parçacık/foton çiftlerini kullanarak bir kuantum anahtar dağıtım protokolü tasarlamış olup bu protokolde parçacık/foton kaynağı gönderici veya alıcı tarafından oluşturulabilmektedir. Şekil 3.3'te genel gösterimine yer verilen bu protokolde, ilk olarak dolanık foton kaynağından bir çift dolanık foton/kuantum parçacığı gönderilerek gönderici ile alıcının her dolanık çiftten bir parçacığa sahip olması sağlanır. BB84 protokolünde olduğu gibi E91 protokolünde de gönderici ile alıcı ölçüm için rastgele bir filtre seçer ve bunları klasik kanal üzerinden paylaşırlar. Eğer gönderici ve alıcı aynı filtreyi kullanırsa dolanıklık ilkesi sebebiyle birbirine zıt sonuçlar elde etmeleri gerekir. Anahtar dağıtım sürecinde yetkisiz erişim olup olmadığının tespiti ise kurulan fiziksel sistemin kuantum mekaniği ilkeleriyle örtüştüğünü ve Bell eşitsizliklerinin ihlal edildiğini gösteren Bell Testleri ile gerçekleştirilmektedir. (Ekert, 1991)

Şekil 3.3. E91 protokolü aşamaları



3.3.3.3. BBM92 Protokolü

Bennett, Brassard ve Mermin tarafından 1992 yılında Ekert'in E91 protokolünü önermesinden kısa bir süre sonra önerilmiş olan BBM92 protokolü, BB84 protokolünün dolanıklık tabanı versiyonu olarak tanımlanmakta, anahtar değişim mekanizması, elenmiş anahtar oluşturma ve gizlilik artırımı gibi ortak temelleri barındırmaktadır. (Mermin, 1992)

3.3.3.4. B92 Protokolü

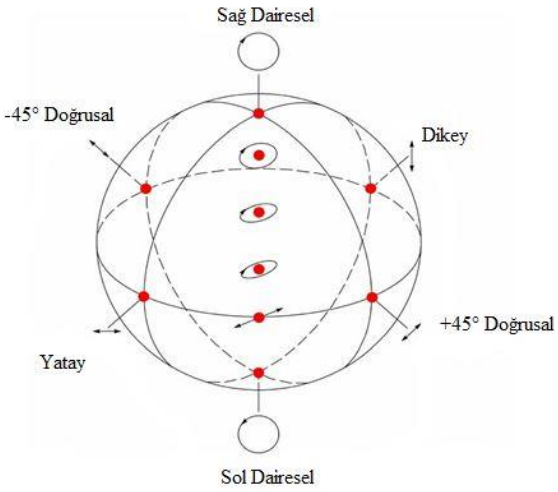
Bennett'in, gizli dinleyicinin varlığını tespit etme yeteneğini etkilemeden kuantum anahtar dağıtımı protokolünün kodlanması ve çözülmesi için ortogonal (dik) olmayan tek bir temelin kullanılabileceğini fark etmesi üzerine 1992 yılında oluşturulan protokol BB84 protokolünün basitleştirilmiş bir versiyonu olarak tanımlanmaktadır. BB84 protokolünde dört farklı foton polarizasyon durumu bulunurken B92 protokolünde sadece iki polarizasyon durumundan biri kullanılmaktadır. Buna göre; 0 bitlik değer doğrusal temelde 0 derece olarak kodlanırken, 1 bitlik değer köşegen temelde 45 derece olarak kodlanmaktadır. BB84 protokolünden önemli diğer bir farkı ise alıcının yanlış filtreyi seçmesi durumunda hiçbir şey ölçemeyecek olmasıdır. (Bennett, 1992)

3.3.3.5. Altı Durumlu Protokol

Altı Durumlu Protokol (Six-State Protocol), Pasquinucci ve Gisin tarafından önerilmiş olup altı polarizasyon durumu ve üç ölçüm tabanı kullanmaktadır (H.B. Pasquinucci, 1999). Ek bir taban eklemesi yapılarak üç ölçüm tabanlı BB84 şeması olarak kabul edilmektedir.

Şekil 3.2'de Poincare küresi gösterilmiş olup; BB84 protokolü küre üzerinde ±x ve ±y yönlerine karşılık gelen dört polarizasyon durumu kullanılarak gösterilebilirken, altı durumlu protokole ±z'ye karşılık gelen iki ekstra polarizasyon durumu daha eklenerek ±x, ±y ve ±z olmak üzere altı polarizasyon durumunu kullanabilir hale getirilmiştir. Bu durum, altı durumlu protokolün BB84 protokolüne kıyasla daha yüksek simetriye ve dolayısıyla daha üstün bir konuma gelmesini sağlamaktadır.

Şekil 3.4. Poincare Küresi



Kaynak: (A. I. Nurhadi, 2018)

3.3.3.6. SARG04 Protokolü

2004 yılında Scarani ve arkadaşları tarafından önerilen protokol, foton kaynağı olarak tek foton kaynağı yerine zayıflatılmış lazer darbesi kullanmaktadır (V. Scarani, 2004). Anahtar dağıtım sürecinin ilk aşamasında BB84 protokolü ile aynı şema kullanılmakla birlikte ikinci aşamada göndericinin kullanmış olduğu filtreyi doğrudan açıklaması yöntemi yerine ortogonal olmayan, 45 derecelik, durum çiftlerinden birinin açıklanması yöntemi izlenmektedir. Eğer alıcı açıklanan pozisyonlardan herhangi birine dik açıda bir okuma yapmışsa ilgili okumayı geçerli saydığını karşı tarafa bildirerek okuduğu kübitin tümleyenini anahtara eklemektedir (A. I. Nurhadi, 2018)

3.3.3.7. COW Protokolü

2004 yılında Nicolas Gisin ve arkadaşları tarafından önerilen COW Protokolü (Coherent One-Way- COW), dolanıklık ilkesini kullanmakla birlikte kübit başına elde edilen bit güvenliğinde daha verimli olduğu değerlendirilmektedir. Bununla birlikte, hattı gizlice dinleyen birinin olması ve her kübit için üretilip yollanan fotonların yakalanıp okuma işleminde kullanılan filtre tiplerinin klasik kanal üzerinden açıklanmasına kadar geçen sürede kuantum belleklerde saklanabilmesi halinde anahtarı öğrenebilmesine neden olan ve PNS (Photon Number Splitting-PNS)

saldırıları olarak adlandırılan saldırılara karşı daha dirençli olduğu ifade edilmektedir. (A. I. Nurhadi, 2018)

Kuantum anahtar dağıtım sistemleri; fiber optik kablo uzunluğu, dalga boyu sönümlenmesi, sıcaklık ve siber saldırılar gibi kısıtlamalara maruz kalmasına rağmen BB84 ile COW gibi çok sayıda kuantum anahtar dağıtım protokolü ticari olarak piyasaya sürülmüş olup kullanımı dünya genelinde yaygınlaşmaktadır. Kuantum anahtar dağıtımı sistemlerinin uygulanabilirliği ise kuantum anahtar dağıtım ağının oluşturulabilmesinde sağlam bir temel sunarak çok sayıda uygulama için uzun vadeli güvenlik sağlamada önemli bir rol üstelenmesi beklenen kuantum internetinin oluşturulmasında kilometre taşı olarak görülmektedir. (Y. Cao, 2022)

3.3.4. Kuantum Anahtar Dağıtımı Uygulama Alanları

Kuantum anahtar dağıtım ağı ve bilgi teknolojileri ekosisteminin bir araya getirilmesi sonucu finansal kurumlar ile devlet kurumlarının kritik bağlantıları gibi birçok farklı alanda çeşitli kuantum anahtar dağıtım güvenlikli uygulamalar ortaya çıkmıştır. Kuantum anahtar dağıtımının bazı spesifik uygulama alanları aşağıda özetlenmiştir.

- **Finans Sektörü:** Gerçekleştirilen işlemler, müşteri verileri ve özel bilgiler gibi oldukça hassas ve değerli verileri işleyen bankacılık sektöründe kuantum anahtar dağıtımı yöntemi, verilerin geleceğe yönelik olarak korunmasına ve nihai güvenlik sağlamasına olanak tanımaktadır. İlk kuantum anahtar dağıtımı güvenlikli banka transferi bir Avusturya bankasının genel merkezi ile Viyana belediye binası arasında 2004 yılında gerçekleştirilmiş (Poppe, 2004), İsviçre'de kritik finansal işlemlerin güvenliğini sağlamak için IPsec protokolü ile birlikte kuantum anahtar dağıtımı kullanımına ilişkin bir senaryo tanımlanarak analiz edilmiş ve finans kurumları tarafından olağanüstü durum anında ağlarının güvenliğini sağlamak için ticari kuantum anahtar dağıtımı sistemleri kullanılmış (S. Ghernaouti-Hélie, 2005), birçok Çin bankası mevcut kuantum anahtar dağıtımı ağlarını kullanarak kuantum anahtar dağıtımı güvenlikli veri transferinin yanı sıra kurumsal kullanıcılar için çevrimiçi bankacılık işlemlerini de uygulamaya koymuştur (Qin, 2019). Çevrimiçi

bankacılık sistemlerinde kimlik doğrulamanın kimlik avı gibi saldırılara karşı potansiyel olarak savunmasız olduğu göz önünde bulundurularak çevrimiçi bankacılık sistemlerinde standart kimlik doğrulamayı geliştirmek için kuantum anahtar dağıtımının benimsenebileceği değerlendirilmektedir (A. Sharma, 2013).

- **Kamu Kurumları ve Milli Güvenlik:** Ulusal sırların korunabilmesi amacıyla devletler uzun ömürlü ve güçlü veri güvenliğine gereksinim duymaktadır. Kuantum anahtar dağıtımının veri hakimiyetini garanti edebilmek amacıyla ülkelere ve savunma sanayi kuruluşlarına uzun vadeli veri güvenliği sunması beklenmektedir. Kuantum anahtar dağıtımı ülke uygulamaları incelendiğinde;
    - 2007 yılında İsviçre tarafından ulusal seçim oy pusulalarını saymak için kullanılan özel bir hattın güvenliğini sağlamak için başarıyla uygulanmış (IDQ),
    - Çin'in Jinan şehrinde inşa edilen kuantum anahtar dağıtım metropolitan ağı kullanılarak sırların korunabilmesi hedefi ile çok sayıda kamu çalışanı tarafından kullanılmış (Zhang & Xu, 2018), (Zhang Q. , 2015)
    - Avustralya'nın başkenti Canberra'da hükümet içi iletişimi güvence altına alabilmek için kuantum anahtar dağıtım ağı kurulduğu

  görülmektedir. Bununla birlikte, kamu kurumlarında kullanılan iletişim sistemleri için yüksek düzeyde veri gizliliği, bütünlüğü ve doğruluğu sağlamak amacıyla yararlanılan sanal özel ağların (Virtual Private Network-VPN) güvenliğini artırabilmek için kuantum anahtar dağıtımı uygulaması çalışmaları gerçekleştirilmektedir (M. Niemiec, 2016), (A. Aguado, 2018).
- **Bulut Depolama ve Veri Merkezleri:** Büyük miktarda ve gizlilik derecesi yüksek veri depolanan veri merkezleri ile bulut depolama sistemleri, gün geçtikçe daha fazla kuruluş tarafından veri yedeklemek, depolamak ve kurtarmak amacıyla kullanılmakta bu sebeple söz konusu sistemlerde veri gizliliği ile güvenliğinin sağlanması büyük önem taşımaktadır. Kullanılan geleneksel güvenlik sistemlerinin kuantum bilişimin oluşturduğu tehditlere karşı savunmasız hale gelme olasılığı da göz önünde bulundurulduğunda kuantum anahtar dağıtımı kullanımının bulut veri korumasında ve veri merkezi ara bağlantılarının güvenliğini artırma potansiyeline sahip olduğu değerlendirilmektedir. Dünya genelindeki uygulamalar incelendiğinde;

  - Hollanda'da Lahey ve Zoetermeer'deki Siemens veri merkezleri arasındaki veri aktarımını güvence altına alabilmek amacıyla bir kuantum anahtar dağıtımı bağlantısı tanıtılmış, Hollanda'da faaliyet gösteren telekomünikasyon şirketi KPN'nin Lahey ve Rotterdam'daki veri merkezleri arasındaki ağda uçtan uca kuantum anahtar dağıtımı uygulanmıştır (KPN, 2016).
  - Çin'de Pekin-Şangay kuantum anahtar dağıtım ağı Pekin ve Şangay arasındaki veri merkezi yedeklemesinin güvenliğini sağlamak için kullanılmaktadır (Chen Y. , 2018), (Q. Zhang, 2019).
  - Kurumsal bulut güvenliği uygulamalarında, Acronis ve Alibaba gibi birkaç şirketin de bulut veri koruması için kuantum güvenli şifreleme algoritmalarını uygulamaktadır (L. Huang, 2021).
- **Kritik Altyapılar:** Enerji, ulaşım ve telekomünikasyon gibi sektörlere ilişkin kötü niyetli veri müdahalesi veya hizmet kesintisi tehditlerine çözüm sunan kuantum anahtar dağıtımı uzun vadeli koruma ve geleceğe yönelik gizlilik sağlama potansiyeli sunmaktadır. Elektrik şebekelerinin korunması, güvenli ve istikrarlı bir şekilde çalışabilmesi amacıyla Çin Halk Cumhuriyeti Elektrik Dağıtım Şirketi'nin yanı sıra Ok Ridge ve Los Alamos Ulusal Laboratuvarları gibi çeşitli kurumlar tarafından kuantum anahtar dağıtım ağlarının uygulanması araştırılmakta; Telefonica, China Telecom ve British Telecom gibi telekomünikasyon şirketleri iletişim ağları üzerinden veri aktarımını güvence altına alabilmek için kuantum anahtar dağıtım sistemlerini mevcut fiber optik altyapılarına entegre edebilmesine ilişkin fizibilite çalışmaları gerçekleştirmektedir. (Y. Cao, 2022)
- **Mobil Haberleşme Sistemleri:** Kuantum anahtar dağıtım sistemlerinin hem uydu tabanlı hem de fiber optik ağlardan yararlanılarak gelişim gösterme potansiyeli, yer istasyonundan uyduya erişimin yanı sıra yer istasyonları arasındaki ve uydudan uyduya iletişimin güvenliğinde de kullanılabilirliği sağlamaktadır (Armengol, 2008). Bu doğrultuda, uydu tabanlı kuantum anahtar dağıtım ağı ile fiber optik tabanlı kuantum anahtar dağıtım metropolitan ağlarının kombinasyonuna dayalı olarak Çin ve Avusturya arasında kıtalararası bir video konferans düzenlenmiş, çok kullanıcılı bir mobil ağda akıllı telefonların güvenliğini sağlayabilmek amacıyla Tokyo kuantum anahtar dağıtım ağından yararlanılarak kuantum anahtar dağıtımı uygulaması

gerçekleştirilmiştir. QuantumCTek tarafından ZTE ile iş birliği içinde ticari bir kuantum anahtar dağıtımı gerçekleştirebilen cep telefonu geliştirilirken, China Telecom ve QuantumCTek özel bir SIM kart ve akıllı telefon uygulamasına dayanan kuantum şifreli telefon görüşmelerinin geliştirilmesini ortaklaşa teşvik etmektedir (Y. Cao, 2022).

3.3.5. Kuantum Anahtar Dağıtım Ağının Diğer Teknolojiler ile Entegrasyonu

Kuantum anahtar dağıtım ağının diğer gelişmiş teknolojilerle entegrasyonuna ilişkin bazı araştırma konularına aşağıda yer verilmiştir.

- **Kuantum Güvenli Kriptografi:** Kuantum anahtar dağıtım sistemlerinin geleneksel şifreleme sistemlerinin işlevlerini tamamen karşılayamaması ve kuantum güvenli kriptografik algoritmaların tamamen yazılım tabanlı olması sebebiyle yakın gelecekte kuantum güvenli kriptosistemlerin kuantum anahtar dağıtımı ile entegre edilerek bütünleşik bir güvenlik sistemi oluşturması beklenmektedir (Yang Y. , 2021).
- **Blokzincir:** Güven eksikliğinin bulunduğu bir ortamda verilerin merkezi olmayan bir veri kayıt defterine kaydedilerek anonim katılımcıların kaydedilen verileri okumasına, doğrulamasına ve kopyalamasına olanak tanıyan ancak silme ve değişiklik yapılmasına izin verilmediği bir veritabanı mekanizması olan blokzinciri, günümüzde güvenli kabul edilse de kuantum bilgisayarlardan gelebilecek saldırılara karşı savunmasızdır. Bu sebeple blokzincirini kuantum güvenli algoritmalar aracılığıyla kuantum hesaplamaya karşı dirençli hale getirme çalışmalarının (T. M. Fernández-Caramès, 2020) yanı sıra kimlik doğrulamanın gerçekleştirilmesinde kuantum anahtar dağıtımına dayalı bir blokzincir platformu oluşturma çalışmaları (Kiktenko, 2018) ile kuantum anahtar dağıtımı tabanlı bir elektronik imza şeması oluşturularak (X. Sun, 2019) kuantuma dirençli blokzinciri oluşturabilmesine yönelik araştırmalar gerçekleştirilmektedir.
- **Nesnelerin İnterneti (IoT):** Fiziksel nesnelerin internete bağlanarak ağ cihazları veya yönlendiriciler aracılığıyla veri alışverişinde bulunduğu, birbirine bağlı nesnelerden oluşan geniş bir ağı ifade eden nesnelerin

internetinin yakın gelecekte günlük hayatımızın ayrılmaz bir parçası haline geleceği öngörülmekle birlikte güvenlik ve gizlilik riskleri konusunda birçok endişe bulunmaktadır. Kuantum hesaplama yöntemleri ile gerçekleşmesi muhtemel saldırılara karşı IoT sistemlerini güvenli hale getirebilmek amacıyla kuantum güvenli kriptografi algoritmalarını IoT sistemlerine uygulamaya yönelik araştırmalar (Fernández-Caramés, 2020) devam etmekle birlikte kuantum anahtar dağıtımını söz konusu sistemlere uygulamaya yönelik çalışmalar henüz başlangıç aşamasındadır.

- **Kablosuz Ağlar:** Günümüzde geliştirilen kuantum anahtar dağıtım ağı bağlantıları kablolu (fiber optik kablo) ve sabit konumlardaki fiziksel düzenekler aracılığıyla gerçekleştirilmekte olup kuantum destekli serbest alan optik iletişiminde yaşanan gelişmelerden esinlenilerek kablosuz/mobil destekli kuantum anahtar dağıtım ağı önemli bir araştırma konusu haline gelmiştir. Bu doğrultuda, kapalı alanlarda kablosuz kuantum anahtar dağıtımı uygulanabilirliğine yönelik araştırmalar gerçekleştirilmiş (O. Elmabrok, 2018), IoT ve mobil cihazların kablosuz iletişiminde kullanılan Diffie-Hellman algoritması gibi algoritmaların yerine kuantum anahtar dağıtımının kullanılabileceğine yönelik değerlendirmelerde bulunulmuştur.

4. KUANTUM KRİPTOGRAFİ ALANINDA STANDARTLAR VE REHBER DOKÜMANLAR

Kuantum kriptografi ile ilişkili olarak standardizasyon kuruluşları, uluslararası kuruluşlar ve ülkeler tarafından çeşitli dokümanlar yayımlanmıştır. Bu bölümde standartlar ve rehber dokümanlar ele alınmıştır.

4.1. ETSI

1988 yılında Avrupa Birliğinin girişimi ile kurulmuş olan Avrupa Telekomünikasyon Standartları Enstitüsü (European Telecommunications Standards Institute – ETSI), altmıştan fazla üye ülke arasında telekomünikasyon altyapılarının birleştirilmesini, terminal donanımlarının uyumluluğunun sağlanmasını ve Avrupa telekomünikasyon ağının oluşturulmasını hedeflemektedir. Başlangıçta bölgesel bir standardizasyon kuruluşu olarak kurulan ETSI, telekomünikasyon pazarının giderek küreselleşmesi ve mobil haberleşmenin yaygınlaşmasıyla birlikte küresel düzeyde de etkili olan standartlar üretmeye başlamıştır.

ETSI, günümüzde kullanılan klasik kriptografik yöntemlerin, gelecekte kullanıma sunulacak olan daha güçlü işlemciler ya da kriptanaliz yöntemleri vasıtasıyla savunmasız hale geleceği endişesi ve kuantum teknolojilerinin iletişim altyapılarına uygulanmasına yönelik ilerlemeyi göz önünde bulundurarak Kuantum Anahtar Dağıtımı Endüstri Spesifikasyon Grubunu (Industry Specification Group (ISG) on Quantum Key Distribution) kurmuştur. Bu grubun amacı, kuantum iletişim endüstrisi için ortak bir arayüz ve standartlar geliştirerek ihtiyaçların karşılanmasına yardımcı olacak faaliyetlere öncülük etmektir.

Dünya genelinde yapım aşamasında olan ve kuantum iletişim altyapısında kullanılan kuantum anahtar dağıtım ağı ile ilişkili dikkate değer gelişmeler göz önünde bulundurularak endüstriyel standartların geliştirilmesine yönelik ihtiyacın karşılanması, kullanılan bileşenler, sistemler ve uygulamalar için ortak arayüzler ve spesifikasyonlar geliştirilmesi ve bu sayede kuantum iletişim ağlarının gelecekte birlikte çalışabilirliğinin sağlanabilmesine yönelik bir temel oluşturabilmek amacıyla

Kuantum Anahtar Dağıtımı Endüstri Spesifikasyon Grubu tarafından 2010 yılından itibaren birçok doküman yayımlanmıştır.

Ayrıca, yeterli bilgi işlem gücüne sahip bir kuantum bilgisayarın inşası halinde savunmasız hale gelecek olan asimetrik anahtarlı algoritmaların sebep olacağı bilgi güvenliği ihlallerinin önüne geçebilmek amacıyla Siber Kuantum Güvenli Kriptografi Çalışma Grubu (Cyber Quantum Safe Cryptography (QSC) Working Group) kurulmuş olup kuantum güvenli kriptografik algoritmaların mevcut durumu ve endüstriyel gereksinimleri göz önünde bulundurularak performans, işlevsellik, belirli uygulamalar özelindeki mimari özellikler vb. hususlarda değerlendirmelerde ve önerilerde bulunulması hedeflenmekte, mevcut durumda en iyi kuantum güvenli alternatiflerin belirlenmesi ve uygulanabilmesi için karşılaştırmalar ve önerilerde bulunulmaktadır.

Siber Kuantum Güvenli Kriptografi Çalışma Grubu tarafından yayınlanan dokümanlardan:

- ETSI GR QSC 006-Quantum-*Safe Cryptography; Limits to Quantum Computing applied to symmetric key sizes;* Dokümanda kuantum bilgisayarların simetrik kriptografi algoritmaları üzerindeki etkisi analiz edilerek 256 bitlik simetrik şifreleme algoritmalarının ve özet fonksiyonlarının 2050 yılında hala kırılmamış olacağın belirtilmektedir. (ETSI, 2017)
- ETSI GR QSC 004- *Quantum-Safe Cryptography; Quantum-Safe threat assessment;* Doküman kapsamında kuantum güvenli kriptografik algoritmalara geçişin zamanlamasına ilişkin bir denklem oluşturulmuş,

  -X: Asimetrik anahtarlı algoritmaların kırılmadan kalması gereken yıl sayısı

  -Y: Mevcut sistemin kuantum güvenli bir sistemle değiştirilebilmesi için harcanacak yıl sayısı

  -Z: Kuantum bilgisayarların veya başka araçların kullanılarak mevcut kriptografik yöntemlerin savunmasız hale getirilmesi için ihtiyaç duyulan yıl sayısı.

  -T: Kuantum güvenli algoritmalara güvenilebilmesi için ihtiyaç duyulan yıl sayısı

  olarak tanımlanmış ve X+Y+T>Z olması halinde asimetrik anahtarlı algoritmalar tarafından korunan tüm verilerin risk altında olduğu ile derhal önlem alınması gerektiği ifade edilmiştir.

- ETSI GR QSC 003-*Quantum Safe Cryptography; Case Studies and Deployment Scenarios;* Dokümanda kuantum güvenli kriptografik yöntemlerin uygulanmasına yönelik kullanım örnekleri incelenmiş ve kuantum güvenli kriptografiye uyum sağlanabilmesi için değiştirilmesi gerekebilecek özellikler vurgulanarak geliştiriciler tarafından dikkate alınması gereken bazı noktalar değerlendirilmiştir. Bu kapsamda;
    - Çevrimiçi ağ güvenlik protokollerinde (TLS) kuantum güvenli kriptografinin mevcut protokole entegrasyonu,
    - Çevrimiçi kimlik doğrulamada kullanılan ve kuantum hesaplama yöntemlerine karşı savunmasız olduğu bilinen elektronik imza algoritmalarının kuantum güvenli ikamelerinin belirlenebilmesi için akademik kuruluşlar ile standardizasyon kuruluşlarının gerçekleştirdiği araştırmaların tamamlamasının gerektiği,
    - Çevrimdışı verilerin (sağlık verileri veya resmi belgeler gibi kritik önemi haiz verileri içeren ve uzun süre orijinal kalması istenen veriler) doğrulanmasında ise asimetrik anahtarlı algoritmaların kuantum güvenli algoritmalarla ikame edilmesinin uygulanabileceği belirtilmekle birlikte uygulamada blokzincir yapısında da kullanılan özetleme ağacı imza şemalarına (Hash tree signature schemes) dayalı yöntemler ile koruma sağlanabileceği

  ifade edilmiştir.

Tablo 4.1. ETSI tarafından yayımlanan standart ve rehber dokümanların özeti

Doküman	**Başlık**	**Amaç**	**Kullanılan Yöntem**
ETSI GR QSC 006 V1.1.1 (2017-02)	Quantum-Safe cryptography (QSC); Limits to Quantum Computing applied to symmetric key sizes	Kriptografi kapsamında kuantum hesaplama gücünün üst sınırlarını açıklayan bilgilendirme dokümanıdır. Analiz Grover algoritmasının simetrik bir anahtarlarda uygulanmasına yönelik açıklamalarda bulunmaktadır.	Kuantum Güvenli Kriptografi
ETSI GR QSC 004 V1.1.1 (2017-03)	Quantum-Safe Cryptography; Quantum-Safe threat assessment	Yüksek bilgi işlem gücüne sahip kuantum bilgisayarın ne zaman üretilebileceği ve oluşturabileceği tehditlere değinilerek kuantum güvenli kriptografiye geçiş için maliyet ve zaman çizelgelerine yer verilmiştir.	Kuantum Güvenli Kriptografi

Tablo 4.1. ETSI tarafından yayımlanan standart ve rehber dokümanların özeti (devamı)

ETSI GR QSC 003 V1.1.1 (2017-02)	Quantum Safe Cryptography; Case Studies and Deployment Scenarios	Kriptografik yöntemlerin kuantum hesaplamalara dirençli olabilmesi için gereksinimler ele alınmış, uygulama özelliklerine dayalı önerilerde bulunulmuştur.	Kuantum Güvenli Kriptografi
ETSI GR QSC 001 V1.1.1 (2016-07)	Quantum-Safe Cryptography (QSC); Quantum-safe algorithmic framework	Kuantum güvenli kriptografik yöntemlere ilişkin değerlendirmeler ve uygulamalara yönelik önerilerde bulunulmuştur.	Kuantum Güvenli Kriptografi
ETSI TR 103 949 V1.1.1 (2023-05)	Quantum-Safe Cryptography (QSC) Migration; ITS and C-ITS migration study	Akıllı ulaşım sistemlerinde geçiş stratejileri gözden geçirilerek tavsiyelerde bulunulmuştur.	Kuantum Güvenli Kriptografi
ETSI TR 103 823 V1.1.2 (2021-10)	CYBER; Quantum-Safe Public-Key Encryption and Key Encapsulation	Kuantum sonrası standardizasyon sürecinin üçüncü turu için NIST tarafından seçilen Anahtar Kapsülleme Mekanizmalarının teknik açıklamalarının bir özeti sunulmaktadır.	Kuantum Güvenli Kriptografi
ETSI TS 103 744 V1.1.1 (2020-12)	CYBER; Quantum-safe Hybrid Key Exchanges	Kuantum güvenli bir anahtar kapsülleme yöntemini klasik bir anahtar değişim yöntemiyle birleştirmek için yöntemler ve mimariler tanımlanmaktadır.	Kuantum Güvenli Kriptografi
ETSI TR 103 692 V1.1.1 (2021-11)	CYBER; State management for stateful authentication mechanisms	Özetleme tabanlı imza şemalarının kullanımının uygunluğu araştırılmış, potansiyel güvenlik açıkları belirlenmiş ve güvenlik risklerinin azaltılmasına yönelik tavsiyelerde bulunulmuştur.	Kuantum Güvenli Kriptografi
ETSI TR 103 619 V1.1.1 (2020-07)	CYBER; Migration strategies and recommendations to Quantum Safe schemes	Bir kuantum güvenli kriptografi algoritmasını benimsemek isteyen ve geçiş yapması gereken kullanıcılar için önerilerde bulunulmuştur.	Kuantum Güvenli Kriptografi
ETSI TR 103 618 V1.1.1 (2019-12)	CYBER; Quantum-Safe Identity-Based Encryption	Kuantum güvenli hiyerarşik kimlik tabanlı şifreleme algoritması için teknik önerilerde bulunulmuştur.	Kuantum Güvenli Kriptografi

Tablo 4.1. ETSI tarafından yayımlanan standart ve rehber dokümanların özeti (devamı)

ETSI TR 103 617 V1.1.1 (2018-09)	Quantum-Safe Virtual Private Networks	Kuantum güvenli algoritmaların sanal özel ağ teknolojilerine entegre edilmesinin etkileri üzerine incelemelerde bulunulmuş ve öneriler sunulmuştur.	Kuantum Güvenli Kriptografi
ETSI TR 103 616 V1.1.1 (2021-09)	CYBER; Quantum-Safe Signatures	Kuantum güvenli imza şemaları için literatürde yer alan önerilerin karşılaştırması sunulmuştur.	Kuantum Güvenli Kriptografi
ETSI TR 103 570 V1.1.1 (2017-10)	CYBER; Quantum-Safe Key Exchanges	Kuantum güvenli anahtar değişim algoritmaları için literatürdeki önerilerin karşılaştırması sunulmuştur.	Kuantum Güvenli Kriptografi

4.2. ISO/IEC

Uluslararası Standardizasyon Teşkilatı (International Organization for Standardization – ISO) uluslararası standart geliştiren ve yayımlayan Türkiye'nin de aralarında bulunduğu 167 ülkeden üyesi bulunan kâr amacı gütmeyen bir organizasyondur. Uluslararası Elektroteknik Komisyonu (International Electrotechnical Commission – IEC) ise, uluslararası standartlar geliştiren ve elektroteknoloji alanında uygunluk değerlendirme sistemlerini işleten, 1906 yılında İsviçre Kanunlarına göre kurulmuş, kâr amacı gütmeyen uluslararası bir sivil toplum kuruluşudur. ISO, elektroteknik standardizasyon ile ilgili tüm konularda IEC ile yakın iş birliği içinde olup birçok standart da söz konusu kuruluşların ortak yayını şeklinde yayımlanmaktadır (ISO, About us, 2023), (IEC, 2023).

ISO/IEC JTC 1/SC 27, ISO ve IEC'nin Ortak Teknik Komitesi 1 (JTC 1) himayesinde faaliyet gösteren; veriler ile bilgi ve iletişim teknolojilerinin korunmasına yönelik standartların geliştirilmesine katkıda bulunan bir standardizasyon alt komitesi olup JTC 1 komitesi tarafından ISO/IEC JTC 1/SC 27'de kuantum anahtar dağıtımının güvenlik gereksinimlerini, test ve değerlendirme yöntemlerini ele alan bir çalışma projesi başlatmıştır. Bu kapsamda yayımlanan;

- "ISO/IEC 23837-1 Information security- Security requirements, test and evaluation methods for quantum key distribution, Part 1: Requirements" adlı

standartta kuantum anahtar dağıtım yöntemlerinde iletişim kuran iki tarafın önceden gizli bir anahtarı paylaştığını varsayan sıkı güvenlik modelleri aracılığıyla uygulanmasının kanıtlanmış protokol güvenliği sunduğu belirtilerek siber tehdit istihbaratı yaşam döngüsü aşamalarında oluşturulan modeller ile uygulamalar arasında tutarsızlıkların ortaya çıktığı ifade edilmiştir. Söz konusu tutarsızlıkların ise kuantum anahtar dağıtım sistemlerinin güvenliğini tehlikeye atan yan kanal saldırıları ve siber saldırılara maruziyet gibi güvenlik açıklıklarına neden olabileceği belirtilerek kuantum anahtar dağıtımına yönelik potansiyel saldırıların tanımlanması ve genel güvenlik gereksinimlerin belirlenmesi amaçlanmış (ISO, 2023), kuantum anahtar dağıtım modülü üreticileri için kuantum anahtar dağıtım protokolünün uygulanmasında klasik ve kuantum ağ bileşenlerinin de dahil edildiği ortak güvenlik spesifikasyonları tanımlanmıştır (ISO, 2023).

- "ISO/IEC 23837-1 Information security- Security requirements, test and evaluation methods for quantum key distribution, Part 2: Evaluation and testing methods" adlı standart ile kuantum anahtar dağıtım sistemlerinde kuantum durum iletimi ve eleme prosedürü testi, verici modülündeki kuantum optik bileşenin foton sayısı ile darbe yoğunluk analizi, durum kodlaması doğruluğunun testi, alıcı modülünde tespit olasılığı tutarlılığı, bilgi sızıntısı ile optik izolasyon testi, sistemde saldırı potansiyeli hesaplanması gibi güvenlik değerlendirme ve test yöntemleri belirtilmiş,uygun güven aralığında iletişim güvenliğinin sağlanabilmesi için tamamlayıcı değerlendirme faaliyetlerine yer verilmiştir, (ISO, 2023)

4.3. ENISA

Avrupa Birliği Siber Güvenlik Ajansı (European Union Agency for Cybersecurity-ENISA), AB, üye devletler, özel sektör ve Avrupa vatandaşları için bir ağ ve bilgi güvenliği uzmanlığı merkezidir. ENISA, bilgi güvenliğinde iyi uygulamalar konusunda rehberler ve öneriler geliştirmek için bu paydaşlarla birlikte çalışmaktadır. ENISA, AB'ye üye devletlerle ilgili AB mevzuatını uygulamada yardımcı olmakta ve Avrupa'nın kritik bilgi altyapısı ve ağlarının dayanıklılığını artırmak için çalışmaktadır (ENISA, 2023).

ENISA, ülkeler arasındaki kuantum bilişim rekabetinde yaşanan gelişmeleri göz önünde bulundurarak Avrupa'nın tehditlere karşı ivedilikle önlem alması gerektiğini vurgulayarak kuantum güvenli şifreleme ile ilişkili çalışmalar gerçekleştirmiş ve tavsiye niteliği taşıyan rehber dokümanlar yayınlamıştır. 2021 yılı Mayıs ayında "Post-Quantum Cryptography: Current state and quantum mitigation" adlı raporunu yayınlayarak kuantum güvenli şifreleme algoritmalarının standardizasyon sürecine ilişkin analiz ve değerlendirmelerde bulunmuş, NIST tarafından düzenlenen kuantum güvenli kriptografi standardizasyon yarışmasında finalist ya da alternatif aday olarak belirlenen algoritmaların kriptotasarımı, uygulama değerlendirmeleri, bilinen kriptanaliz girişimleri ile avantaj ve dezavantajlarına ilişkin bilgiler sunulmuştur (ENISA, 2021).

2022 yılının Ekim ayında yayınlanan ve 2021 yılında yayınlanan raporun devamı niteliğinde olan "Post-Quantum Cryptography: Integration study" adlı raporda ise standardizasyon süreci sonrasında yaşanabilecek zorluklara ilişkin bilgi verilerek kuantum güvenli kriptografi algoritmalarının mevcut protokollere entegrasyonu, kuantum güvenli kriptografik algoritmalar doğrultusunda tasarlanan yeni protokoller ve kuantum güvenli etkin protokollere yönelik standardizasyon çalışmalarına değinilmiştir. Raporda ayrıca;

- Kuantum teknolojiler alanında yaşanan tüm gelişmelerin paylaşılmadığı ve yeterli bilgi işlem gücüne sahip bir kuantum bilgisayarın üretilmesi halinde duyurulmamasının ihtimaller dahilinde olduğu,
- Yeni bir şifreleme sisteminin kullanıma sunulmasının büyük bir çaba ve zaman gerektirdiği, bu sebeple gerekli önlemlerin alınabilmesi amacıyla hazırlıklara bir an önce başlanması gerektiği,
- NIST tarafından düzenlenen yarışmada seçilen kuantum güvenli kriptografik algoritmaların çözümün bir parçası olduğu ancak mevcut protokollere entegre edilmesinin ya da yeni bir sistemin veya protokolün tasarlanmasını gerektireceğinden anahtar ile şifreli metin boyutu, hesaplama süreleri ve özel kullanım durumları gibi beklenmedik problemler yaşanabileceği, bu durumun her kullanım durumuna özel bir geçişin ve dolayısıyla daha fazla ek yüke sebebiyet verebilecek çok sayıda alternatif oluşturulmasının gerekebileceği,

- Önerilen kuantum güvenli kriptografik algoritmaların güvenlik seviyelerine yönelik ilk aşamalarda belirsizlikler olabileceği, mevcut kriptografik yöntemlerden geçiş yapıldığında yeni bir kriptanalitik saldırı yöntemlerinin keşfedilebileceği, kuantum güvenli kriptografik sistemlere geçişin yıllarca sürecek bir araştırmayı ve kanıtlanmış güvenlik seviyelerini gerektirmesi sebebiyle ilk uygulayıcıların yeterli güvenlik düzeyinde olduğu kanıtlanmış şifreleme algoritmalarını kuantum güvenli kriptografik algoritmaların güvenliğinin kanıtlanıncaya dek ikili şifreleme gibi yöntemlerle kullanmaya devam etmesi önerilmiş, standartlaştırma sürecindeki algoritmalara ilişkin kesin bir karar verilinceye dek büyük değişikliklerden imtina edilmesi gerektiği, aksi takdirde yapılan herhangi bir değişikliğin hem tasarım hem de uygulama düzeyinde güvenlik zafiyetine sebebiyet verebileceği,
- Standardizasyon kuruluşlarının kuantum saldırılara karşı savunmasız olduğu bilinen şifreleme protokollerini hala standartlaştırmaya devam ettiği belirtilerek bu tür gelişmiş protokollere hibrit sistem kavramlarının (çift şifreleme, çift imza vb.) uygulanmasının önerildiği, yeni standartlar geliştirilirken veya mevcut standartlar güncellenirken kuantum güvenli kriptografi entegrasyonunun mutlaka dikkate alınması gerektiği

ifade edilmiştir (ENISA, 2022).

4.4. GSMA

Küresel Mobil İletişim Sistemi Derneği (GSM Association – GSMA), pozitif iş ortamları ve toplumsal değişim için temel teşkil eden yenilikleri keşfetmeyi, geliştirmeyi ve sunmayı amaçlayarak mobil ekosistemi birleştiren küresel bir organizasyondur. GSMA vizyonunu insanların, endüstrinin ve toplumun gelişmesi için bağlantının gücünü ortaya çıkarmak olarak belirtmişlerdir. Mobil ekosistem ve bitişik sektörlerdeki mobil operatörleri ve kuruluşları temsil eden GSMA, üyelerine "Endüstri Hizmetleri ve Çözümleri, İyi Bağlantı ve Sosyal Yardım" ana başlıklarında hizmet vermektedir (GSMA, About us, 2023)

GSMA, kuantum kriptografi alanında da çalışmalar gerçekleştirmiş olup 2022 yılında gerçekleştirilen "Mobile World Congress Las Vegas" konferansında telekomünikasyon

şirketlerini kuantum çağına hazırlamak ve ekosistemi bir araya getirmek amacıyla IBM ve Vodafone tarafından başlatılan "Post Quantum Telco Network" adlı görev gücünü kurmuştur. Görev gücü önemli bir ilerleme kaydetmiş, 50'den fazla şirket ve 20'den fazla büyük operatör sürece dahil olmuştur. 2023 yılında gerçekleştirilen "Mobile World Congress Las Vegas 2023" konferansında ise "Guidelines for Quantum Risk Management for Telco" isimli teknik incelemesini yayınlamıştır. Bahse konu teknik inceleme ne zaman gerçekleşeceği henüz belli olmasa da yeterli bilgi işlem gücüne sahip bir kuantum bilgisayarın gelecekte kullanıma sunulacağının kabul edildiği ve telekomünikasyon sistemlerini korumak için faydalanılan asimetrik anahtarlı algoritmaların savunmasız hale geleceğini, hatta kuantum bilgisayarın inşasından öncesinde dahi kötü niyetli kişilerin daha sonrasında şifreyi çözmek için şifrelenmiş verileri toplayıp sakladığı "şimdi depola, şifresini sonra çöz" saldırısı ile kuantum bilgisayara eriştiği bir zaman diliminde savunmasız hale getirebileceğini belirterek telekomünikasyon şirketlerinin;

- En riskli kategoride yer alan veri ve sistemlerin belirlenebilmesi için bir kriptografi risk değerlendirmesi planlanmasını,
- Gelişmelerinden ve karşılaşılabilecek risklerinden haberdar olabilmek için konuya ilişkin uzmanlardan oluşan bir ekip tayin edilmesini,
- Kuantum güvenli kriptografik algoritmalara ilişkin bir geçiş planı geliştirilmesini

tavsiye etmiştir (GSMA, 2023)

4.5. Elektrik ve Elektronik Mühendisleri Enstitüsü

Elektrik ve Elektronik Mühendisleri Enstitüsü (Institute of Electrical and Electronics Engineers-IEEE); elektrik, elektronik ve bilgi işlem alanlarında insanlığın yararı için inovasyonu ve teknolojik mükemmelliği geliştirmeye adanmış bir kuruluş olup dünyanın en büyük teknik profesyonel topluluğu olarak tanımlanmaktadır (IEEE, 2024). IEEE teknik ilgi alanlarını temsil eden 39 teknik topluluk bulunmakla birlikte IEEE Bilgisayar Topluluğu (IEEE Computer Society), IEEE İletişim Topluluğu (IEEE Communications Society), IEEE Sinyal İşleme Topluluğu (IEEE Signal Processing Society), IEEE Fotonik Topluluğu (IEEE Photonics Society) ile IEEE Standart Birliği (IEEE Standards Association) gibi katılımcı topluluklar ile birlikte kuantum

teknolojileri alanındaki tüm gelişmeleri izlemek, zorlukları ve fırsatları belirlemek gibi amaçlarla IEEE Kuantum Teknik Komitesi (IEEE Quantum Technical Community-QTC) oluşturulmuştur (IEEE Quantum, 2024).

Ulusal ve uluslararası alanda çeşitli konferanslar ve sempozyumlar gerçekleştirerek en yeni çalışmaların paylaşımını sağlayan IEEE'nin konferans bildirilerini yayımladığı dijital kütüphane IEEE Xplore internet sayfasında kuantum anahtar dağıtımı ile kuantum dirençli kriptografi alanlarında yapılan güncel çalışmalara aşağıda yer verilmektedir.

- Saniyede trilyon döngü anlamına gelen ve milimetre altı radyasyon olarak bilinen THz (Terahertz) dalgalarının kullanıldığı yüksek hızlı THz frekans aralığındaki iletişiminin kuantum anahtar dağıtımında kullanılabilirliğine yönelik araştırmaların gerçekleştirilmiş ve bu iletişim yönteminin kısa mesafelerde mümkün olduğu görülmüştür (Ottaviani, 2020) (S. R. Hasan, 2023).
- Kuantum anahtar dağıtımı yönteminde yer istasyonları arasında ulaşılabilir kuantum anahtar dağıtım aralığını genişletebilmek için düşük maliyetli mikro-uydu teknolojisi ile yüksek kapasiteli THz frekanslarının LEO tabanlı uydular arası kuantum iletişim aracı olarak kullanılabilirliği araştırılmış ve söz konusu entegrasyonun küresel ölçekte kuantum iletişim için kolaylaştırıcı bir adım olabileceği değerlendirilmiştir (Z. Wang, 2019).
- Optik iletim ortamının taşıma kapasitesinin artırılması için farklı dalga boylarındaki optik taşıyıcılar kullanılarak birden fazla sinyalin tek bir fiber optik kablo üzerinden çoğaltılmasının yanı sıra fiber optik kablonun bağlantı kapasitesini artıran taşıma tekniği yoğun dalga boyu bölmeli çoğullama sistemi (Dense Wavelength Division Multiplexing)[1] üzerinden kuantum anahtar dağıtımı yönteminin kullanıldığı bir şema önerilmiştir (J. Azocar, 2021).
- Kuantum anahtar dağıtım yönteminin gelecek vaat eden bir teknoloji olması ve büyük ölçekli uygulamalar için uygun maliyetli bir teknoloji haline getirilebilmesi için mevcut klasik iletişim ağlarının altyapısına uyarlanmasının

[1] Yoğun dalga boyu bölmeli çoğullama sistemi; tek bir fiber optik kablo üzerinden farklı bilgileri farklı dalga boyu kullanan taşıyıcılardan yararlanarak birden fazla bilginin birbirini etkilemeden iletilmesini sağlayan sistemlerdir.

beklenmesi sebebiyle yoğun dalga boyu bölmeli çoğullama tekniklerinin kullanılarak aynı fiber kablo üzerinde hem kuantum hem de klasik verilerin eşzamanlı olarak iletiminin gerçekleştirilebileceği bir yöntemde karşılaşılan gürültü kaynaklarının elimine edilebilmesi uygun bir dalga boyu atamasının yapılması önerilerek bir model sunulmuş ve ulaşılabilir gizli anahtar üretim oranının iyileştirilebileceği gösterilmiştir (S. Bahrani, 2016).

- Birbirleriyle etkileşime girebilen milyarlarca makinenin birbirine bağlanmasını sağlayan nesnelerin interneti teknolojisinde, şifreleme, kimlik doğrulama vb. koruma mekanizmalarının uygulanmasının cihazların doğası gereği zor olması nedeniyle sunucuya gönderilen verileri şifrelemek amacıyla IoT cihazları ile sunucu arasındaki kuantum anahtar dağıtımını simüle eden yeni yaklaşımların önerilmişitir (Ati, 2023), (Ristov & Koceski, 2023), (Al-Mohammed & Yaacoub, 2021).
- Günümüz kriptografik yöntemleri, kuantum kriptografi ve kuantum dirençli kriptografik algoritmaların TLS 1.3'e entegre edilebilmesine yönelik bir şema önerilmiştir (Garcia, Aguilera, Olmos, Monroy, & Rommel, 2023).
- Fiber optik veya uydu tabanlı kanallarla oluşturulmaya çalışılan kuantum ağlarının mobil, yeniden yapılandırılabilir ve kablosuz platformları içerecek şekilde genişletilebilmesi amacıyla drone tabanlı bir mobil platform kuantum anahtar dağıtım sistemi geliştirilmesi önerilmiştir (Isaac & vd., 2022).
- Kamu kurumları, kritik altyapı kuruluşları, veri merkezleri, ve finans sektörü gibi yüksek güvenlik ihtiyacı bulunan kurum ve kuruluşlarda kuantum öncesi kriptografik algoritmalar, kuantum anahtar dağıtım yöntemleri ve kuantum dirençli kriptografik algoritmaların hibrit bir şekilde kullanımı sağlanarak üç anahtarlı bir birleştirici şema oluşturulmuş ve güvenliği kanıtlanmıştır (Ricci & vd., 2024).
- Şifreleme altyapısında açık anahtar altyapısı ile özetleme fonksiyonlarını kullanan blokzincir teknolojisinin yeterli bilgi işlem kapasitesine sahip kuantum bilgisayarın inşası ve dolayısıyla Groover ile Shor algoritmalarının uygulanabilir hale gelmesi neticesinde güvenliğinin tehdit altına girecek olması sebebiyle blokzincirler için en uygun kuantum sonrası şifreleme sistemleri ve bu süreçte karşılaşılacak temel zorluklar analiz edilmiştir (Fernández-Caramès & Fraga-Lamas, 2020).

- Kuantum anahtar dağıtım yönteminde kuantum bit hata tahmini ve hata düzeltme aşamalarında gerçekleştirilen anahtar ayrıştırma işleminde yapay sinir ağlarının entegrasyonu ile anahtar dağıtım performansının yönetilebilirliği incelenmiştir (Das & Kule, 2022).
- Fiber optik kanalları vasıtasıyla iletimin gerçekleştirilmeye çalışıldığı kuantum anahtar dağıtım yöntemlerinde kuantum sinyallerinin zayıfladıktan veya kaybolduktan sonra kopyalanamaması veya kurtarılamaması nedeniyle pratikte uygulaması oldukça zor olan kuantum tekrarlayıcılar yerine kuantum sinyallerinin daha yoğun bir şekilde dağıtımının gerçekleştirildiği bir yöntem ile birlikte özel bir frekans dönüşümü gerçekleştiren alıcıların kullanıldığı bir sistem uygulanarak kodlanmış kuantum bilgilerin geri yüklenebilmesi sağlanmış ve BB84 protokolünün uygulanabilirliği kanıtlanmıştır (Velev & vd., 2015).
- Kuantum anahtar dağıtım yönteminde fiber optik kablolarda yaşanan gizli anahtar iletim başarı oranının mesafenin artmasıyla birlikte sınırlanması sebebiyle uydu bağlantılarının kullanılmasının daha makul olduğu belirtilerek çok yüksek irtifada sabit konumda bulunan Yerdurağan Yörünge Uyduları ile yalnızca belirli bir yer istasyonu tarafından sınırlı bir süre boyunca görülebilen alçak yörünge uydularının kullanılarak yavaş fakat sürekli bir anahtar üretim hizmeti sağlanabileceği ortaya konularak küresel ölçekte BB84 protokolünün kullanılabildiği bir yönlendirme ve kaynak tahsis modeli oluşturulabileceği kanıtlanmıştır (Grillo & vd., 2021).
- Kuantum anahtar dağıtım yönteminin büyük ölçekli ağlarda ve uzak mesafelerde verimli bir şekilde kullanılabilmesi amacıyla ağa kuantum tekrarlayıcıların ve güvenilir düğümlerin eklenerek dolanıklık tabanlı çalışan E91 kuantum anahtar dağıtım yönteminin performansı değerlendirilmiş, belirli mesafelerdeki iletişimlerde optimal bir şekilde yerleştirilen bir güvenilir düğümün[2] ağa eklenmesinin ideal tekrarlayıcı teknolojisiyle bile ulaşılabilen anahtar hızı iletimini büyük ölçüde iyileştirebileceği ortaya konulmuştur (Amer & vd., 2020).

[2] Güvenilir düğüm: Kullanıcı tarafından iletilen anahtarı yeniden şifreleyerek bir sonraki düğüme iletimini gerçekleştiren düğüm

- Kuantum anahtar dağıtım yöntemlerinde kullanılan klasik iletişim kanalının kimlik doğrulama mekanizmasının olmaması ve kuantum bilgisayarlara karşı veri gizliliği sağlamamasından kaynaklanan güvenlik açığının üstesinden gelebilmek için bu iletişim kanalında Falcon ve Crystal-Kyber gibi kuantum dirençli kriptografik algoritmaların kullanımı önerilmiştir (Dhanush & Jain, 2023)

Bu çerçevede son yıllarda IEEE tarafından gerçekleştirilen konferanslarda kuantum kriptografi alanında; kuantum anahtar dağıtım yöntemlerinin daha geniş alanlarda kullanılabilmesi amacıyla uydu tabanlı ve fiber optik kablo tabanlı iletişim kanallarında foton iletimine yönelik yaşanan problemlere ilişkin çözüm yöntemlerinin araştırıldığı ve anahtar üretim hızının artırılmaya çalışıldığı, kuantum anahtar dağıtım yönteminde kullanılabilen klasik iletişim kanalının güvenilirliğini artırmaya yönelik çalışmalar gerçekleştirildiği, kuantum hesaplama teknolojilerinin yeterli bilgi işlem seviyesine ulaşmadan önce IoT cihazlarında, blokzincir teknolojisinde ve kritik altyapı sektörlerinde kullanılacak kriptografik yöntemlerin kararlaştırılmasına yönelik araştırmaların olduğu anlaşılmaktadır.

5. ÜLKE UYGULAMALARI VE DÜZENLEME ÖRNEKLERİ

Bu bölümde kuantum mekaniğine dayalı yöntemler kullanılarak yüksek güvenlikli iletişime olanak tanıyan bir iletişim altyapısının geliştirilmesine yönelik olarak dünya genelinde gerçekleştirilen çalışmalar ve düzenleme örnekleri ile konuya ilişkin ülkemiz mevzuatı incelenmiştir. Ülke düzeyinde gerçekleştirilen çalışmalar incelendiğinde, günümüzde yaygın olarak kullanılan kriptografi algoritmalarının özellikle kuantum bilgisayarların da yeterli bilgi işlem kapasitesine ulaşması ile siber saldırılara karşı savunmasız hale geleceği endişesi ile fiber optik kablolar ve uydu tabanlı bağlantıların oluşturularak güvenli iletişime olanak tanıyan kuantum anahtar dağıtımı yöntemine dayalı kuantum iletişim altyapısının oluşturulmaya çalışıldığı, bununla birlikte güvenli bir şekilde saklanmak istenen verilerin kuantum bilgisayar tehditlerine dirençli olduğu düşünülen kuantum güvenli kriptografik algoritmalar ile korunmasına yönelik planlamaların yapıldığı görülmektedir.

5.1. Avrupa Birliği

Avrupa Birliği (AB), kuantum teknolojileri alanında yürütülen projeler ile kuantum teknolojilerin sebebiyet vereceği yıkıcı etkilerinden korunmanın yanı sıra finanse edilen araştırma-geliştirme faaliyetleri ve projeler ile Avrupa'nın kuantum teknolojileri alanındaki bilimsel liderliğinin sağlamlaştırılmasını ve kuantum teknolojilerinin yıkıcı etkilerini, bu etkilerden yararlanan ticari uygulamalara dönüştürülmesini hedeflediği görülmektedir. Bu doğrultuda, Avrupa Kuantum Teknolojileri Amiral Gemisi (Quantum Technologies Flagship-QT-Flagship), QuantERA programı, COST Eylemleri ve uzay programı gibi kuantum iletişim projelerini finanse eden AB programları bulunmakla birlikte kuantum anahtar dağıtımına ilişkin standardizasyon çalışmaları ETSI tarafından gerçekleştirilmektedir.

AB, 2016 yılının Mayıs ayında yaşanan teknolojik devrimde Avrupa'nın öncü rolü üstlenmesini sağlamak ve kuantum teknolojileri alanında Avrupa girişiminin başlatılabilmesi için bir çağrı niteliğinde olan "Quantum Manifesto-A New Era of Technology" isimli bildirisini yayımlamış ve bilimsel araştırma girişimi olan "Horizon 2020" (Ufuk 2020) programı kapsamında 2018 yılında faaliyetlerine başlamak üzere

10 yıllık bir zaman dilimi için 1 milyar Avroluk kaynak ayrılmıştır. Ayrıca bildiride kuantum güvenli kriptografik algoritma tasarımı ile kuantum anahtar dağıtımına dayalı iletişime de yer verilmiş;

- Kısa vadeli hedeflerde (0-5 yıl), uçtan uca güvenli iletişimi garanti eden kuantum iletişimin altyapısında kullanılan kuantum sinyal tekrarlayıcı teknolojisinin geliştirilmesi,
- Orta vadeli hedeflerde (5-10 yıl), kuantum iletişim ağı vasıtasıyla uzak şehirler arasında güvenli iletişimin sağlanması ve yer istasyonları ile uydular arasındaki iletişimin kuantum kriptografi aracılığıyla gerçekleştirilmesi,
- Uzun vadeli hedeflerde (>10 yıl) ise kuantum iletişim protokolleri ve kuantum tekrarlayıcılarının da kullanılarak Avrupa'daki büyük şehirleri birbirine bağlayan güvenli ve hızlı bir kuantum internet oluşturması

hedeflenmiştir (EuropenCommission, 2016).

QT Flagship 2016 yılında yayımlanan kuantum manifestosunun ardından 2018 yılında başlatılan, AB tarafından finanse edilen, 1 milyar Avro bütçeli, büyük ölçekli ve uzun vadeli bir araştırma girişimidir. Proje ile, araştırma kurumları, endüstri ve kamu kuruluşlarının finansörlüğünde Avrupa'nın kuantum teknolojileri alanındaki bilimsel liderliğinin ve üstünlüğünün sağlamlaştırılması, gerçekleştirilen araştırmalar ile kuantum teknolojilerinin yıkıcı etkilerinin bu etkilerden yararlanan ticari uygulamalara dönüştürülmesi hedeflenmektedir.

Ekim 2018- Eylül 2021 arasındaki *QT Flagship* projesinin yükseliş aşaması olduğu ifade edilen zaman diliminde, kuantum bilişim, kuantum simülasyon, kuantum iletişim ile kuantum metroloji ve algılama projeleri ile birlikte uluslararası işbirliği faaliyetleri de finanse edilerek toplam 24 proje için 152 milyon Avroluk bütçe tahsis edilmiştir. *QT Flagship*'in Ufuk Avrupa (Horizon Europe) projesi kapsamında finanse edilen bir sonraki aşaması ise başlamış olup gerçekleştirilen araştırmalar neticesinde edinilen veriler sayesinde endüstriyel uygulamalara dönüşümün daha da yakınlaştığı ifade edilmektedir (AvrupaKomisyonu, Quantum Technologies Flagship, 2023).

Bunun yanı sıra, AB'nin teknolojik olarak diğer ülkelere bağımlılığının azaltılması ile teknolojik kapasitesinin geliştirilmesi amacıyla oluşturulan, 7.5 milyar Avroluk bütçesiyle ekonomik toparlanmayı hızlandırmayı ve Avrupa toplumu ve ekonomisinin

dijital dönüşümünü şekillendirmeyi amaçlayan ve Ufuk Avrupa programı gibi diğer AB programları aracılığıyla sağlanan fonları tamamlayıcı nitelikte olan Dijital Avrupa Programı (Digital Europe Programme) kapsamında 2021-2027 yılları arasında kuantum teknolojilerine ek finansman desteği sunulacağı ifade edilmiştir (AvrupaKomisyonu, 2023).

QT Flagship araştırma hedefleri, 2000'den fazla Avrupalı kuantum uzmanının katkıda bulunduğu Stratejik Araştırma Gündemi (Strategic Research Agenda) tarafından belirlenmektedir. 2020 yılının Mart ayında yayımlanan söz konusu Stratejik Araştırma Gündeminde kuantum iletişim ile ilişkili olarak;

- Durağan ve aktarım halindeki verilerin gizliliği, güvenliği ve bütünlüğünün sağlanmasının yanı sıra bu verilere kuantum güvenli erişimin Avrupa'nın stratejik vizyonunun önemli bir parçası olduğu belirtilerek hem kamu hem de özel sektörde kuantum güvenli bir bilişim ekosisteminin oluşturulabilmesi amacıyla gerekli altyapı yatırımlarının yapılması gerektiği,
- Güvenli ağ işlevselliğinin daha da geliştirilerek dağıtık kuantum işlemcilerini ve sensörlerini birbirine bağlaması ile yeni uygulamaların geliştirilmesine olanak sağlayacak ve uçtan uca kuantum iletişimin gerçekleştirilmesine imkan tanıyacak olan kuantum ağlarına ilişkin olarak Avrupa'nın teknolojik liderliğini garanti altına almak amacıyla Ar-Ge yatırımlarının yapılmasının yanı sıra bu teknolojinin laboratuvardan çıkarılarak test ortamlarına aktarılmasının, Avrupa teknolojisinin dünya çapında erken benimsenmesinin ve bu konuda eğitim verilmesinin sağlanarak gelecekteki kuantum internet standartlarını belirlemek için destek sunulması gerektiği,
- Dinamik ve sağlam bir kuantum endüstrisinin büyümesi için insanlara, teknolojilere ve ticari ölçekli üretim tesislerine yatırım yapılması gerektiği, gerekli inovasyon ekosistemini oluşturmak için temel bilimden mühendisliğe kadar yeni konseptlere ve bileşen geliştirmeye yatırım yapılması gerektiği, sürecin akademiden sanayiye ve karar vericilere kadar kuantum bilincine sahip bir işgücü sağlamak için disiplinler arası eğitim ve öğretim programlarıyla tamamlanması gerektiği, uygulamaların, protokollerin ve kuantum yazılımlarının geliştirilmesinin önem arz ettiği, Avrupa'daki Küçük ve Orta Büyüklükteki İşletmelerin (KOBİ) büyük ölçekli yatırımlara gerek kalmadan kuantum cihazları üretmek için gerekli fabrikasyon ve diğer tesislere

erişebilmelerinin sağlanması, yatırımcıların risklerinin azaltılması, Avrupa'da yeni nesil kuantum KOBİ'lerinin büyümesinin teşvik edilmesi ve Avrupa'daki yüksek teknoloji üretim sektörünün canlandırılması için desteklenmesi gerektiği

ifade edilmiştir. Bu kapsamda oluşturulan yol haritasında belirlenen 3 yıllık vizyon çerçevesinde;

- Şehirler arası uçtan uca kuantum güvenli iletişimin sağlanabilmesi amacıyla uygun maliyetli ve ölçeklenebilir cihazlar ile sistemler geliştirilmesinin yanı sıra anahtar yönetimi ve uygulama yazılımları dahil olmak üzere yazılım geliştirilmesi,
- Dünya genelinde güvenli anahtar dağıtımı için uydu tabanlı kuantum kriptografinin geliştirilmesi,
- Kuantum anahtar dağıtımı ve kuantum rastgele sayı üreteçlerinin kullanımına yönelik paydaşlarla birlikte standartlar geliştirilmesi,
- Ağ performansı, uygulamalar, protokoller ve yazılımlar için testlerin gerçekleştirilmesi,
- Avrupa genelindeki üniversitelerde kuantum iletişimi ve güvenliğine yönelik eğitim faaliyetlerinin başlatılması

hedefleri, yol haritasında 6-10 yıllık belirlenen vizyon çerçevesinde ise;

- Fiber optik kablo altyapısının kullanılarak en az 800 km uzaklıkta kuantum iletişim uygulamasının gerçekleştirilmesi,
- Bir kuantum ağına bağlı en az 20 kübitlik bir kuantum ağ düğümünün oluşturulması,
- Uydu tabanlı bağlantıların kullanılarak dolanıklık oluşumunun gösterilmesi,
- Gelecekteki işgücünü oluşturacak bireyler ile birlikte endüstride faaliyet gösteren ağ ve güvenlik çalışanlarına yönelik eğitimlerin düzenlenmesi ve sürece dahil edilmesi

hedefleri belirlenmiştir (AvrupaKomisyonu, 2020) .

Kuantum iletişim projelerini finanse eden Kuantum Teknolojileri Avrupa Araştırma Alanı Ağı (The Quantum ERA-NET-QuantERA) konsorsiyumu ise, 31 ülkeden 41 araştırma fonu kuruluşundan oluşan ve Türkiye'yi temsilen Türkiye Bilimsel ve Teknolojik Araştırma Kurumu (TÜBİTAK)'nun tam üye olduğu bir Avrupa Araştırma

Alanı Ağı (European Research Area Networks-ERA-NET) programıdır. Programın temel amacı, uluslararası iş birlikleri yoluyla Kuantum Bilimleri ve Teknoloji alanlarında çığır açacak ileri araştırma projelerinin desteklenmesidir. Bu amaçla QuantERA Proje Konsorsiyumu tarafından düzenli olarak ortak uluslararası çağrılara çıkılmaktadır (QuantERA, 2023).

Bilim ve Teknoloji Alanında Avrupa İşbirliği (European Cooperation in Science and Technology-COST) ise bilim ve teknolojide Avrupa iş birliği için 1971 yılında oluşturulmuş olan ve ulusal kaynaklarla desteklenmiş araştırma projelerinin Avrupa düzeyinde koordinasyonunu sağlayan hükümetler arası bir kuruluştur. Kurucu üyeler arasında ülkemizin de yer aldığı kuruluşun Türkiye'deki bilimsel koordinatörlüğü TÜBİTAK tarafından yürütülmektedir. COST'un misyonu, Avrupalı araştırmacılar arasında etkileşim ve iş birliğini destekleyerek; Avrupa'yı barışçıl amaçlar için bilimsel ve teknik araştırmada güçlendirmektir. Bu amaçla COST, ulusal olarak desteklenen tüm alanlardaki araştırma projelerinin yürütücülerinin Avrupa düzeyinde oluşturulmuş ağlara (aksiyonlara) dahil olmalarını sağlamakta ve belirli bir konu çerçevesinde iş birliği yapılması ile deneyim paylaşımının gerçekleştirilmesi için platform oluşturmakta; ancak araştırmaları finanse etmemektedir. "Aksiyon" olarak adlandırılan bilimsel konu başlıkları, benzer çalışmalar yapan Avrupalı araştırmacıları bir araya getirmekte, aksiyonlara atanacak araştırmacıların seçimi ise her ülkenin ilgili mercii tarafından gerçekleştirilmektedir. Bu görev ülkemizde TÜBİTAK tarafından gerçekleştirilmektedir.

Ayrıca Avrupa Komisyonu, ulusal ve sınır ötesi düzeyde stratejik sahaları birbirine bağlayan güvenli bir kuantum iletişim altyapısı oluşturmayı (European Quantum Communication Infrastructure - EuroQCI) hedeflemekte olup bu hususta Avrupa Uzay Ajansı (European Space Agency-ESA) ile birlikte çalışmaktadır. Girişim, 2019 yılında 27 AB Üye Devletinin tamamı tarafından imzalanan *EuroQCI Deklarasyonu* ile başlatılmış olup Kuantum Amiral Gemisi 'yükselme aşaması' kapsamında geliştirilen yenilikçi kuantum iletişim teknolojileri üzerine inşa edilmiştir. Avrupa Komisyonu'nun Dijital Avrupa Programı kapsamında finanse edilen *EuroQCI'*nin ilk uygulama aşaması Ocak 2023'te başlamış olup;

- *EuroQCI* için temel teknolojik yapı taşlarını geliştirmek ve olgunlaştırmak için kuantum anahtar dağıtımı cihazlarının geliştirilmesi, güvenilirliğinin test

edilmesi gibi teknolojinin olgunlaşmasını sağlayacak bir takım endüstriyel projeye ve

- Üye devletlerin karasal segmentin temelini oluşturacak ulusal kuantum iletişim ağlarını tasarlamalarına ve inşa etmelerine, farklı teknolojileri ve protokolleri test etmelerine ve bunları her ülkenin özel ihtiyaçlarına uyarlamalarına olanak tanıyan ulusal projelere

odaklanılmıştır. *EuroQCI*'nin, kuantum tabanlı sistemleri mevcut iletişim altyapılarına entegre ederek hassas verileri ve kritik altyapıları koruması, kuantum fiziğine dayalı ek bir güvenlik katmanı sağlaması, devlet kurumları, veri merkezleri, hastaneler ve enerji şebekeleri gibi kritik altyapıların korunmasını güçlendirmesi ve AB'nin gelecek yıllar için Siber Güvenlik Stratejisinin ana sütunlarından biri haline gelmesi beklenmektedir (Avrupa Komisyonu, 2023).

Kuantum iletişim teknolojisinin gerçekleştirilebilmesi amacıyla ESA, üç farklı kuantum anahtar dağıtım projesi üzerinde çalışmaktadır. Bu kapsamda QUARTZ ve QKDSat adı verilen projelerin her ikisi de 2020'li yıllarda ticari hizmet sunmayı amaçlayan alçak irtifa uydu yörüngesi tabanlı kuantum anahtar dağıtım hizmeti sunmaya çalışırken SAGA adı verilen yüksek irtifa uydu yörüngesi tabanlı kuantum anahtar dağıtım sisteminin sunduğu kıtasal kapsama oranı ile daha geniş yüzölçümlerinde anahtar dağıtımına imkan tanıyarak güvenli iletişim hususunda avantajlı olacağı ve alçak irtifa uydu yörüngesi tabanlı kuantum anahtar dağıtım sistemleri ile entegre bir şekilde kullanılarak anahtar dağıtımında tamamlayıcı bir hizmet sunacağı ifade edilmektedir (ESA, 2023)

5.1.1. Üye Devletlerin Kuantum İletişim Teknolojileri Alanında Gerçekleştirdiği Uygulamalar

Avrupa'da kuantum iletişiminin yaygınlaştırılması için gereken teknoloji bileşenlerinin geliştirilmesi için halihazırda çeşitli girişimler bulunmakla birlikte birkaç ülke kendi kuantum iletişim altyapılarını geliştirmeye başlamıştır. Bu doğrultuda;

- Hollanda'da Amsterdam, Delft, Leiden ve Lahey arasında gelecekte inşa edilecek bir "Kuantum internetine" yönelik ilk adım olduğu iddia edilen bir kuantum ağı kurulmaktadır.

- Avusturya ve İsviçre'de kuantum ağları kurmuş ve kuantum anahtar dağıtımı saha içi deneyleri gerçekleştirmiştir.
- Almanya yakın zamanda kuantum tekrarlayıcıların geliştirilmesi için 15 milyon Avroluk bir projeyi finanse etmiştir.
- 2018 yılında başlatılmış olan Madrid kuantum ağının (MadQCI) kuantum iletişim altyapısının bir bileşeni İspanyol telekomünikasyon şirketi olan Telefónica de España Üretim Ağına, diğer bileşeni ise Madrid Araştırma Ağına (REDIMadrid) aittir. Üretim ağındaki bölümde yüksek teknoloji-hazırlık seviyesindeki cihazların testinde kullanılmakta iken iki bağımsız ağ servis sağlayıcısının (Telefonica ve REDIMadrid) altyapılarını da birbirine bağlaması ve çok kiracılı bir kuantum ağının ilk örneği olması MadQCI ağını dünya genelinde benzersiz kılmaktadır.
- INRiM (National Metrology Institute of Italy) tarafından koordine edilen İtalyan ulusal kuantum iletişim altyapısı, Torino'dan Floransa'ya uzanan bir kuantum anahtar dağıtım ağı içermekte ve Floransa'da bir kuantum anahtar dağıtımı metropol alan ağı inşa edilmektedir (Avrupa Komisyonu, 2022).

5.1.2. Avrupa Birliği Düzenlemeleri

Bununla birlikte Avrupa Parlamentosu ve Avrupa Birliği üyesi ülkeler 2.4 milyar Avro bütçeli 2023-2027 dönemi için Güvenli Bağlantı Programı (EU Secure Connectivity Programme) üzerinde anlaşmış ve EU 2023/588 sayılı Yönetmelik ile "IRIS" adı verilen ve AB Üye Devletlerine askeri uygulamaların yanı sıra kritik altyapının korunması, gözetim ve dış eylem veya kriz yönetimi desteği gibi operasyonel ihtiyaçlarını karşılayan yüksek güvenlikli, egemen ve küresel bağlantı hizmetlerine garantili erişim sağlama hedefleri olan uydu sistemi güvenliğinde kuantum kriptografi de dahil olmak üzere gelişmiş şifreleme teknolojilerinin kullanılmasına karar verilmiştir. EU 2023/588 sayılı düzenlemede ayrıca, kuantum anahtar dağıtım teknolojisi ile ürünlerinin Avrupa Birliği gizli bilgilerinin korunması için kullanılacak kadar olgunlaşmadığı belirtilerek kuantum anahtar dağıtım protokollerinin standardizasyonu, yan kanal analizi ve değerlendirme metodolojisi gibi güvenliğine ilişkin ana konuların hala çözülememiş olduğundan bahisle Programın, EuroQCI'yi

desteklemesinin ve mümkün olduğunda onaylanmış kriptografik ürünlerin altyapıya dahil edilmesine izin verilmesinin gerektiği ifade edilmiştir (AvrupaBirliği, 2023).

Bununla birlikte, Avrupa'nın dijital dönüşüm hedeflerini içeren Dijital Pusula 2030 (2030 Digital Compass: the European way for the Digital Decade) Avrupa Birliği'nin kuantum teknolojilerine yatırım yapması gerektiği belirtilerek iletişim ve veri aktarım güvenliğinin artırılması hususlarına yer verilmiş ancak 2030 hedefleri arasına dahil edilmemiştir (Avrupa Komisyonu, 2021).

2023 yılının Haziran ayında yayınlanan Avrupa Ekonomik Güvenlik Stratejisinde (European Economic Security Strategy, JOIN (2023)) kuantum hesaplama teknolojilerine yönelik araştırmaların yapılması ve endüstriyel tabanın desteklenmesi gerektiği belirtilmiştir (Avrupa Komisyonu, 2023). Ortak bir risk değerlendirmesinin yapıldığı ve ekonomik güvenlik için kritik teknoloji alanlarını belirleyen Ekim 2023 tarihli Komisyon Tavsiyesinde (Commission Recommendation of 03.10.2023) ise ekonomik değeri olan endüstriyel sırların çalınmasına yönelik olarak kuantum teknolojileri grubunda kuantum iletişim, kuantum kriptografi, kuantum hesaplama ve kuantum algılama alanları en yüksek önceliğe sahip olan dört teknoloji grubu arasında yer almış, üye devletlerle birlikte toplu bir risk değerlendirmesine tabi tutulması gerektiği ifade edilmiştir (Avrupa Komisyonu, 2023).

2023 yılının Aralık ayında ise Fransa, Belçika, Hırvatistan, Yunanistan, Finlandiya, Slovakya, Slovenya, Çek Cumhuriyeti, Malta, Estonya ve İspanya tarafından onaylanan Kuantum Teknolojilerine İlişkin Avrupa Deklarasyonu (European Declaration on Quantum Technologies) ile bahsi geçen imzacı üye devletler, kuantum teknolojilerinin AB'nin bilimsel ve endüstriyel rekabet gücü açısından stratejik önemini kabul etmiş ve Avrupa'yı dünyanın "kuantum vadisi haline getirilmesi ve Avrupa çapında dünya standartlarında bir kuantum teknolojisi ekosisteminin geliştirilmesi amacıyla işbirliği yapmayı taahhüt etmiştir. Bu amaç doğrultusunda, dünya üzerinde ve uzayda güvenli iletişim, kuantum hesaplama, kuantum simülasyon ve kuantum algılama alanlarında geleceğin Avrupa çapında kuantum altyapılarını kolektif olarak inşa etmek için faaliyetlerde bulunulmasında üye devletler ve Avrupa Komisyonu ile birlikte çalışmayı kabul etmişlerdir (AvrupaKomisyonu, 2023).

5.2. Amerika Birleşik Devletleri

Dünya genelinde ilk fiber tabanlı kuantum anahtar dağıtım ağı 2004 yılında DARPA (Defense Advenced Research Projects Agency-DARPA) tarafından finanse edilerek oluşturulan, Harvard Üniversitesi, Boston Üniversitesi ve BBN Technologies'in Cambridge'deki (Massachusetts) ofisinde bulunan tesislerini altı düğümle birbirine bağlayan bir fiber optik ağıdır (Colvin, 2005). DARPA'nın 2006 yılında bu proje ile ilişkili faaliyetlerini durdurduğu ve Amerika Birleşik Devletleri (ABD) devlet kurumları tarafından başka hiçbir saha uygulaması bulunmadığı (Avrupa Komisyonu, 2022) bilinmekle birlikte;

- ABD Enerji Bakanlığı'na bağlı Los Alamos Ulusal Laboratuvarı ile Oak Ridge Ulusal Laboratuvarının bir kamu hizmet şirketi ile birlikte enerji şebekesinin güvenliğini sağlamak için kuantum anahtar dağıtımı kullanımını geliştirmek üzere çalışmalar gerçekleştirdiği,
- Kar amacı gütmeyen özel bir şirket olan Batelle'nin 2013 yılından itibaren İsviçreli üretici IdQuantique tarafından sağlanan donanımı kullanarak dahili kullanım için kuantum anahtar dağıtım ağı kurduğu,
- Quantum Exchange isimli bir şirketin ise Boston ile Washington'ı 800 km boyunca dark fiber[1] kablolar ile birbirine bağlama ve konuya ilişkin olarak Toshiba ile teknik iş birliğinin devam ettiği ve finans kurumları için tasarlanmış bir kuantum anahtar dağıtım hizmetini abonelik temelinde sunmayı planladığı bilinmektedir (Avrupa Komisyonu, 2022).

Düzenleme boyutunda, 21 Aralık 2018 tarihinde imzalanan Ulusal Kuantum Girişimi Yasası (National Quantum Initiative Act) Amerika Birleşik Devletleri'nin ekonomik ve ulusal güvenliği için kuantum araştırma ve geliştirmesini hızlandırmak amacıyla imzalanmış ve NIST, Ulusal Bilim Vakfı (National Science Foundation-NSF) ve Enerji Bakanlığı'na (Department of Energy-DOE) kuantum bilişim programlarını, merkezlerini ve konsorsiyumlarını güçlendirme yetkisi verilmiştir. Yasa ayrıca sivil, savunma ve istihbarat sektörleri de dahil olmak üzere Birleşik Devletler Hükümeti

[1] Dark fiber kablolar fiber kabloların aksine ışık iletimi yapmayan- aktif olmayan kablolardır. Genellikle telekomünikasyon şirketleri tarafından kurulmakta ve kullanıcının kendi ağını kurabilmesine, istediği protokolü ve ekipmanı seçmesine, tercih ettiği ölçüde bant genişliği kullanabilmesine ve ağını ölçeklendirmesine imkan tanımaktadır. (TürkNet, 2023)

genelinde kuantum teknolojileri alanında Araştırma ve Geliştirme (Ar-Ge) çabalarına koordineli bir yaklaşım çağrısında bulunmaktadır (NQCO, 2023). Bununla birlikte, 2019, 2020 ve 2022 mali yılları için Ulusal Savunma Yetkilendirme Yasası (National Defense Authorization Act) ve 2022 Yarı İletkenlerin Üretilmesi İçin Faydalı Teşvikler Yaratılması ve Bilim Yasasında da (Creating helpful incentives to produce semiconductors (CHIPS) and Science Act) Ulusal Kuantum Girişimi Yasasını tamamlayan kuantum teknoloji alanındaki ilgili mevzuat hükümleri yer almaktadır. Bu doğrultuda, ABD'de geliştirilmekte olan kuantum bilgi bilimi teknolojilerinin teknolojiye hazırlık seviyesini artırma, kuantum bilgi bilimi ve teknolojisi işgücünün gelişimini destekleme, farkındalık artırma, araştırma geliştirme faaliyetleri gerçekleştirilmektedir.

Diğer yandan, istihbarat ve siber güvenlik faaliyetleri yürüten Amerikan Ulusal Güvenlik Ajansı (National Security Agency-NSA) ulusal güvenlik sistemlerinde veri iletimi güvenliğini sağlayabilmek amacıyla kriptografi çözümlerinin kullanımını değerlendirmeye devam ettiğini ve NIST tarafından standartlaştırma sürecinde olan kuantum güvenli kriptografi algoritmalarına ilişkin yürütülen çalışmaların tamamlanmasının akabinde ulusal güvenlik sistemlerini korumak için kamu standartlarının kullanımının belirlendiği “NSA CNSSP-15” dokümanının güncelleneceğini belirterek kuantum anahtar dağıtım yöntemlerinin kullanımını önermediğini ifade etmektedir. Ayrıca;

- Kuantum anahtar dağıtımı yönteminin yalnızca kısmi bir çözüm sağladığı, uygulama yöntemi olarak yalnızca gizlilik sağlayan bir şifreleme algoritması için anahtarlama malzemesi ürettiği, iletiminin kimlik doğrulaması yapılmadan gerçekleştiği bu sebeple kuantum anahtar dağıtım sistemlerinde asimetrik kriptografi algoritmalarının kullanılması gerektiği ifade edilerek kuantum anahtar dağıtımının sunduğu gizlilik hizmetlerinin kuantum güvenli kriptografik algoritmalar ile daha güvenli ve daha uygun maliyetlerde sunulabileceğini,
- Kuantum anahtar dağıtım yönteminin özel amaçlı ekipmanlar gerektirdiği, güvenliğinin benzersiz fiziksel katman iletişimlerinden kaynaklanması sebebiyle yazılım olarak ya da ağ üzerinde bir hizmet olarak uygulanamayacağı ve mevcut ağ ekipmanlarına kolaylıkla entegre edilemeyeceği, donanım tabanlı

olması sebebiyle yükseltmeler veya güvenlik yaması için esneklikten yoksun olduğunu,

- Güvenilir kanalların kullanımını gerektirdiği için altyapı maliyetlerini, dahili tehdit risklerini artırdığı için ek güvenlik gereksiniminin sağlanmasının gerektiğini,
- Kuantum anahtar dağıtımının güvence altına alınmasının ve doğrulanmasının sıklıkla dile getirilen fizik yasalarına dayalı koşulsuz güvenlik ile değil donanım ve mühendislik tasarımlarıyla elde edilebilecek sınırlı güvenlik ile ilişkili olduğu, bu durumun ticari amaçlı üretilmiş kuantum anahtar dağıtım sistemlerine yönelik saldırılar ile güvenlik açıklarının ortaya çıkmasına sebebiyet verebileceğini,
- Kuantum anahtar dağıtımının güvenlik iddialarının teorik temeli olarak bir gizli dinleyiciye karşı hassasiyeti de içermesi, hizmeti geçici veya süresiz olarak aksatarak bir makinenin veya ağ kaynaklarının asıl kullanıcılar tarafından erişilmemesini hedefleyen hizmet dışı bırakma saldırılarının (Denial of Service attack-DoS) söz konusu sistemler için önemli bir risk olduğunu,

belirtmiş, kuantum güvenli kriptografiyi kuantum anahtar dağıtımından daha uygun maliyetli ve bakımı daha kolay bir çözüm olarak gördüğünü ve ulusal güvenlik sistemlerinde iletişimi korumak için kuantum anahtar dağıtım kullanımını desteklemediğini bu sebeple herhangi bir kuantum anahtar dağıtım güvenlik ürününü sertifikalandırmayı veya onaylamayı öngörmediğini ifade etmiştir (National Security Agency, 2023).

Kritik altyapıları tehditlere karşı korumakla görevlendirilmiş olan Amerikan Siber Güvenlik ve Altyapı Güvenliği Ajansı (Cybersecurity and Infrastructure Security Agency-CISA), NIST'in 2024'te yayımlayacağı yeni kuantum sonrası kriptografi standardına sorunsuz bir geçiş sağlamak için hükümet ve kritik altyapı kuruluşlarının koordineli hazırlık önlemleri alması gerektiğini ifade ederek 2022 yılında Kuantum Güvenli Kriptografi Girişimini (Post-Quantum Cryptography Initiative) başlatmış ve kuantum güvenli kriptografik yöntemlere geçiş için plan yapılması gereken noktaların tanımlandığı şekil 5.1'deki yol haritası oluşturulmuştur (CISA, 2022). Buna göre Kurumlar;

- Gerekli algoritma ve protokol değişiklikleri ile ilişkili gelişmeleri takip edebilmek amacıyla standart geliştiren kuruluşlarla etkileşimlerini artırmalı ve bu hususta yöneticilerini yönlendirmelidir.
- Hangi verilerin risk altında olabileceği ve yeterli bilgi işlem gücüne sahip bir kuantum bilgisayarın üretilmesi halinde hangi kriptografik algoritmaların savunmasız hale geleceğine ilişkin analiz çalışmalarının gerçekleştirilmesi gerekmektedir.
- Gelecekte sorunsuz bir geçişi olanaklı kılmak için herhangi bir işlev için kriptografik teknolojileri kullanan tüm sistemlerin bir envanteri oluşturulmalıdır.
- Kurumdaki siber güvenlik yetkilileri kuantum sonrası gereksinimleri yansıtacak şekilde güncellenmesi gereken satın alma, siber güvenlik ve veri güvenliği standartlarını belirlemelidir.
- Asimetrik anahtarlı algoritmaların nerede ve ne amaçla kullanıldığını belirleyerek envanterde savunmasız olarak işaretlenmelidir.
- Kriptografik geçiş için belirlenen sistemin diğer sistemlere göre önceliklendirilmesi kuruluşun işlevlerine, hedeflerine ve ihtiyaçlarına göre belirlenmelidir. Önceliklendirme işlemi için kuruluşlar kuantum tehditlerine karşı savunmasız olduğu düşünülen sistem değerlendirmesinde aşağıdaki faktörleri göz önünde bulundurmalıdır:
    - Sistem kurumsal gereksinimlere göre yüksek değerli bir varlık mıdır?
    - Sistem hangi bilgileri korumaktadır (örneğin anahtar depoları, parolalar, kişisel bilgiler vb.)?
    - Sistem başka hangi sistemlerle iletişim kurmaktadır?
    - Sistem diğer kuruluşlarla ne oranda bilgi paylaşmaktadır?
    - Sistem kritik bir altyapı sektörünü desteklemekte midir?
    - Verilerin ne kadar süreyle korunması gerekmektedir?
- Kurumlar envanter ve önceliklendirme bilgilerini kullanarak yeni kuantum güvenli kriptografik standardın yayınlanmasının ardından sistem geçişleri için bir plan geliştirmelidir. Geçiş planları, gelecekteki düzenlemeleri kolaylaştırmak ve beklenmedik değişiklikler durumunda esneklik sağlamak için kriptografik çeviklik oluşturmayı göz önünde bulundurmalıdır. Siber

güvenlik yetkilileri geçiş planlarının oluşturulması için rehberlik sağlamalıdır (CISA, 2021).

Şekil 5.1. Kuantum güvenli kriptografik yöntemlere geçiş için yol haritası

Kaynak: (CISA, 2022)

Aynı doğrultuda 21.12.2022 tarihinde yürürlüğe giren Kuantum Bilişim Siber Güvenlik Hazırlık Yasası'nda (H.R.7535-Quantum Computing Cybersecurity Preparedness Act 117-260) kurumların bilgi teknolojileri sistemlerini kuantum bilgisayarlardan gelen saldırılara karşı dayanıklı olan kuantum güvenli kriptografi algoritmalarına geçirmelerine ilişkin olarak;

- Yasanın yürürlüğe girdiği tarihten itibaren en geç 180 gün içerisinde kullanımda olan bilgi teknolojilerinin kuantum güvenli kriptografiye geçişinin sağlanması için risk altında olan sistemlerin yer aldığı envanterin, envanterin önceliklendirilmesini sağlayacak kriterlerin ve raporlanması talep edilen bilgilere ilişkin açıklamanın yer aldığı bir kılavuzun yayımlanmasına,
- Yasanın yürürlüğe girmesinden itibaren en geç bir yıl içerisinde süreklilik arz edecek şekilde her kurum yöneticisinin talep edilen envanter ve raporlanması talep edilen tüm bilgileri düzenli olarak iletmesine,
- NIST tarafından yayımlanacak olan standartlaştırılmış kuantum güvenli kriptografi algoritmalarının duyurulmasının akabinde en geç bir yıl içerisinde her kurumun önceliklendirilmiş bilgi teknolojileri sistemlerinden başlamak üzere kuantum güvenli algoritmalara geçişe ilişkin bir plan belirlemesine,
- Yasanın yürürlüğe girmesinden itibaren en geç 15 ay içerisinde Bütçe ve Yönetim Ofisi (Office of Management and Budget) tarafından; kurumların bilgi teknolojilerinin zayıflatılmış şifrelemeye karşı savunmasızlığının yarattığı riski ele almak için bir strateji, söz konusu riskten korunabilmek için

kurumların ihtiyaç duyduğu tahmini finansman miktarı ve zaman çizelgesi bilgilerinin yer aldığı bir rapor sunulmasına,

- Kurumların önceliklendirilmiş bilgi teknolojileri sistemlerinden başlamak üzere kuantum güvenli algoritmalara geçişe ilişkin belirlemiş olduğu plandan itibaren en geç 1 yıl, NIST tarafından yayımlanacak olan standartlaştırılmış kuantum güvenli kriptografi algoritmalarının duyurulmasından itibaren en geç 5 yıl içerisinde kurumların kuantum güvenli kriptografik algoritmaları benimseme ve ilerlemelerine yönelik bir rapor sunulmasına

karar verilmiştir (Congress.gov, 2022).

5.3. Çin Halk Cumhuriyeti

Kuantum teknolojileri alanında gerçekleştirilen araştırma geliştirme faaliyetleri alanında uluslararası lider olduğu ifade edilen Çin Halk Cumhuriyeti, en yakın rakiplerine kıyasla (AB ve ABD) kuantum teknolojilerine on kat daha yüksek bütçe ayırmış ve hem yer tabanlı hem de uydu tabanlı kuantum telekomünikasyon ağının geliştirilmesinde ön sıralarda yer almıştır (IDB, 2019).

Uzay Ölçeğinde Kuantum Deneyleri (Quantum Experiments at Space Scale-QUESS) projesi kapsamında 2016 yılında fırlatılan alçak irtifa uydusu Micius ile çeşitli kuantum iletişim deneyleri gerçekleştirilmiş olmakla birlikte en dikkat çekici uygulaması 2017 yılında Çin ile Avusturya arasında kuantum anahtar dağıtım yönteminin kullanılması yolu ile şifrelenen bir video konferansın gerçekleştirilmesi olmuştur. 2021 yılında ise 700'den fazla fiber optik kablo bağlantılarının uydu tabanlı bağlantılarla entegre edilmesi yöntemi ile kuantum anahtar dağıtım ağı düğümlerinin 2.600 kilometreye kadar genişletildiği ve ağdaki kullanıcıların 4.600 kilometre uzaklıktaki kullanıcılarla iletişim kurmasının mümkün kılındığı belirtilmiştir (Chen Y. Z., 2021).

Çin, 2016 yılında uygulamaya koyduğu 13. Beş Yıllık Planı kapsamında, kuantum hesaplama ve kuantum iletişim teknolojileri alanında bir "mega proje" başlatmış, proje kapsamında Çin'in ulusal kuantum iletişim altyapısının genişletilmesi, genel bir kuantum bilgisayar prototipinin geliştirilmesi ve pratik bir kuantum simülatörünün

inşası da dahil olmak üzere 2030 yılına kadar bu teknolojilerde büyük atılımlar gerçekleştirilmesi hedeflenmiştir. Ayrıca, 1 milyar doların üzerindeki başlangıç finansmanıyla gelecekteki araştırma ve geliştirme faaliyetleri için kilit rol oynayacağı düşünülen Ulusal Kuantum Bilgi Bilimleri Laboratuvarı'nı da inşa etmiştir (CNAS, 2018).

2021 yılının Mart ayında kabul edilen ve 2021-2025 yıllarını kapsayan ve geçmiş planlardan farklı olarak 2035 yılına yönelik "uzun vadeli hedefler" hakkında kısa bir bölüm de içeren Çin'in 14. Beş Yıllık Planı kapsamında ise kuantum iletişim teknolojilerine ilişkin olarak "Şehir içi, şehirler arası ve uydu tabanlı kuantum iletişim teknolojilerini araştırıp geliştirme hedefi yinelenmiştir (CSET, 2021).

Kuantum güvenli kriptografi algoritmalarına ilişkin gerçekleştirilen çalışmalar incelendiğinde ise, Çin Kriptoloji Araştırma Derneği'nin (Chinese Association for Cryptologic Research-CACR) de NIST tarafından düzenlenen kuantum güvenli kriptografi yarışmasına benzer şekilde bir yarışma düzenlediği görülmektedir. Yalnızca Çinli araştırmacılara açık olduğu ve toplamda 36 başvurunun gerçekleştiği yarışmada; algoritmalara NIST yarışmasından farklı olarak 128 ve 256 bit güvenlik seviyesinde elektronik imza, açık anahtar şifreleme ve anahtar anlaşması protokolleri için kriptografik mekanizmalar uygulandığı (GSMA, 2023), üç birincilik ödülü verildiği ve CACR uzmanlarının kafes tabanlı algoritmaları tercih ettiği bilinmekle birlikte yarışma materyallerinin sadece küçük bir kısmının mevcut olması sebebiyle uluslararası topluluğun erişimini zorlaştırdığı bilinmekte ancak Çin'in küresel veri güvenliği endüstrisi üzerindeki etkisinin oldukça büyük olması nedeniyle kuantum sonrası gelişmelerini uluslararası düzeyde, örneğin ISO düzeyinde, standartlaştırmaya gönüllü olabileceği belirtilmektedir (QApp, 2023).

5.4. Japonya

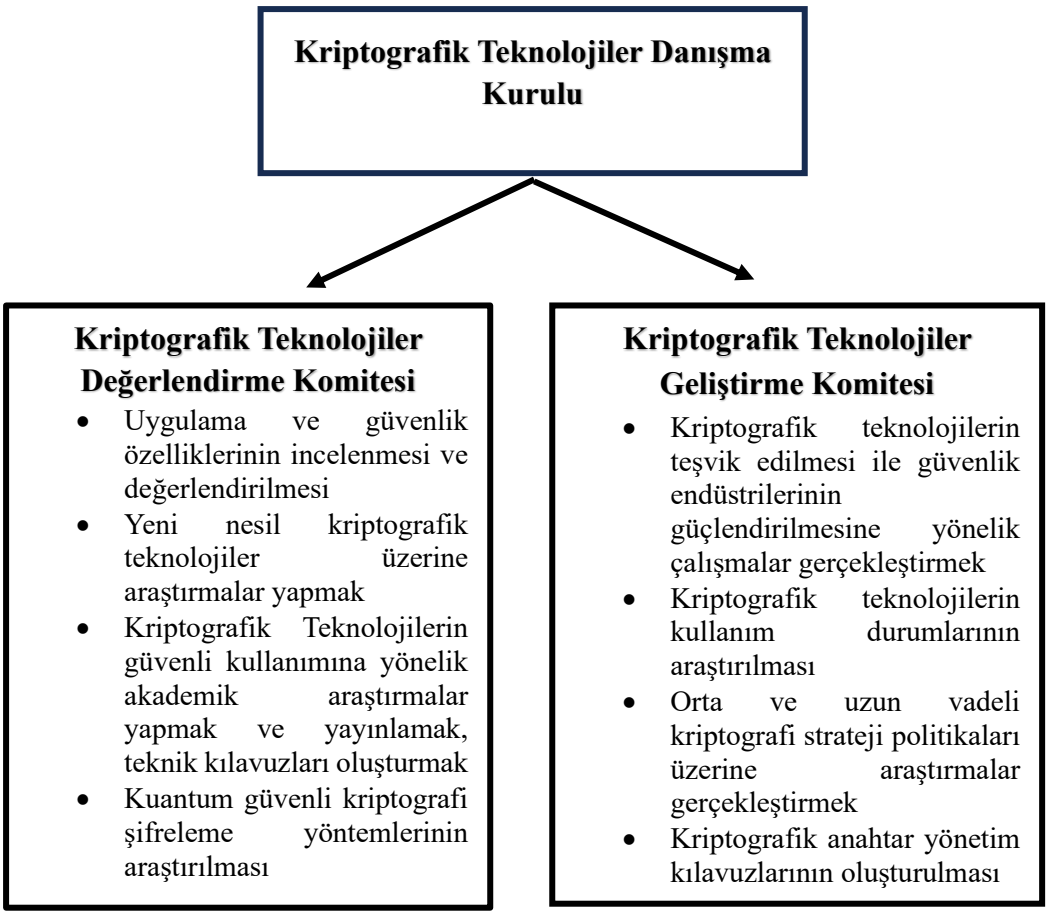
2010 yılında Tokyo'da video iletimi, gizli dinleme tespiti ve ikincil güvenli bağlantılara yeniden yönlendirme gibi işlemlerin gerçekleştirilebildiği kapsamlı bir kuantum ağı inşa edilmiş olmakla birlikte akıllı telefonlarda tek kullanımlık şerit şifrelemesi ile iletişimin sağlanması, depolanmış verilerin uzun vadeli bütünlüğünün sağlanabilmesi için imza ve kimlik doğrulama şemalarının kullanımı gibi uygulamalar

hayata geçirilmiştir. Söz konusu gelişimde özel sektörde yer alan öncü firmaların da payı olmakla birlikte temel destek Japon Ulusal Bilgi ve Teknolojisi Enstitüsü (National Institute of Information and Communications Technology-NICT) tarafından sağlanmıştır (Avrupa Komisyonu, 2022). Kuantum güvenli ağlar, kuantum anahtar dağıtımı ve kuantum güvenli kriptografi alanlarında ulusal ve ticari araştırma ve geliştirme çalışmalarına devam eden Japonya, 2020 yılında fiber ve uydu tabanlı iletişimi içeren 100 düğümlü küresel bir kuantum anahtar dağıtım ağı kurulmasına ilişkin projesini duyurmuştur (GSMA, 2023).

NICT'in de yönetiminde söz sahibi olduğu Kriptografi Araştırma ve Değerlendirme Komiteleri (Cryptography Research and Evaluation Committees-CRYPTREC) projesi ise e-Devlet altyapısında kullanılan kriptografik protokollerin güvenliğini değerlendirmek, izlemek, kriptografinin uygun uygulama ve işletim yöntemlerini araştırmak ve incelemek için 2000 yılında başlatılan bir projedir. Söz konusu proje başlangıçta, kamu kuruluşlarında kullanım için mükemmel güvenlik ve uygulanabilirliğe sahip olduğu değerlendirilen kriptografik tekniklerin bir listesini derlemeyi amaçlamış olup proje kapsamında bir şifreler listesi üretilmiş ve birçok özel şirket ile kamu kurumu tarafından kullanılmıştır (CRYPTREC, 2023). Yirmi yılı aşkın süreyle yürütülen proje kapsamına kuantum güvenli kriptografi ile kuantum anahtar dağıtımı da dahil edilmiş olup Şekil 5.2'de proje organizasyon yapısı ile konu ilişkili gerçekleştirilen çalışmaların genel yapısına yer verilmiştir.

Japonya ayrıca, kuantum güvenli kriptografik algoritmalara ilişkin NIST tarafından yürütülen standartlaştırma çalışmalarına dahil olmuş ve gelecekte kuantum güvenli algoritmaların benimsenmesini tavsiye etmiş, 2013 yılında yayımlanan ve e-Devlet sisteminde kullanılması tavsiye edilen şifreleme yöntemlerini kuantum güvenli algoritmaları içerecek şekilde güncellemiştir (CRYPTEC, 2023).

Şekil 5.2. CRYPTREC Organizasyon Yapısı



Kaynak: CRYPTEC, 2023

5.5. Hindistan

2020 yılında Hindistan Bilim ve Teknoloji Bakanlığı (Department of Science & Technology) tarafından uygulanmak üzere 5 yıllık bir süre için yaklaşık 1.1 milyar dolarlık bütçe ayrılan Kuantum Teknolojileri ve Uygulamaları Ulusal Misyonu (National Mission on Quantum Technologies & Applications - NM-QTA) duyurularak kuantum teknolojileri alanında gelişmekte olan teorik yapılardan pek çok ticari uygulamanın ortaya çıkmasının beklendiği belirtilmiş ve bu doğrultuda kuantum hesaplama, kuantum anahtar dağıtımı, şifreleme, kripto cihazları ve kuantum analizi ile ilişkili teknolojilerin destekleneceği, geliştirileceği ve aynı zamanda yeni nesil vasıflı insan gücünün hazırlanmasının sağlanarak girişimciliğin ve yeni kurulan ekosistemin gelişiminin teşvik edilmesinin hedeflendiği ifade edilmiştir (DST, 2020).

Hindistan Uzay Araştırma Enstitüsü (Indian Space Research Organisation- ISRO) 2021 yılında hazırla ve ölç yaklaşımına dayalı uydu tabanlı kuantum anahtar dağıtım yöntemini 300 metrelik bir mesafede başarıyla uygulayarak geleceğe dönük veri güvenliği için kuantum iletişimine yönelik hazırlıkların devam ettiğini ifade etmiştir (ISRO, 2023).

Hindistan Telekomünikasyon Bakanlığı'na bağlı telekom araştırma ve geliştirme kuruluşu olan Telematik Geliştirme Merkezi (Centre for Development of Telematics - C-DOT), NM-QTA'nın kuantum iletişim alanındaki faaliyetlerine katkıda bulunarak mevcut iletişim ağları aracılığıyla çeşitli kritik sektörler tarafından taşınan verilerin güvenliğine yönelik oluşturduğu tehdidi bertaraf edebilmek amacıyla fiber optik kablolar aracılığıyla 100 kilometreden fazla bir mesafede özgün olarak tasarlanan yerli kuantum anahtar dağıtımı yöntemini geliştirdiğini duyurmuştur (C-DOT, 2021).

Hindistan ordusu ise Singapur Ulusal Güvenlik Konseyi Sekreterliği (National Security Council Secretariat) desteğiyle bir kuantum laboratuvarı kurulduğunu duyurarak yürütülen araştırmalar ile kuantum iletişim gibi yeni nesil iletişim yöntemlerinin hayata geçirilmesinin ve Hint Silahlı Kuvvetlerindeki mevcut kriptografik altyapının kuantum güvenli kriptografiye dönüştürülmesinin hedeflendiğini ifade etmiştir (MoD, 2021).

5.6. Ülkemiz Düzenlemeleri ve Uygulamaları

Ülkemiz bilgi güvenliği alanında önemli düzenlemelere, strateji belgelerine ve dokümanlara sahiptir. Bu bölümde ülkemizde kriptografi ile ilişkili olarak bilgi güvenliği sağlayan düzenlemeler ele alınmış ve TÜBİTAK ile Aselsan tarafından gerçekleştirilen çalışmalara yer verilmiştir.

5.6.1. TÜBİTAK

TÜBİTAK, toplumun yaşam kalitesinin artması ve ülkemizin sürdürülebilir gelişmesini sağlamak amacıyla akademik ve endüstriyel araştırma geliştirme çalışmalarının ve yeniliklerin desteklenmesi, ulusal öncelikler doğrultusunda

Araştırma-Teknoloji-Geliştirme çalışması yürüten Ar-Ge enstitülerinin işletimi, ülkemizin bilim ve teknoloji politikalarının belirlenmesi ve toplumun her kesiminde söz konusu hususlara yönelik farkındalığı artırmak üzere kitaplar ve dergiler yayımlanması faaliyetlerini yürüten Sanayi ve Teknoloji Bakanlığına bağlı kuruluştur (TÜBİTAK, Biz Kimiz?, 2023).

Temelleri 1972 yılında atılmış olan Ulusal Elektronik ve Kriptoloji Araştırma Enstitüsü (UEKAE) ise TÜBİTAK Bilişim ve Bilgi Güvenliği İleri Teknolojiler Araştırma Merkezi (BİLGEM) bünyesinde faaliyet gösteren ve laboratuvarlarında hem sivil hem de askeri ihtiyaçlara hitap eden farklı alanlardaki kritik teknolojik cihazların ve sistemlerin üretimini gerçekleştiren bir Ar-Ge kuruluşudur (UEKAE, Biz Kimiz?, 2023). Bununla birlikte, 5201 sayılı Kanun gereği oluşturulan "Kontrole Tâbi Tutulacak Harp Araç Ve Gereçleri İle Silah, Mühimmat Ve Bunlara Ait Yedek Parçalar, Askerî Patlayıcı Maddeler, Bunlara Ait Teknolojilere İlişkin Listesi"nin 1 inci maddesinin "Askeri komuta kontrol, muhabere ve bilgi sistemleri" başlıklı (g) bendinde yer alan:

> *"2) Askerî amaçlı ve/veya emniyetli (kriptolu) telli ve telsiz muhabere sistem cihazları ile içerisinde yazılım bulunduran koruma ve yönetim devresini haiz bataryaları (Bu cihazlara ait kulaklık, mikrofon takımları, aksesuarlar ve piller hariç).*
>
> *3) Askerî amaçlı veya ulusal güvenlik amaçlı üretimi yapılan ve kullanılan her türlü kripto ve ses emniyet cihazları ile bu cihazlar için özel olarak tasarlanmış kriptografik amaçlı yazılım ve donanımlar."*

cinsi cihazların üretiminin ve ihracat ile ithalatına ilişkin izin işlemlerinin gerçekleştirilmesinin Milli Savunma Bakanlığı'nın sorumluluğunda ve bilgisi dahilinde yapılacağı düzenlenmiştir. Bu doğrultuda TÜBİTAK, Milli Savunma Bakanlığından temin ettiği üretim izin belgesi ile birlikte bünyesinde milli kripto cihaz ve sistemlerinin üretimini de gerçekleştirmektedir.

TÜBİTAK BİLGEM UEKAE bünyesinde kuantum kriptografi ve kuantum anahtar dağıtımı konularını da içeren ulusal ve uluslararası ölçekli çeşitli projeler yürütüldüğü, 2023 yılında "Kuantum Teknolojileri Bölümü" adında yeni bir birim kurulduğu ve kuantum teknolojileri alanında çağın gereksinimlerinin yakalanarak altyapı ve yetişmiş insan gücü birikiminin oluşturulmasının, Ar-Ge projelerinin yürütülmesinin,

hem sivil hem de askeri uygulamalar için kuantum teknolojileri tabanlı sistemler geliştirilmesinin hedeflendiği belirtilerek kuantum hesaplama, kuantum haberleşme, kuantum görüntüleme, kuantum algılama ve metroloji gibi başlıca alanlarda gerçekleştirilecek faaliyetler ve geliştirilecek sistemler ile ülkemizin kuantum teknolojilerinde söz sahibi olmasına ve ilerlemesine önemli seviyede katkı sağlanmasının beklendiği ifade edilmektedir (UEKAE, 2023).

UEKAE tarafından 2022 yılında paylaşılan bir duyuru ile; kuantum bilgisayarların kriptografik algoritmalar üzerindeki etkisinin incelendiği ve on yıl içerisinde geliştirilmesi muhtemel bazı kuantum bilgisayarların anahtar paylaşımı ve elektronik imza amacıyla kullanılan birçok asimetrik algoritma ile yeterli büyüklükte parametrelerin kullanılmadığı simetrik algoritmalar için tehlike oluşturacağının gözlemlendiği belirtilerek özellikle kritik bilgi işleyen ülkemiz kurumlarının 15 yıl ve üzeri süre boyunca gizli kalması istenen verilerinin güvenliğinin sağlanabilmesi amacıyla önlem alması gerektiği ifade edilmiştir. Bu kapsamda, kuantum anahtar dağıtımı yönteminin teorik olgunluk, güvenlik, etkinlik ve maliyet gibi faktörler altında incelenmiş olduğu ve kullanımının tavsiye edilmediği, kuantum güvenli kriptografik algoritmaların da incelenerek önümüzdeki 5 yıl içerisinde;

- Simetrik şifreleme için kullanılacak algoritmalardan anahtar boyu 256-bit olanların tercih edilmesinin tavsiye edildiği,
- Asimetrik algoritmalar kullanıldığında, önceden paylaşılmış simetrik anahtar veya kuantum hesaplamaya dayanıklı algoritma kullanma yöntemlerinden en az birinin klasik asimetrik algoritmalar ile beraber (hibrit olarak) kullanılmasının tavsiye edildiği,
- Kuantum hesaplamaya dayanıklı algoritmaların tercih edilmesi durumunda; teorik olgunluk, güvenlik, etkinlik, maliyet ve basitlik gibi kıstaslar dikkate alınarak literatürde belirli bir olgunluğa erişmiş olan Crystals-Kyber, FrodoKEM, Crystals-Dilithium ve Sphincs+ gibi yöntemlerin veya millî yöntemlerin tavsiye edildiği,

ifade edilmiştir (TÜBİTAK BİLGEM, 2022).

Bununla birlikte, 2001 yılında TÜBİTAK BİLGEM UEKAE bünyesinde kurulan laboratuvar birimi Milli Açık Anahtar Altyapısı (MA3) ile açık anahtar altyapısı

teknolojisinin tamamen yerli ve milli bir perspektifle geliştirilerek kamu ve özel kurumların kullanımına sunulmasının ve bu sayede ülkemizin dijital güvenliğinin sağlanmasının hedeflendiği, bu kapsamda oluşturulan Elektronik Sertifika Yönetim Altyapısının askeri ve kamu kurumları ile elektronik sertifika hizmet sağlayıcılarında kullanıldığı (M3 LAB, 2023), TÜBİTAK-BİLGEM Test ve Değerlendirme Başkan Yardımcılığı bünyesinde oluşturulan Kripto Analiz Laboratuvarı ile 1995 yılından bu yana askeri, kamu ve özel kurum/kuruluşlara yönelik bilgi güvenliği çözümlerinin kriptografik açıdan yeterli güvenlik seviyesinde olup olmadıklarına yönelik analiz ve değerlendirme çalışmalarının yapıldığı, bu kapsamda hem açık literatürde yer alan kripto analiz metotlarına hem de özgün olarak geliştirilmiş saldırı yöntemlerine karşı kripto algoritmasının ve mimarisinin dayanıklılığının ölçüldüğü bilinmektedir (TÜBİTAK, 2023).

5.6.2. ASELSAN

Türk Silahlı Kuvvetleri'nin haberleşme ihtiyaçlarının milli imkanlarla karşılanması amacıyla 1975 yılında kurulmuş olan ASELSAN, Türk Silahlı Kuvvetlerini Güçlendirme Vakfı'na bağlı anonim bir şirkettir. Başta Türk Silahlı Kuvvetleri olmak üzere yurt içi ve yurt dışı ihtiyaç makamlarının, haberleşme ve bilgi teknolojileri, radar ve elektronik harp, elektro-optik, aviyonik, insansız sistemler, kara, deniz ve silah sistemleri, hava savunma ve füze sistemleri, komuta kontrol sistemleri, ulaştırma, güvenlik, trafik, otomasyon ve sağlık teknolojilerine yönelik ihtiyaçlarını karşılayabilecek çok geniş bir ürün yelpazesine sahip olan ASELSAN çeşitli Ar-Ge faaliyetlerini de gerçekleştirmektedir (ASELSAN, Hakkımızda, 2023).

Bilgi güvenliği, anahtar yönetim sistemleri ve kripto cihazlarına ilişkin çeşitli çalışmalar gerçekleştiren ASELSAN, asimetrik algoritma kullanımı kaynaklı kuantum ataklarına karşı zafiyet içeren 5G ağ mimarisine destek vererek dayanıklı bir mimari oluşturulmasının sağlanacağını ve kuantum güvenli algoritmalardaki test ihtiyaçlarının etkin bir şekilde yürütüleceğini (ASELSAN, 2022), aviyonik platformlarda siber güvenlik çalışmaları kapsamında kuantum ataklara karşı dayanıklı güvenli kimlik doğrulama, anahtar değişimi ve imzalama protokol geliştirilmesinin amaçlandığını (ASELSAN, 2023) ve TOBB Ekonomi ve Teknoloji Üniversitesi yerleşkesinde kurulan Kuantum Araştırma Laboratuvarında (KUANTAL) yürütülecek projeler ile

ülkemizin kuantum teknolojiler alanındaki bilgi birikimi ve teknolojik hazırlık seviyesinin artırılarak yerli ve milli sistemlerin üretiminin hedeflendiği, bu doğrultuda akademik iş birlikleriyle araştırma ve prototip geliştirme faaliyetlerinin gerçekleştirilmesinin planlandığı ifade edilmektedir (ASELSAN, 2023).

Bununla birlikte, Aselsan'ın TÜBİTAK BİLGEM ile birlikte kuantum güvenli kriptografi alanında ortak çalışmalar yürüttüğü, bu kapsamda 2019 yılında "Kuantum Sonrası Kriptografi Çalıştayı" düzenlendiği ve 29 Şubat-1 Mart 2020 tarihleri arasında gerçekleşen ASELSAN-TÜBİTAK BİLGEM İş Birliği Çalıştayında alınan kararlar doğrultusunda projelendirilmesi muhtemel Milli Savunma Bakanlığı ve Savunma Sanayii Başkanlığı projelerinde ortak çalışma kararı alındığı bilinmekte, klasik kriptografi ile kuantum güvenli kriptografi çözümlerinin birlikte kullanılarak ASELSAN tarafından tasarlanan güvenli ağ mimarisi çözümlerinde kullanılacak kripto cihazlarında uygulanması beklenmektedir (İlter & Çetin, 2020).

5.6.3. Ülkemizdeki Yasal Düzenlemeler

Bu başlıkta kriptografiye dayalı bilgi güvenliği ile ilgili olduğu değerlendirilen ülkemiz yasal düzenlemeleri ele alınmıştır.

5.6.3.1. Elektronik Haberleşme Kanunu

05.11.2008 tarihli ve 5809 sayılı Elektronik Haberleşme Kanunu'nun (EHK) "İlkeler" başlıklı 4 üncü maddesinin birinci fıkrasında yer alan *"(h) Millî güvenlik ile kamu düzeni gereklerine ve acil durum ihtiyaçlarına öncelik verilmesi"* hükmü ile *"(l) Bilgi güvenliği ve haberleşme gizliliğinin gözetilmesi"* hükmü uyarınca ilgili merciler tarafından elektronik haberleşme hizmetinin sunulmasında ve bu hususta yapılacak düzenlemelerde milli güvenlik ihtiyaçlarına öncelik verileceği ile bilgi güvenliği ve haberleşme gizliliğinin gözetileceği belirtilmiş, mezkur Kanunun "Bakanlığın görev ve yetkileri" başlıklı 5 inci maddesinin birinci fıkrasında yer alan; *"(c) Elektronik haberleşme alt yapı, şebeke ve hizmetlerinin; teknik, ekonomik ve sosyal ihtiyaçlara, kamu yararına ve millî güvenlik amaçlarına uygun olarak kurulması, geliştirilmesi ve*

birbirlerini tamamlayıcı şekilde yürütülmesini sağlamaya yönelik politikaları belirlemek." hükmü ve *"(h) Ulusal siber güvenliğin sağlanması amacıyla politika, strateji ve hedefleri belirlemek, kamu kurum ve kuruluşları ile gerçek ve tüzel kişilere yönelik siber güvenliğin sağlanmasına ilişkin usul ve esasları belirlemek, eylem planlarını hazırlamak, ilgili faaliyetlerin koordinasyonunu sağlamak, kritik altyapılar ile ait oldukları kurumları ve konumları belirlemek, gerekli müdahale merkezlerini kurmak, kurdurmak ve denetlemek, her türlü siber müdahale aracının ve millî çözümlerin üretilmesi ve geliştirilmesi amacı ile çalışmalar yapmak, yaptırmak ve bunları teşvik etmek ve siber güvenlik konusunda bilinçlendirme, eğitim ve farkındalığı artırma çalışmaları yürütmek, siber güvenlik alanında faaliyet gösteren gerçek ve tüzel kişilerin uyması gereken usul ve esasları hazırlamak."* hükmü ile Ulaştırma ve Altyapı Bakanlığına siber güvenliğin sağlanmasında politika ve stratejileri belirleme ile siber güvenlik alanında gerçek ve tüzel kişilerin uyması gereken usul ve esasları hazırlama görevleri verilmiş, elektronik haberleşme alt yapı ve şebekelerinin milli güvenlik hedeflerine uygun olarak kurulması ve geliştirilmesine yönelik politikaların belirlenmesi gerektiği hükme bağlanmıştır.

EHK'nin "Kurumun görev ve yetkileri" başlıklı 6 ncı maddesinin birinci fıkrasında yer alan; *"(c) Abone, kullanıcı, tüketici ve son kullanıcıların hakları ile kişisel bilgilerin işlenmesi ve gizliliğinin korunmasına ilişkin gerekli düzenlemeleri ve denetlemeleri yapmak"* hükmü ile son kullanıcı verilerinin gizliliğinin korunmasına ilişkin gerekli düzenlemelerin yapılması, *"(e) Elektronik haberleşme sektöründeki gelişmeleri takip etmek, sektörün gelişimini teşvik etmek amacıyla gerekli araştırmaları yapmak veya yaptırmak ve bu konularda ilgili kurum ve kuruluşlarla işbirliği halinde çalışmak"* hükmü ile elektronik haberleşme sektöründeki gelişmelerin takibinin yapılması ve gelişiminin teşvik edilmesi, konuya ilişkin ilgili kurum ve kuruluşlarla işbirliği halinde çalışılması, *"(p) Elektronik haberleşme sektörü ile ilgili uluslararası birlik ve kuruluşların çalışmalarına katılmak, kararların uygulanmasını takip etmek ve gerekli koordinasyonu sağlamak"* hükmü ile sektörle ilişkili uluslararası kuruluşlar tarafından alınan kararların uygulanmasının takibinin gerçekleştirilmesi, *"(ş) Elektronik haberleşme sektörüne yönelik olarak, millî güvenlik, kamu düzeni veya kamu hizmetinin gereği gibi yürütülmesi amacıyla mevzuatın öngördüğü tedbirleri almak"* hükmü ile milli güvenlik hedefleri doğrultusunda gerekli tedbirlerin alınması görevleri Bilgi Teknolojileri ve İletişim Kurumu'na (BTK) verilmiş,

aynı maddenin (v) bendinde yer alan *"Siber güvenlik ve internet alan adları konularında Cumhurbaşkanı, Bakanlık ve/veya Siber Güvenlik Kurulu tarafından verilen görevleri Telekomünikasyon İletişim Başkanlığı veya diğer birimleri marifetiyle yerine getirmek"* hükmü ile anılan Kanun'un "Kurumun yetkisi ve idari yaptırımlar" başlıklı 60'ıncı maddesinde yer alan *"Kurum, kamu kurum ve kuruluşları ile gerçek ve tüzel kişilerin siber saldırılara karşı korunması ve bu saldırılara karşı caydırıcılık sağlamak için her türlü tedbiri alır veya aldırır."* hükmü uyarınca BTK'ye siber güvenlik alanında geniş bir yetki tanınmıştır.

EHK'nin "Kodlu ve kriptolu haberleşme" başlıklı 39 uncu maddesinin birinci fıkrasında yer alan *"Telsiz haberleşme sistemleri üzerinden kriptolu haberleşme yapmaya Türk Silahlı Kuvvetleri, Jandarma Genel Komutanlığı ve Sahil Güvenlik Komutanlığı, Milli İstihbarat Teşkilatı, Emniyet Genel Müdürlüğü ve Dışişleri Bakanlığı yetkilidir. Ayrıca yukarıda belirtilen kurumlara ait olanlar dışında kamu kurum ve kuruluşları ile gerçek ve tüzel kişilerin elektronik haberleşme hizmeti içinde kodlu veya kriptolu haberleşme yapma usul ve esasları Kurum tarafından belirlenir."* hükmü ile kodlu veya kriptolu haberleşme usul ve esaslarının BTK tarafından belirleneceği düzenlenmiştir.

5.6.3.2. Elektronik İmza Kanunu

Elektronik imzanın hukuki ve teknik yönleri ile kullanımına ilişkin esasları düzenlemek amacıyla 5070 sayılı Elektronik İmza Kanunu hazırlanmış ve 15.01.2004 tarihinde yürürlüğe girmiştir. Kanunda elektronik imzanın hukuki yapısı, elektronik sertifika hizmet sağlayıcılarının faaliyetleri ve her alanda elektronik imzanın kullanımına ilişkin hususlar belirlenmekle birlikte elektronik imzaya ilişkin ikincil düzenlemelerin hazırlanması, elektronik sertifika hizmet sağlayıcılarının yapacakları bildirimin değerlendirilmesi ve elektronik imza uygulamaları çerçevesinde elektronik sertifika hizmet sağlayıcıları denetlenmesi konularında BTK sorumlu ve yetkili kılınmıştır.

Elektronik İmza Kanunu'nun "Tanımlar" başlıklı 3 üncü maddesinin (b) bendinde elektronik imzanın; *"Başka bir elektronik veriye eklenen veya elektronik veriyle mantıksal bağlantısı bulunan ve kimlik doğrulama amacıyla kullanılan elektronik veriyi"*, (d) bendinde imza oluşturma verisinin; *"İmza sahibine ait olan, imza sahibi*

tarafından elektronik imza oluşturma amacıyla kullanılan ve bir eşi daha olmayan şifreler, kriptografik gizli anahtarlar gibi verileri", (f) bendinde imza doğrulama verisinin *"Elektronik imzayı doğrulamak için kullanılan şifreler, kriptografik açık anahtarlar gibi verileri"* ifade ettiği belirtilerek "Güvenli elektronik imza" başlıklı 4 üncü maddesi ile güvenli elektronik imza; *"münhasıran imza sahibine bağlı olan, sadece imza sahibinin tasarrufunda bulunan güvenli elektronik imza oluşturma aracı ile oluşturulan, nitelikli elektronik sertifikaya dayanarak imza sahibinin kimliğinin ve imzalanmış elektronik veride sonradan herhangi bir değişiklik yapılıp yapılmadığının tespitini sağlayan elektronik imza"* olarak tanımlanmıştır.

Mezkur Kanun'un "Güvenli elektronik imza oluşturma araçları" başlıklı 6 ncı maddesi ile güvenli elektronik imza oluşturma araçları; *"ürettiği elektronik imza oluşturma verilerinin kendi aralarında bir eşi daha bulunmamasını, üzerinde kayıtlı olan elektronik imza oluşturma verilerinin araç dışına hiçbir biçimde çıkarılamamasını ve gizliliğini, üzerinde kayıtlı olan elektronik imza oluşturma verilerinin, üçüncü kişilerce elde edilememesini, kullanılamamasını ve elektronik imzanın sahteciliğe karşı korunmasını, imzalanacak verinin imza sahibi dışında değiştirilememesini ve bu verinin imza sahibi tarafından imzanın oluşturulmasından önce görülebilmesini sağlayan imza oluşturma araçları"* olarak tanımlanmış olup elektronik imza oluşturma araçlarının güvenli sayılabilmesi için elektronik imza oluşturma verilerinin araç dışına hiç bir şekilde çıkarılamaması, gizliliğinin sağlanması, üçüncü kişilerce elde edilememesi gerektiği hükme bağlanmıştır.

Elektronik İmza Kanunu'nda ayrıca "Elektronik sertifika hizmet sağlayıcısının yükümlülükleri" başlıklı 10 uncu maddesinde yer alan *"(d) İmza oluşturma verisinin sertifika hizmet sağlayıcısı tarafından veya sertifika talep eden kişi tarafından sertifika hizmet sağlayıcısına ait yerlerde üretilmesi durumunda bu işlemin gizliliğini sağlamak veya sertifika hizmet sağlayıcısının sağladığı araçlarla üretilmesi durumunda, bu işleyişin güvenliğini sağlamakla yükümlüdür"* hükmü ile elektronik imza oluşturma veri güvenliğinin sağlanması hususunda elektronik sertifika hizmet sağlayıcıları sorumlu kılınmış ve "Denetim" başlıklı 15 inci maddesinde yer alan *"Elektronik sertifika hizmet sağlayıcılarının bu Kanunun uygulanmasına ilişkin faaliyet ve işlemlerinin denetimi Kurumca yerine getirilir."* hükmü ile elektronik sertifika hizmet sağlayıcılarını denetleme yetkisi BTK'ye verilmiştir.

Elektronik imza ile ilişkili hükümlerin yanı sıra elektronik mühür ve internet sitesi kimlik doğrulama sertifikaları ile ilgili hükümlere de Elektronik İmza Kanunu'nda yer verilmiş olup elektronik imzaya ilişkin hükümlerin elektronik mühür, internet sitesi kimlik doğrulama sertifikası ve benzer altyapıyı kullanan diğer elektronik sertifikalar hakkında da uygulanacağı ifade edilmiştir.

5.6.4. İkincil Düzenlemeler

Bu başlıkta kriptografiye dayalı bilgi güvenliği ile ilgili olduğu değerlendirilen ikincil düzenlemeler incelenmiştir.

5.6.4.1. Elektronik İmza Kanununun Uygulanmasına İlişkin Usul ve Esaslar Hakkında Yönetmelik

Elektronik İmza Kanununun Uygulanmasına İlişkin Usul ve Esaslar Hakkında Yönetmelik 06.01.2005 tarihli ve 25692 sayılı Resmi Gazete'de yayımlanarak yürürlüğe girmiş olup elektronik imzanın hukuki ve teknik yönleri ile uygulanmasına ilişkin olarak;

- Kamu kurum ve kuruluşları ile gerçek veya özel hukuk tüzel kişilerinin elektronik sertifika hizmet sağlayıcısı olma talebine ilişkin bildirim ve sertifikasyon sürecine,
- Elektronik sertifika sağlayıcılarının, nitelikli elektronik sertifika sahibinin, üçüncü kişilerin ve BTK'nin yükümlülüklerine,
- Güvenli sistem ve cihazlar kullanmakla yükümlü kılınan elektronik sertifika hizmet sağlayıcılarının teknik hususlar ve güvenlik ile ilişkili sorumluluklarına,
- Elektronik sertifika hizmet sağlayıcılarının uymakla yükümlü olduğu mali hususlara,
- Denetim sonucu ile BTK tarafından ya da elektronik sertifika hizmet sağlayıcısının talebi üzerine faaliyetin sona ermesi durumunda gerçekleştirilmesi gereken iş ve işlemlere,

yönelik usul ve esaslar belirlenmiş, elektronik sertifika hizmet sağlayıcılarının imza oluşturma ve doğrulama verilerine ilişkin uyulması gereken teknik kriterlerin tebliğ ile belirlendiği ifade edilmiştir.

5.6.4.2. Elektronik İmza ile İlgili Süreçlere ve Teknik Kriterlere İlişkin Tebliğ

06.01.2005 tarihli ve 25692 sayılı Resmi Gazete'de yayımlanarak yürürlüğe giren Elektronik İmza ile İlgili Süreçlere ve Teknik Kriterlere İlişkin Tebliğ ile elektronik imzaya ilişkin süreçler ve teknik kriterler detaylı olarak belirlenmiştir. Bu doğrultuda, Tebliğ'in "Teknik Hususlar" kenar başlıklı ikinci bölümünün "Algoritmalar ve Parametreler" başlıklı 6 ncı maddesi;

"(Değişik cümle: RG-13/7/2017-30123) İmza oluşturma ve doğrulama verileri ile özetleme algoritmalarının, ETSI TS 119 312 standardına ve aşağıda yer alan şartlara uygun olması gerekir.

a) İmza sahibinin imza oluşturma ve doğrulama verileri:

i. RSA için en az 2048 bit veya

ii. DSA için en az 3072 bit veya

iii. DSA Eliptik Eğrisi için en az 256 bit

b) ESHS'nin imza oluşturma ve doğrulama verileri:

i. (Değişik: RG-24/3/2020-31078) İmzalamalarda RSA-PSS kullanılmak şartıyla RSA için en az 4096 bit veya

ii. DSA için en az 3072 bit veya

iii. DSA Eliptik Eğrisi için en az 256 bit

c) (Değişik: RG-24/3/2020-31078) Özetleme algoritması:

i. SHA2-256 veya

ii. SHA2-384 veya

iii. SHA2-512 veya

iv. SHA3-256 veya

v. SHA3-384 veya

vi. SHA3-512

(Değişik fıkra: RG-28/12/2022-32057) Birinci fıkrada belirtilen algoritmalar ve parametreler 31/12/2025 tarihine kadar geçerlidir."

hükmünü amirdir.

5.6.4.3. Kayıtlı Elektronik Posta Sistemine İlişkin Usul ve Esaslar Hakkında Yönetmelik

25.08.2011 tarihli ve 28036 sayılı Resmi Gazete'de yayımlanarak yürürlüğe giren Kayıtlı Elektronik Posta Sistemine İlişkin Usul ve Esaslar Hakkında Yönetmelik ile kayıtlı elektronik posta sistemine, bu sistemle yapılacak işlemler ile bu işlemlerin sonuçlarına, kayıtlı elektronik posta adresine sahip gerçek ve tüzel kişilere, kayıtlı elektronik posta hizmet sağlayıcılarının hak ve yükümlülüklerine, yetkilendirilmelerine ve denetimlerine ilişkin usul ve esaslar düzenlenmiştir.

Yönetmelik'in "Teknik Hususlar ve Güvenlik" kenar başlıklı yedinci bölümünün "Güvenlik kriterleri" başlıklı 23 üncü maddesinin dördüncü fıkrası *"KEPHS; güvenli sistem ve cihazlar kullanır, bu sistem ve cihazlar ile bunların bulunduğu bina veya alanın korunmasını sağlar."* şeklinde düzenlenerek kayıtlı elektronik posta hizmet sağlayıcıları güvenli sistem ve cihaz kullanımı ile sorumlu tutulmuş, kullanılan sistem ve cihaz güvenliği kriterlerinin ise; "Teknik hususlara ilişkin tebliğ" başlıklı 25 inci maddesinin birinci fıkrasında yer alan *"KEP sisteminin tüm süreçlerine ve işleyişine, KEPHS'nin faaliyetleri için kullandığı sistemlere ve cihazlara, fizikî güvenliğe ve personeline ilişkin uyulması gereken teknik kriterler Tebliğ ile belirlenir."* hükmü ile tebliğde belirtileceği ifade edilmiştir.

5.6.4.4. Kayıtlı Elektronik Posta Sistemi ile İlgili Süreçlere ve Teknik Kriterlere İlişkin Tebliğ

25.08.2011 tarihli ve 28036 sayılı Resmi Gazete'de yayımlanarak yürürlüğe giren Kayıtlı Elektronik Posta Sistemi ile İlgili Süreçlere ve Teknik Kriterlere İlişkin Tebliğ ile kayıtlı elektronik posta hizmet sağlayıcılarının işleyişine, faaliyetleri için kullandığı sistem, cihaz ile fiziki güvenliğine, personeline ve hizmetlerine ilişkin teknik hususlar belirlenmiştir.

Tebliğ'in "Algoritma ve parametreler" başlıklı 6 ncı maddesi *"KEPHS, elektronik imza, işlem sertifikası ve özetleme algoritmalarına ilişkin olarak 6/1/2005 tarih ve 25692 sayılı Resmî Gazete'de yayımlanan "Elektronik İmza ile İlgili Süreçlere ve Teknik Kriterlere İlişkin Tebliğ"in 6 ncı maddesinin (b) ve (c) bendinde yer alan şartlara uyar."* şeklinde düzenlenerek elektronik sertifika hizmet sağlayıcılarının da uymakla yükümlü kılındığı güvenlik seviyesindeki asimetrik anahtarlı algoritmalar ile özetleme algoritmalarına atıfta bulunulmuştur.

5.6.4.5. Elektronik Haberleşme Sektöründe Şebeke ve Bilgi Güvenliği Yönetmeliği

Elektronik Haberleşme Sektöründe Şebeke ve Bilgi Güvenliği Yönetmeliği 13.07.2014 tarihli ve 29059 sayılı Resmî Gazete'de yayımlanarak yürürlüğe girmiştir. Yönetmelik ile şebeke ve bilgi güvenliğinin sağlanmasına yönelik olarak işletmecilerin uymaları gereken usul ve esaslar belirlenmiştir.

Yönetmelik'in "İlkeler" başlıklı 4 üncü maddesinde *"(a) İşletmecilerin yükümlülüklerinin belirlenmesinde, şebeke ve bilgi güvenliğinin sağlanmasına yönelik tedbirlerin tespitinde ve uygulanmasında mümkün olduğu ölçüde risk temelli değerlendirmelerin yapılması"* ile *"(ç) Ulusal düzenleme ile ulusal ve/veya uluslararası standartların dikkate alınması"* ilkelerinin gözetileceği ifade edilerek "Şebeke güvenliği" başlıklı 21 inci maddesinde yer alan *"(1) İşletmeciler, şebekelerinin tehditlerden korunması ve şebekeleri kullanan sistem ve uygulamaların güvenliğinin sağlanması amacıyla gerekli önlemleri alır."* hükmü ile işletmecilerin şebekelerinde gerekli önlemleri almaları yükümlülüğü getirilmiştir.

5.6.4.6. Kamu Kurum ve Kuruluşları ile Gerçek ve Tüzel Kişilerin Elektronik Haberleşme Hizmeti İçinde Kodlu veya Kriptolu Haberleşme Yapma Usul ve Esasları Hakkında Yönetmelik

23.10.2010 tarihli ve 27738 sayılı Resmi Gazete'de yayımlanarak yürürlüğe giren Kamu Kurum ve Kuruluşları ile Gerçek ve Tüzel Kişilerin Elektronik Haberleşme Hizmeti İçinde Kodlu veya Kriptolu Haberleşme Yapma Usul ve Esasları Hakkında

Yönetmelik ile 05.11.2008 tarihli ve 5809 sayılı Elektronik Haberleşme Kanununa göre kamu kurum ve kuruluşları ile gerçek ve tüzel kişilerin elektronik haberleşme hizmeti içinde kodlu veya kriptolu haberleşme sistemi üretimi, başvuru esasları, değerlendirilmesi, izin işlemleri, emniyet ve muhafaza tedbirleri, denetim, müeyyide ve kayıtlarının tutulmasında uygulanacak usul ve esaslar ile yapılacak iş ve işlemler belirlenmiştir. Anılan Yönetmeliğin "Değerlendirme" başlıklı 6 ncı maddesinin üçüncü ve dördüncü fıkraları;

> *"(3) Kamu kurum veya kuruluşları ile gerçek ve tüzel kişilerin yurtdışından yolcu beraberinde veya kesin dönüşte getirilen veya bireysel olarak ithal edilen veya posta ile gelen kodlu veya kriptolu haberleşme cihaz/sistemlerine, bu cihaz/sistemlere ait kod veya kripto anahtarlarının Kuruma teslim edilmesi halinde, kullanma ve kurma izni verilebilir. Kurumdan izin alınmadan yapıldığı tespit edilen kodlu veya kriptolu haberleşmeler iletişime kapatılır ve ilgililer hakkında suç duyurusunda bulunulur.*
>
> *(4) Üretici tarafından yapılacak başvurularda ilgili mevzuata uygun görülmeyen kodlu veya kriptolu cihaz/sistem başvuruları reddedilir."*

şeklinde düzenlenerek kodlu veya kriptolu elektronik haberleşme hizmetinden yararlanmak isteyen gerçek ya da tüzel kişilerin, bireysel olarak beraberinde getirdikleri ya da imalat yoluyla piyasaya arz ettikleri cihazlara ait kod veya kripto anahtarlarını BTK'ye teslim etmesi gerektiği; aksi takdirde BTK tarafından izin alınmadan gerçekleştirilen kodlu veya kriptolu haberleşmelerin iletişime kapatılarak ilgililer hakkında suç duyurusunda bulunulacağı hüküm altına alınmıştır.

5.6.4.7. Gizlilik Dereceli Belgelerde Uygulanacak Usul ve Esaslar Hakkında Yönetmelik

26.04.2022 tarihli ve 31821 sayılı Resmi Gazete'de yayımlanarak yürürlüğe giren Gizlilik Dereceli Belgelerde Uygulanacak Usul ve Esaslar Hakkında Yönetmelik ile kamu kurum ve kuruluşlarında muhteviyatına veya güncelliğine göre gizlilik dereceli belgeler için uygulanacak usul ve esasların belirlenmesi ve gizlilik dereceli belgelerde uygulama birliğinin sağlanması amaçlanmıştır.

Yönetmelik'in "Gizlilik derecelerinin tanımları" başlıklı 4 üncü maddesinde çok gizli, gizli ve hizmete özel olmak üzere üç farklı gizlilik derecesi tanımına yer verilmiş olup Çok Gizli ve Gizli gizlilik derecesine sahip olan belgelerin zorunlu hal kapsamında fiziksel ortamda; Hizmete Özel gizlilik derecesine sahip belgelerin ise elektronik ortamda üretileceği belirtilerek söz konusu belgelerin kriptolu olarak saklanabilmesine yönelik kriptolu veri depolama cihazlarının kullanımına ilişkin güvenlik tedbirlerine yer verilmiştir.

5.6.5. Strateji Planları

Bu başlıkta kriptografiye dayalı bilgi güvenliği ile ilgili olduğu değerlendirilen strateji planları incelenmiştir.

5.6.5.1. On İkinci Kalkınma Planı 2024-2028

Cumhurbaşkanlığı Strateji ve Bütçe Başkanlığı tarafından hazırlanan On İkinci Kalkınma Planı (2024-2028), 30.10.1984 tarihli ve 3067 sayılı Kanun gereğince, Türkiye Büyük Millet Meclisi Genel Kurulunun 31.10.2023 tarihli 15 inci birleşiminde onaylanmış olup birçok konu başlığında ülkemizin gelişimine yönelik hedefler içermektedir. Söz konusu plan içerisinde kuantum teknolojilerine yönelik hedefler de belirlenmiş,

- Uzun Vadeli (2024-2053) Gelişmenin Stratejisi ve On İkinci Kalkınma Planının (2024-2028) Temel Amaç ve İlkeleri ile Hedef ve Politikaları başlıklı ikinci bölümünün:
    - "Uzun Vadeli (2024-2053) Gelişmenin Stratejisi" başlığının "2053 Yılında Türkiye" alt başlıklı bölümünde;
      "270. Önümüzdeki dönemde ülkemiz bilim ve araştırma temelini güçlendirerek bilgi ve teknoloji üretimini artıracak, buluş ve yenilikçilikte iddialı ülkeler arasına girecektir. Bu çerçevede, temel bilimlere özel önem verilerek başta doktoralı olmak üzere araştırmacı insan gücü nicelik ve niteliğinin artırılması, yapay zekâ, robotik, biyoteknoloji, kuantum ve uzay araştırmaları gibi kritik alanlarda

ülkemizin bölgesinde ve dünyada bilim insanları için çekim merkezi haline gelmesi önem taşımaktadır. Türkiye'nin 2053 vizyonu, bilim ve teknoloji alanında kimseyi geride bırakmayan, yenilikçiliği içselleştirerek teknoloji girişimlerini ve Ar-Ge yatırımlarını teşvik eden bir ekosistemi güçlendirmek suretiyle ileri teknolojilerin merkezi haline gelmektir. 2053 ufkunda en az 5 üniversitemizin dünyanın ilk 100 üniversitesi arasında yer alması, ülkemizin küresel yenilik endeksi içinde ilk 10 ülke arasına girmesi ve Ar-Ge harcamalarının milli gelirdeki payının yüzde 4 düzeyine yükselmesi hedeflenmektedir."

- Yeşil ve Dijital Dönüşümle Rekabetçi Üretim başlığının "Elektronik" alt başlıklı bölümünde;

  "452. Yapay zekâ, siber güvenlik, kuantum bilişim ve nesnelerin interneti gibi alanlardaki yeniliklere uyum sağlanacak ve bu alanlardaki yetkinlik artırılacaktır."
- Yeşil ve Dijital Dönüşümle Rekabetçi Üretim başlığının "Savunma Sanayii" alt başlıklı bölümünde;

  "520.2. Kuantum teknolojileri, yapay zekâ, otonom sistemler, hipersonik teknolojiler gibi derin ve çığır açan teknolojilerde askeri ve sivil kullanıma yönelik Ar-Ge ve Ür-Ge faaliyetleri desteklenecektir."
- Yeşil ve Dijital Dönüşümle Rekabetçi Üretim başlığının "Bilim Teknoloji ve Yenilik" alt başlıklı bölümünde;

  "557. Ülkemizde Milli Teknoloji Hamlesinin gerçekleştirilmesine yönelik yapay zekâ, nesnelerin interneti, artırılmış gerçeklik, büyük veri, siber güvenlik, ileri malzeme, robotik, mikro/ nano/opto-elektronik, biyoteknoloji, hidrojen teknolojileri, yenilenebilir enerji teknolojileri, batarya teknolojileri, genom düzenleme, karbon yakalama, kullanma ve depolama teknolojileri, yeni nesil nükleer reaktörler, füzyon, kuantum, algılayıcı teknolojileri ve katmanlı imalat teknolojilerine ilişkin gerekli Ar-Ge altyapısının tesis edilmesi, projelerin yürütülmesi ve ihtiyaç duyulan nitelikli insan kaynağının yetiştirilmesi sağlanacaktır."
- Nitelikli İnsan, Güçlü Aile, Sağlıklı Toplum başlığının "Eğitim" alt başlıklı bölümünde;

"688.6. 5G ve ötesi yeni nesil iletişim teknolojilerinde yazılım, donanım ve altyapı alanlarında, nesnelerin interneti, yapay zekâ, büyük veri, kuantum, siber güvenlik, akıllı ulaşım, artırılmış gerçeklik gibi gelişen teknoloji alanlarında nitelikli insan gücü yetiştirilmesi çalışmalarına ağırlık verilecektir."

hususlarına yer verilmiştir.

On İkinci Kalkınma Planı (2024-2028), kuantum teknolojilerine yönelik olarak incelendiğinde yeniliklere uyum sağlanarak yetkinliğin artırılmasının, araştırmacı insan gücü nicelik ve niteliğinin artırılarak bir yol haritasının hazırlanmasının ve gerekli altyapının oluşturulmasının, ayrıca askeri ve sivil kullanıma yönelik gerçekleştirilecek faaliyetlerin desteklenerek ülkemizin ileri teknolojilerde öncü olmasının hedeflendiği değerlendirilmektedir.

5.6.5.2. Ulusal Siber Güvenlik Stratejisi ve Eylem Planı (2020-2023)

2020/15 sayılı Cumhurbaşkanlığı Genelgesi ile Ulaştırma ve Altyapı Bakanlığı tarafından hazırlanan Ulusal Siber Güvenlik Stratejisi ve Eylem Planı (2020-2023) yayımlanmıştır. Söz konusu belgede 8 stratejik amaca ilişkin olarak kurum ve kuruluşlar tarafından gerçekleştirilmesi planlanan 40 adet eylem ve 75 adet uygulama adımı yer almaktadır. Yer alan stratejik amaçlardan:

- "I. Kritik Altyapıların Korunması ve Mukavemetin Artırılması" başlığının alt başlıklı "Siber Uzayda Ulusal Güvenlik" bölümünde;

"Ülkemizde "Elektronik Haberleşme", "Enerji" "Finans", "Ulaştırma", "Su Yönetimi" ve "Kritik Kamu Hizmetleri" olarak tanımlanan kritik altyapı sektörlerinin korunmasına yönelik önemli faaliyetler gerçekleştirilmiştir. Süreklilik içerisinde yürütülmesi gerekli bu faaliyetlerin, değişen siber tehdit vektörleri ve ortaya çıkan ulusal ihtiyaçlar ile teknolojide yaşanan gelişmeler dikkate alınarak daha etkin bir şekilde yürütülmesine devam edilecektir. Bu amaçla kritik altyapıların korunması stratejik amaçlardan biri olarak belirlenmiştir. Siber tehditler karşısında kamu ve özel sektörün korunmasını sağlayacak tedbirler alınarak ulusal mukavemetin artırılması hedeflenmektedir.

Bu çerçevede gerçekleştirilecek çalışmalarda; uluslararası bilgi güvenliği standartlarının kamu ve özel sektörde uygulanmasının yaygınlaştırılması, altyapılarda üretici bağımlılığının önüne geçilmesi, yurt içinde üretilen verilerin yurt içinde kalması gibi konular anahtar rol oynayacaktır. Bunun yanında, sektörel düzenlemelerin geliştirilmesi ve denetim mekanizmalarının oluşturulması, acil durum hazırlık planlarının hayata geçirilmesi ve güvenli bir teknolojik dönüşümün sağlanması önceliklerimiz arasında yer almaktadır"

- "VI. Yerli ve Milli Teknolojilerin Geliştirilmesi ve Desteklenmesi" başlığının "Türkiye'nin Teknolojisi" alt başlıklı bölümünde;

"Yeni nesil teknolojilerin entegre edildiği yerli ve milli siber güvenlik çözümlerinin sayısının artırılması ve kullanımının yaygınlaşması ülkemizin 2023 vizyonu kapsamındaki hedeflerine ulaşmamıza katkı sağlayacaktır. Ülke olarak siber güvenlik alanında öncü olmak hedefi ile yürütülen çalışmalar kapsamında özel sektörün gelişimi, büyümesi, ihracat kapasitesini artırarak ekonomiye katkı sağlaması ve teknolojiye yön veren bir konumda olması temel hedeftir."

- "VII. Siber Güvenliğin Milli Güvenliğe Entegrasyonu" başlığının "Ulusal Güvenlik İçin Siber Güvenlik" alt başlıklı bölümünde;

"Siber güvenlik ulusal güvenliğin ayrılmaz bir parçasıdır. Bu bağlamda üst düzey milli güvenlik politikalarımızda siber güvenliğe ilişkin hususların da azami derecede dikkate alınması, bu politikalarda kara, hava, deniz ve uzay güvenliğinin yanında siber savunmanın da yerini alması, ülkemizin diğer unsurlarla birlikte siber unsurları da içeren hibrit tehditlerden korunması ve caydırıcılığın artırılması amaçlanmaktadır."

ifadelerine yer verilmiştir.

Bu çerçevede, Ulusal Siber Güvenlik Stratejisi ve Eylem Planı (2020-2023) içerisinde yer alan stratejik amaçlar incelendiğinde; elektronik haberleşme ve kritik kamu hizmetleri gibi kritik altyapı sektörlerinin korunmasına yönelik yürütülen faaliyetlerin ulusal ihtiyaçlar ve teknolojide yaşanan gelişmelerin dikkate alınarak daha etkin bir şekilde yürütülmesinin, yeni nesil teknolojilerin entegre edildiği yerli ve milli siber

güvenlik çözümlerinin sayısının artırılmasının ve kullanımının yaygınlaştırılmasının, siber güvenliğin ulusal güvenliğin ayrılmaz bir parçası olduğu düşüncesiyle milli güvenlik politikalarında siber güvenliğe ilişkin hususların da azami derecede dikkate alınmasının ve ülkemizin siber unsurları da içeren hibrit tehditlerden korunmasının hedeflendiği görülmekte ve söz konusu hedeflerin gelecekte ulusal güvenliğimizi tehdit etme ihtimali yüksek olan kuantum bilgisayarlara karşı geliştirilecek olan kuantum kriptografi algoritmaları için önem arz ettiği değerlendirilmektedir.

5.6.6. Bilgi ve İletişim Güvenliği Rehberi

06.07.2019 tarihinde yayımlanarak yürürlüğe giren Bilgi ve İletişim Güvenliği Tedbirleri konulu Cumhurbaşkanlığı Genelgesi uyarınca, kamu kurumları ve kritik altyapı hizmeti veren işletmeler; karşılaşılan güvenlik risklerinin azaltılması, etkisiz kılınması ve özellikle gizliliği, bütünlüğü veya erişilebilirliği bozulduğunda milli güvenliği tehdit edebilecek veya kamu düzeninin bozulmasına yol açabilecek kritik türdeki verilerin güvenliğinin sağlanması amacıyla belirli güvenlik tedbirlerini uygulamakla yükümlü kılınmıştır. Genelge ile farklı güvenlik seviyelerinde tedbirler içeren Bilgi ve İletişim Güvenliği Rehberinin Cumhurbaşkanlığı Dijital Dönüşüm Ofisi tarafından hazırlanması, kapsam dâhilindeki Kurumların Rehbere uyum sağlaması öngörülmüştür. Bu doğrultuda 27 Temmuz 2020 tarihinde Bilgi ve İletişim Güvenliği Rehberi, Kurumlar tarafından gerekleri yerine getirilmek üzere yayımlanmıştır. Kurumların Rehbere uyum sağlarken yerine getirmesi gereken adımlardan biri olan denetim süreci ise Bilgi ve İletişim Güvenliği Denetim Rehberinde düzenlenmiştir.

Bilgi ve İletişim Güvenliği Rehberinde uygulama süreci tanımlanarak planlama, uygulama, kontrol etme ve önlem alma ile değişiklik yönetimi alt süreçlerinden oluştuğu ifade edilmiş, planlama kapsamında; kurum varlıklarının gruplandırılması, gruplama sonucu elde edilen varlık gruplarının kritiklik derecelendirmesinin yapılması, bu varlık grubuna uygulanması gereken güvenlik tedbirlerinin mevcut durumunun analizi ve boşluk analizinin yapılarak yol haritasının hazırlanması faaliyetlerinin yürütüleceği, kontrol etme ve önlem alma süreci kapsamında ise rehber kapsamında yürütülen çalışmaların izlenmesi ve kontrolü faaliyetlerinin gerçekleştirileceği belirtilmiştir.

Rehberde varlık tanımı "Elektronik ve/veya fiziksel ortamlarda yer alan; iletişim yoluyla aktarılabilen bilgiyi içeren, kurumun iş süreçleri açısından değer taşıyan tüm bilgi ve bilgi işleme olanakları, bilgiyi kullanan ve taşıyan personel ile bilgiyi barındıran fiziksel mekânlar" olarak ifade edilmiş, tanımlanan varlık gruplarının ise;

- Ağ ve Sistemler
- Uygulamalar
- Taşınabilir Cihaz ve Ortamlar
- Nesnelerin İnterneti (IoT) Cihazları
- Fiziksel Mekânlar
- Personel

olduğu belirtilmiştir.

Rehberin "Uygulama ve Veri Güvenliği" bölümünde iletişim güvenliğinde alınması gereken tedbirlere yer verilerek kritik verinin şifrelenmesinde *"Ulusal düzeyde kritik veri işleyen uygulamalar tarafından oluşturulan trafikten kripto analiz yöntemleri ile bilginin ifşası için yapılabilecek saldırılar engellenmelidir. Bu veri şifreli trafik üzerinden ayrıca şifrelenerek taşınmalıdır."* tedbirine yer verilmiş, "Uygulama ve Teknoloji Alanlarına Yönelik Güvenlik Tedbirleri" bölümünün "Kripto Uygulamaları Güvenliği" başlığında;

- Kriptografik algoritma seçiminin, algoritma kullanım amacı, algoritmayı kullanacak taraflar ve bu kapsamda işlenecek bilgi/verinin kritiklik seviyesi göz önünde bulundurularak yapılması gerektiği,
- Kurum varlıklarının kritiklik derecesine uygun kripto modüllerin kullanılması gerektiği,
- Kritik bilgi/veri işleyen kurumların, kritiklik seviyesine uygun tipte milli kriptografik algoritmaların gerçeklendiği cihazları temin etmesi gerektiği,

belirtilerek denetim faaliyetlerinde kriptografik algoritma seçiminde varlık grubuna ait kritiklik derecesinin, kullanım amacının ve kullanım ortamı gereksinimlerinin dikkate alınıp alınmadığının denetlenmesi önerilmiştir.

Bu çerçevede, Bilgi ve İletişim Güvenliği Rehberinde bilgi güvenliğinin sağlanabilmesi amacıyla kriptografik algoritma güvenliğinin ele alınarak kurumlarda

bulunan verilerin kritiklik seviyesine göre sınıflandırılmasının sağlandığı görülmekle birlikte kullanılan algoritma sınıfının belirtilmesinin talep edilmemesi sebebiyle kuantum hesaplama teknolojilerine savunmasız olduğu değerlendirilen algoritmaların kurumların hangi bilgi sistemleri veya uygulamalarında kullanıldığına ilişkin tespitin söz konusu rehber kapsamında yapılamayacağı değerlendirilmektedir.

SONUÇ VE ÖNERİLER

SONUÇ

Bilgi, insanlık tarihi boyunca toplulukların gelişiminde, kültürel evriminde ve teknolojik ilerlemesinde kilit rol oynamış, zamanla ekonomik kalkınma ile ulusal güvenliğin temel unsuru haline gelmiştir. Bu sebeple milattan önce 1900'lü yıllardan itibaren bilginin yetkisiz kişilerce anlaşılmaz hale getirilmesinde kullanılan çeşitli kriptografik yöntemler geliştirilmiş, yazının icadı, matematik ve teknolojinin gelişimi ile birlikte şifreleme yöntemleri gelişmiş, farklılaşmış ve kullanımı yaygınlaşmıştır. Günümüzde yaygın olarak kullanılan ve temeli klasik bilgisayarların çözemeyeceği matematiksel tekniklere dayanan modern kriptografik yöntemler gizlilik, veri bütünlüğü, kimlik doğrulama, inkar edilemezlik özelliklerinin sağlanabilmesi için çeşitli algoritmalar vasıtasıyla;

- İmza sahibinin mesajı imzaladığına, imzalanan mesajın iletimi aşamasında bütünlüğünün ve içeriğinin değiştirilmediğine dair güvence sunan elektronik imzaların,
- Kodlu kriptolu haberleşmenin,
- İletim veya depolama aşamasında gizli belgelerin korunmasında, internet üzerinde güvenli iletişimin gerçekleştirilmesine imkan tanıyan SSL/TLS ile IPsec protokollerinin,
- Kablosuz bir ortamda ağın ve birbirine bağlı cihazların korunmasını sağlayan kablosuz ağ güvenliğinin,
- Uygulamalara ve verilere her yerden ve her zaman ulaşabilme imkanı sunan bulut bilişim güvenliğinin,
- Çeşitli sensörler içeren ve internete bağlanabilen cihazların birbirleriyle güvenli veri alışverişi yapmalarına ve çeşitli görevleri bağımsız olarak gerçekleştirmelerine imkan tanıyan IoT güvenliğinin,
- Güven eksikliğinin bulunduğu ortamlarda verilerin merkezi olmayan bir veri kayıt defterine kaydedilerek anonim katılımcıların kaydedilen verileri okumasına, doğrulamasına ve kopyalamasına olanak tanıyan ancak silme ve değişiklik yapılmasına izin verilmediği veritabanı mekanizması olan blokzinciri güvenliğinin

altyapısı da dahil olmak üzere günlük yaşamımızın birçok farklı alanında kullanılmaktadır.

Atom ve atom altı ölçekte madde ve ışığın özelliklerini, etkileşimlerini ve eylemlerini inceleyen bilim dalı olarak tanımlanan kuantum mekaniğinin ise makro dünyada gözlemlenmesi mümkün olmayan dolanıklık, süperpozisyon gibi çeşitli kuantum özellikleri sayesinde oluşturulan;

- Klasik bilgisayarlar ile simüle edilmesi mümkün olmayan durumların/davranışların yeniden üretilmesinde kullanılan kuantum simülasyon,
- Kuantum parçacıklarının çevresine karşı geliştirdiği olağanüstü duyarlılıktan yararlanarak klasik ölçüm cihazlarına kıyasla sıcaklık, basınç, frekans, ivmelenme, dönüş, manyetik ve elektrik alan gibi çeşitli fiziksel özellikleri daha hassas ve kesin bir şekilde ölçmemize olanak sağlayan kuantum algılama,
- Klasik bilgisayarlar ile çözülmesi mümkün olmayan veya makul zaman aralığında çözülemeyen üstel işlem zamanı gerektiren problemleri, kuantum mekaniği ilkelerinden yararlanarak hızla çözebilmeyi hedefleyen kuantum hesaplama,
- Kuantum mekaniği yasalarının kullanılarak; bilginin ve kuantum kaynaklarının güvenli bir şekilde iletilebilmesi amacıyla kuantum bilgisayarların, simülatörlerin ve sensörlerin birbirine bağlandığı bir iletişim ağını ifade eden kuantum iletişim

teknolojileri ile insanlık için yeni ve büyük fırsatlar sunması beklense de günümüzde yaygın olarak kullanılan AES, 3DES, RSA, Diffie Hellman ve ECC gibi kriptografik algoritmalarının; kuantum üstünlüğüne ulaşmış bir kuantum bilgisayarın kullanılması ve Grover'ın arama algoritması ile Shor'un çarpanlara ayırma algoritmasının uygulanması yöntemi ile polinom zamanda çözümlenebilir hale gelerek savunmasız kalacak olması ülkelerin ulusal bilgi güvenliğini tehdit etmektedir. Bu sebeple yaşanacak kuantum devriminin olumsuz etkilerinden korunabilmek için kuantum sonrası kriptografi uygulamaları üzerine araştırmalar şimdiden başlatılmıştır.

Bu doğrultuda 2016 yılında NIST tarafından "NIST Kuantum Sonrası Kriptografi Standardizasyon Süreci" olarak adlandırılan kuantum güvenli kriptografi standardizasyon süreci başlatılarak yeterli bilgi işlem gücüne sahip kuantum

bilgisayarlar oluşturulmadan önce tehdit altında olduğu değerlendirilen kriptografik algoritmaların yerine yenilerini koymak üzere yeni elektronik imza şemaları, anahtar üretimi ve değişimi için kullanılan anahtar kapsülleme mekanizmaları ve asimetrik anahtar şifreleme şemaları aranmaya başlanmıştır. Söz konusu süreç, Aralık 2016'da Kuantum Sonrası Kriptografi Standardizasyon Sürecine başvuruların gerçekleştirilebilmesi için halka açık bir çağrı yayınlanarak başlatılmış, Kasım 2017'de standardizasyon sürecinin son başvuru tarihinden önce 82 aday algoritma sunulmuş; hem başvuru koşullarını hem de minimum kabul edilebilirlik kriterlerini karşılayan 69 aday standardizasyon sürecinin ilk turuna kabul edilmiştir. Adayların bir yıl süren inceleme sürecinin ardından Ocak 2019'da ikinci değerlendirme turuna geçmek üzere hem iç analiz hem de kamuoyu görüşü göz önünde bulundurularak 26 algoritma seçilmiş, ilk tura kıyasla daha geniş bir topluluk ile yapılan değerlendirmeler sonucunda Temmuz 2020'de üçüncü tura geçmek üzere 7 finalist ve 8 yedek algoritma seçilmiş, üçüncü turun sonunda finalistlerin; dördüncü tur sonunda ise alternatif adayların standartlaştırılması amaçlanmıştır. Bahse konu sürecin 2024 yılı içerisinde tamamlanmasının hedeflendiği, akabinde ise standartlar ile uygulama kılavuzları üzerindeki çalışmaların devam edeceği ifade edilmektedir.

Kuantum bilgisayar tehdidine dirençli kriptografik algoritmalar oluşturulmasına ilişkin gerçekleştirilen çalışmaların yanı sıra güvenliğinin fizik yasalarınca garanti edildiği ve "Kuantum Anahtar Dağıtımı" olarak bilinen güvenli anahtar dağıtım yöntemi üzerine gerçekleştirilen çalışmalar da devam etmektedir. Bilginin ışığın kuantum durumlarında kodlanmasıyla uygulamasının gerçekleştirildiği bu yöntem; üçüncü kişiler tarafından veri trafiğinin gözlemlenmesi halinde alıcıya iletilen bilgi birimlerinin değerinin tespit edilebilir bir şekilde değişmesi, kuantum durumlarında kodlanmış verilere erişilmesi durumunda iletilen verinin yetkili taraflarca tespit edilebilecek şekilde değişmesi ve hataların ortaya çıkmasına sebep olması nedeniyle veri akışındaki bilgi biriminin bir kopyasının oluşturulmasının ve dolayısıyla gizli dinleme faaliyetinin gerçekleştirilmesinin imkansız olması gibi özellikler sunarak kuantum saldırıları da dahil olmak üzere tüm saldırı yöntemlerine karşı dirençli olduğu 'teorik' olarak kanıtlanmış bir güvenlik vadetmektedir. Öte yandan, kuantum anahtar dağıtım yönteminin uygulama aşamasında güvenlik unsurunun yalnızca kuantum yasalarına değil, uygulamanın gerçekleştirildiği cihaz güvenliğine de bağlı olması sebebiyle donanımsal özelliklerin kötüye kullanılarak gizli bilgilerin açığa

çıkarılmasına yönelik tehditler barındırdığı bilinmekte, uluslararası kuruluşlar tarafından uygulamada kullanılan cihazların sahip olması gereken güvenlik özelliklerine yönelik standart belirleme çalışmaları devam etmektedir.

Uluslararası kuruluşlar tarafından yayımlanan dokümanlar incelendiğinde; günümüzde yaygın bir şekilde kullanımda olan asimetrik şifreleme algoritmaları ile bazı simetrik şifreleme algoritmalarının, gelecekte kuantum hesaplama teknolojilerinin gelişimi ile kullanıma sunulacak olan daha güçlü işlemciler ya da kriptanaliz yöntemleri vasıtasıyla savunmasız hale geleceği endişesini taşıdıkları görülmüştür. ETSI tarafından yayımlanan dokümanda kuantum güvenli kriptografik algoritmalara geçişin zamanlamasına ilişkin bir denklem oluşturularak; asimetrik anahtarlı algoritmaların kırılmadan kalması gereken yıl sayısı, mevcut sistemin kuantum güvenli bir sistemle değiştirilebilmesi için harcanacak yıl sayısı ve kuantum güvenli algoritmalara güvenilebilmesi için ihtiyaç duyulan yıl sayısı toplamının kuantum bilgisayarların veya başka araçların kullanılarak mevcut kriptografik yöntemlerin savunmasız hale getirilmesi için ihtiyaç duyulan yıl sayısından fazla olması halinde asimetrik anahtarlı algoritmalar tarafından korunan tüm verilerin risk altında olduğu ile derhal önlem alınması gerektiği ifade edilmiştir. Bu amaçla çeşitli kuruluşlar tarafından;

- Kuantum anahtar dağıtımı alanında ortak bir arayüz ve standart geliştirme çalışmalarının gerçekleştirildiği,
- Kuantum güvenli kriptografi alanında ise algoritmaların mevcut durumu ve endüstriyel gereksinimleri göz önünde bulundurularak performans, işlevsellik, belirli uygulamalar özelindeki mimari özellikler gibi niteliklerin değerlendirilerek en iyi kuantum güvenli alternatiflerin belirlenmesi ve uygulanabilmesi için karşılaştırmalar ve önerilerde bulunulduğu,

görülmektedir. Bunun yanı sıra, kuantum bilgisayarın inşasından öncesinde dahi kötü niyetli kişilerin daha sonrasında şifreyi çözmek için şifrelenmiş verileri toplayıp sakladığı “şimdi depola, şifresini sonra çöz” saldırısı ile kuantum bilgisayara eriştiği bir zaman diliminde kullanılan şifreleme sistemlerini savunmasız hale getirebileceğinden bahisle kriptografi risk değerlendirmesi planlamasının yapılarak kuantum güvenli kriptografik algoritmalara ilişkin bir geçiş planı geliştirilmesi tavsiye edilmektedir.

Ülke uygulamaları incelendiğinde ise ABD'nin, kuantum anahtar dağıtımı yönteminin kimlik doğrulaması yapılmadan yalnızca gizlilik sağlayan bir şifreleme algoritması için anahtarlama malzemesi üretmesi sebebiyle asimetrik kriptografi algoritmalarının yönteme dahil edilmesi gerektiğinin ve kuantum anahtar dağıtımının sunduğu gizlilik hizmetlerinin kuantum güvenli kriptografik algoritmalar ile daha güvenli ve daha uygun maliyetlerde sunulabileceğini değerlendirmesi sebebiyle ulusal güvenlik sistemlerinde iletişimi korumak için kuantum anahtar dağıtım kullanımını desteklemediğini bu sebeple herhangi bir kuantum anahtar dağıtım güvenlik ürününü sertifikalandırmayı veya onaylamayı öngörmediği görülmüştür. Bu doğrultuda, kritik altyapıları tehditlere karşı korumakla görevlendirilmiş olan CISA tarafından 2022 yılında Kuantum Güvenli Kriptografi Girişiminin başlatılarak kuantum güvenli kriptografik yöntemlere geçiş için bir yol haritası oluşturulmuş, 21.12.2022 tarihinde yürürlüğe giren Kuantum Bilişim Siber Güvenlik Hazırlık Yasası (H.R.7535) ile kurumların bilgi teknolojileri sistemlerini kuantum bilgisayarlardan gelen saldırılara karşı dayanıklı olan kuantum güvenli kriptografi algoritmalarına belirli süreler içerisinde geçirmelerine yönelik bir dizi görev verilmiştir.

Avrupa Birliği ise kuantum siber saldırılara karşı bilgi güvenliğini sağlamaya yönelik kuantum güvenli kriptografi ile ilişkili bir strateji belirlememiş olmakla birlikte kuantum iletişim teknolojileri ve kuantum anahtar dağıtım yöntemi uygulamalarına odaklanmıştır. Bu doğrultuda;

- 2023-2027 dönemi için Güvenli Bağlantı Programı üzerinde anlaşılmış ve EU 2023/588 sayılı düzenleme ile "IRIS" adı verilen ve AB Üye Devletlerine askeri uygulamaların yanı sıra kritik altyapının korunması, gözetim ve dış eylem veya kriz yönetimi desteği gibi operasyonel ihtiyaçlarını karşılayan yüksek güvenlikli, egemen ve küresel bağlantı hizmetlerine garantili erişim sağlama hedefleri olan uydu sistemi güvenliğinde kuantum kriptografi de dahil olmak üzere gelişmiş şifreleme teknolojilerinin kullanılmasına karar verilmiş,
- 2023 yılının Aralık ayında Fransa, Belçika, Hırvatistan, Yunanistan, Finlandiya, Slovakya, Slovenya, Çek Cumhuriyeti, Malta, Estonya ve İspanya tarafından onaylanan Kuantum Teknolojilerine İlişkin Avrupa Deklarasyonu ile imzacı üye devletler dünya üzerinde ve uzayda güvenli iletişim, kuantum hesaplama, kuantum simülasyon ve kuantum algılama alanlarında geleceğin pan-Avrupa kuantum altyapılarını kolektif olarak inşa etmek için faaliyetlerde

bulunulmasında üye devletler ve Avrupa Komisyonu ile birlikte çalışmayı kabul etmiştir.

Kuantum teknolojileri alanında gerçekleştirilen araştırma geliştirme faaliyetleri alanında uluslararası lider olduğu ifade edilen Çin Halk Cumhuriyeti (IDB, 2019) ise hem yer tabanlı hem de uydu tabanlı kuantum telekomünikasyon ağının geliştirilmesinde ön sıralarda yer almakla birlikte kuantum güvenli kriptografi alanında NIST tarafından düzenlenen standardizasyon çalışmalarına benzer şekilde yalnızca Çinli araştırmacılara açık bir yarışma düzenlemiş ve 128 ile 256 bit güvenlik seviyesinde elektronik imza, açık anahtar şifreleme ve anahtar anlaşması protokolleri için kriptografik mekanizmalar belirlemeyi hedeflemiştir.

2010 yılında akıllı telefonlarda tek kullanımlık şerit şifrelemesi ile iletişimin sağlanması, depolanmış verilerin uzun vadeli bütünlüğünün sağlanabilmesi için imza ve kimlik doğrulama şemalarının kullanımı gibi uygulamaların kullanımına imkan tanıyan bir kuantum ağını inşa eden Japonya;

- 2020 yılında fiber ve uydu tabanlı iletişimi içeren 100 düğümlü küresel bir kuantum anahtar dağıtım ağı kurulmasına ilişkin projesini duyurmuş,
- Kuantum güvenli kriptografik algoritmalara ilişkin NIST tarafından yürütülen standartlaştırma çalışmalarına dahil olmuş,
- e-Devlet altyapısında kullanılan kriptografik protokollerin güvenliğini değerlendirmek, izlemek, kriptografinin uygun uygulama ve işletim yöntemlerini araştırmak ve incelemek için 2000 yılında başlatılan CRYPTEC projesi kapsamına kuantum güvenli kriptografi ile kuantum anahtar dağıtımı da dahil edilmiş,
- 2013 yılında yayımlanan ve e-Devlet sisteminde kullanılması tavsiye edilen şifreleme yöntemlerini kuantum güvenli algoritmaları içerecek şekilde güncellemiştir.

Ülkemizde ise TÜBİTAK BİLGEM UEKAE bünyesinde kuantum kriptografi ve kuantum anahtar dağıtımı konularını da içeren ulusal ve uluslararası ölçekli çeşitli projeler yürütüldüğü, 2023 yılında “Kuantum Teknolojileri Bölümü” adında yeni bir birim kurulduğu ve kuantum teknolojileri alanında çağın gereksinimlerinin

yakalanarak altyapı ve yetişmiş insan gücü birikiminin oluşturulmasının, Ar-Ge projelerinin yürütülmesinin, hem sivil hem de askeri uygulamalar için kuantum teknolojileri tabanlı sistemler geliştirilmesinin hedeflendiği, kuantum hesaplama, kuantum haberleşme, kuantum görüntüleme, kuantum algılama ve metroloji gibi başlıca alanlarda gerçekleştirilecek faaliyetler ve geliştirilecek sistemler ile ülkemizin kuantum teknolojilerinde söz sahibi olmasına ve ilerlemesine katkı sağlanmasının amaçlandığı bilinmektedir. Diğer yandan ASELSAN'ın TOBB Ekonomi ve Teknoloji Üniversitesi yerleşkesinde kurulan Kuantum Araştırma Laboratuvarında yürütülecek projeler ile ülkemizin kuantum teknolojiler alanındaki bilgi birikimi ve teknolojik hazırlık seviyesinin artırılarak yerli ve milli sistemlerin üretimini hedeflediği, ayrıca TÜBİTAK BİLGEM ile birlikte kuantum güvenli kriptografi alanında ortak çalışmalar yürüttüğü, bu kapsamda 29 Şubat-1 Mart 2020 tarihleri arasında gerçekleşen ASELSAN-TÜBİTAK BİLGEM İş Birliği Çalıştayında alınan kararlar doğrultusunda projelendirilmesi muhtemel Milli Savunma Bakanlığı ve Savunma Sanayii Başkanlığı projelerinde ortak çalışma kararı alındığı bilinmekte, klasik kriptografi ile kuantum güvenli kriptografi çözümlerinin birlikte kullanılarak ASELSAN tarafından tasarlanan güvenli ağ mimarisi çözümlerinde kullanılacak kripto cihazlarında uygulanmasının planlandığı bilinmektedir.

Ülkemiz yasal ve ikincil düzenlemeleri incelendiğinde EHK'nın;

- 5 inci maddesinde her türlü siber müdahale aracının ve millî çözümlerin üretilmesi ve geliştirilmesi amacı ile çalışmalar yapma ve siber güvenlik alanında faaliyet gösteren gerçek ve tüzel kişilerin uyması gereken usul ve esasları hazırlama görevlerinin Ulaştırma ve Altyapı Bakanlığına verildiği,
- 6 ncı maddesinde milli güvenlik hedefleri doğrultusunda gerekli tedbirlerin alınması ile kurum ve kuruluşlar ile gerçek ve tüzel kişilerin siber saldırılara karşı korunması ve bu saldırılara karşı caydırıcılık sağlamak için gerekli tedbirlerin alınması görevlerinin BTK'ye verildiği

görülmekle birlikte BTK uhdesinde yer alan "Elektronik İmza Kanununun Uygulanmasına İlişkin Usul ve Esaslar Hakkında Yönetmelik" ile "Kayıtlı Elektronik Posta Sistemine İlişkin Usul ve Esaslar Hakkında Yönetmelik" altyapısında kullanılan kriptografik algoritmaların kuantum hesaplama teknolojilerinin gelişimi ile birlikte kuantum siber saldırılara karşı savunmasız hale geleceği belirtilen yöntemler olduğu, benzer şekilde kamu kurum ve kuruluşlarında muhteviyatına veya güncelliğine göre

gizlilik dereceli belgeler için uygulanacak usul ve esasların belirlendiği "Gizlilik Dereceli Belgelerde Uygulanacak Usul ve Esaslar Hakkında Yönetmelik" kapsamında yer alan ve kritik önemi haiz verileri içeren hizmete özel belgelere ilişkin işlemlerde uygulanan kriptografik yöntemlerin de kuantum bilgisayar tehdidine karşı dirençli olmadığı görülmektedir. Bununla birlikte, kodlu veya kriptolu haberleşme hizmetinden yararlanılması öncesinde cihazlara ait kod veya kripto anahtarlarının BTK'ye teslim edilmesi gerektiğini düzenleyen "Kamu Kurum ve Kuruluşları ile Gerçek ve Tüzel Kişilerin Elektronik Haberleşme Hizmeti İçinde Kodlu veya Kriptolu Haberleşme Yapma Usul ve Esasları Hakkında Yönetmelik" kapsamına, tarafların kriptolu haberleşme öncesinde kuantum anahtar dağıtımına dayalı tek şeritli şifreleme yöntemi ile şifre oluşturarak güvenli iletişimin sağlanabildiği kuantum iletişim teknolojilerinden yararlanan haberleşme cihazlarının da dahil olabileceği öngörülmektedir.

Diğer yandan, On İkinci Kalkınma Planı (2024-2028) ile kuantum teknolojilerine yönelik yetkinliğin artırılmasının, araştırmacı insan gücü nicelik ve niteliğinin artırılarak bir yol haritasının hazırlanmasının ve gerekli altyapının oluşturulmasının, ayrıca askeri ve sivil kullanıma yönelik gerçekleştirilecek faaliyetlerin desteklenerek ülkemizin ileri teknolojilerde öncü olması hedeflerinin yer aldığı, Ulusal Siber Güvenlik Stratejisi ve Eylem Planında (2020-2023) ise elektronik haberleşme ve kritik kamu hizmetleri gibi kritik altyapı sektörlerinin korunmasına yönelik yürütülen faaliyetlerin ulusal ihtiyaçlar ve teknolojide yaşanan gelişmelerin dikkate alınarak daha etkin bir şekilde yürütülmesi, yeni nesil teknolojilerin entegre edildiği yerli ve milli siber güvenlik çözümlerinin sayısının artırılması ve kullanımının yaygınlaştırılması amaçlarının yer aldığı görülmektedir.

Bu kapsamda, birçok ülkenin ulusal verilerinin güvenliği ile kritik altyapı ve sistemlerinin sürdürülebilirliğini kuantum siber saldırılardan korumaya yönelik gerekli çalışmaları halihazırda başlattığı, ancak ülkemiz planlamalarında kuantum teknolojilerine yönelik yetkinliğin artırılması hedeflerine yer verilmiş olmasına rağmen yakın gelecekte ülkemizin ulusal güvenliğini tehdit etme ihtimali yüksek olan kuantum hesaplama teknolojilerinin yıkıcı etkilerinden korunmak için belirlenmiş bir ulusal politikanın veya stratejinin henüz mevcut olmadığı görülmektedir.

ÖNERİLER

Tez kapsamında incelenen ülke uygulamaları, uluslararası kuruluşların yayınları ve ülkemizde gerçekleştirilen çalışmalar göz önünde bulundurularak hızlı bir şekilde gelişim gösteren ve yakın bir zaman diliminde hayatımızda önemli bir yer edineceği öngörülen kuantum hesaplama teknolojilerinin neden olabileceği bilgi güvenliği tehditlerinin ortadan kaldırılabilmesini teminen önerilen hususlar aşağıda ifade edilmektedir.

- **Ülkemizde üretilen kritik verinin kuantum teknolojilerindeki gelişmeler paralelinde güvenliğinin sağlanması amacıyla yerli ve milli çözümler geliştirilmesi önerilmektedir.**

Hızlı bir gelişim göstererek klasik bilgisayarlar ile kriptanalizi mümkün olmayan ve günlük hayatta askeri haberleşme, bankacılık işlemleri, cep telefonu görüşmeleri, elektronik imzalar, internet üzerinden güvenli iletişim kurulabilmesi için kullanılan protokoller, blokzincir güvenliği gibi sıklıkla kullanılan şifreleme algoritmalarını savunmasız bırakması beklenen kuantum hesaplama teknolojileri, ulusal güvenliğin en önemli bileşenlerinden biri olan siber güvenliği de tehdit etmektedir. Bu sebeple gizliliği, bütünlüğü veya erişilebilirliği bozulduğunda milli güvenliği tehdit edebilecek veya kamu düzeninin bozulmasına sebebiyet verebilecek kritik önemi haiz verilerin güvenliğinin sağlanabilmesi amacıyla söz konusu problemin çözümünde uygulanacak yöntemlerin geliştirilmesinin, gerekli planlamaların yapılmasının ve uygulamaya geçirilmesinin kayda değer bir zaman gerektireceği de göz önünde bulundurularak kuantum siber güvenlik tehditlerine yönelik gerekli tedbirlerin ivedilikle alınması gerekmektedir.

Ülke uygulamaları incelendiğinde ABD ve Çin'in kendi kuantum güvenli kriptografik algoritmalarını oluşturma temelli bir politika izlediği ancak Avrupa Birliği ile Japonya'nın bilgi güvenliği hususunda kuantum anahtar dağıtım yöntemlerine ağırlık verdiği ve kuantum siber güvenlik tehditlerine yönelik olarak kendi kriptografik algoritmalarını oluşturmaktan ziyade NIST tarafından gerçekleştirilen standardizasyon çalışmalarına yetkin personel dahli ile destek verdiği ve süreci takip ettiği görülmektedir.

Ülkemizde ise TÜBİTAK BİLGEM UEKAE bünyesinde kuantum kriptografi ve kuantum anahtar dağıtımı konularını da içeren ulusal ve uluslararası ölçekte çeşitli projeler yürütüldüğü, daha öncesinde gerçekleştirilen çalışmalarda TÜBİTAK bünyesinde bulunan laboratuvarlar aracılığıyla yerli ve milli perspektifle asimetrik anahtarlı algoritmaların geliştirildiği ve bahse konu algoritmaların yeterli güvenlik seviyesinde bulunup bulunmadıklarına yönelik analiz ve değerlendirme çalışmalarının yine TÜBİTAK tarafından yapıldığı bilinmektedir. Diğer yandan, ülkemizin kuantum siber saldırılara yönelik ulusal verilerinin güvenliğini, kritik altyapı ve sistemlerinin sürdürülebilirliğini sağlayacak bir ulusal politika veya stratejinin henüz belirlenmediği görülmektedir.

ABD kriptanaliz amacıyla kullanılması muhtemel kuantum bilgisayarların üretimi için 2030 yılını işaret etmekte ve bu doğrultuda ulusal güvenliğin sağlanabilmesi için dünya genelinde çeşitli önlemler alınmaktadır. Aynı doğrultuda, ülkemizin yaklaşan kuantum siber saldırılardan korunabilmesi için kamu kurum ve kuruluşları ile kritik altyapı sektörleri öncellikli olmak şartıyla veri iletiminde veya uygulama altyapılarında kullanılan kriptografik algoritmalarının kuantum güvenli kriptografik algoritmalarla değiştirilmesine yönelik bir ulusal politikanın belirlenerek yol haritasının oluşturulması gerekmektedir.

Bu amaçla uygulanması gereken ilk adımın ise; kriptografik algoritma üretiminde deneyimli ve geliştirilen algoritmaların yeterli güvenlik seviyesine sahip olup olmadığına yönelik analiz ve değerlendirme çalışmalarını gerçekleştirebilecek altyapıya sahip olan TÜBİTAK tarafından yerli ve milli perspektifle geliştirilmiş kuantum güvenli kriptografik algoritmaların üretilmesi olduğu değerlendirilmektedir. Bu doğrultuda;

- NIST tarafından şeffaf bir şekilde yürütüldüğü ifade edilen ve 2024 yılında tamamlanması hedeflenen “NIST Kuantum Sonrası Kriptografi Standardizasyon Süreci” benzeri bir sürecin TÜBİTAK tarafından başlatılabileceği,
- Sürece araştırma kuruluşları, üniversiteler ve ülkemiz yetkili kurumlarından etkin ve yetkin personel dahli ile detayları kamuya açıklanmamak üzere belirli değerlendirme kriterleri ile güvenlik tanımlarının yapıldığı algoritma

tasarımlarına yönelik önerilerinin alınarak TÜBİTAK tarafından değerlendirmeye tabi tutulabileceği,

- Asgari kabul edilebilirlik gereklerini karşıladığı değerlendirilen kripto sistemlerin gerek görülmesi halinde Ulusal Siber Olaylara Müdahale Merkezi (USOM) bünyesinde oluşturulan bir çalışma grubu aracılığıyla güvenliğinin test edilmesinde NIST tarafından dikkate alınması gerektiği ifade edilen (NIST, 2022) şifreli metin saldırısı (IND-CCA2), seçilmiş düz metin saldırısı (IND-CPA) ve seçilmiş mesaj saldırısı (EUF-CMA) gibi saldırı analizlerinin gerçekleştirilerek ihtiyatlı kararlar alınmasında, tutarlı seçimler yapılmasında ve güvenlik/performans analizlerinin gerçekleştirilmesinde katkıda bulunulabileceği

değerlendirilmektedir.

Bu çerçevede, kamu kurum ve kuruluşları ile kritik altyapı sektörlerinde bulunan ve gizliliği, bütünlüğü veya erişilebilirliği bozulduğunda milli güvenliği tehdit edebilecek veya kamu düzeninin bozulmasına yol açabilecek kritik türdeki veriler ile nüfus, sağlık, iletişim kayıt bilgileri, genetik ve biyometrik veriler gibi kişisel verilerin, geliştirilen yerli ve milli kuantum güvenli kripto sistemler aracılığıyla güvenli bir şekilde iletiminin gerçekleştirilmesi ile e-Devlet altyapısında kullanılan kriptografik protokollerinin yerli ve milli kuantum güvenli kripto sistemleri ile değiştirilmesinin uygun olacağı değerlendirilmektedir.

Diğer yandan, gerçekleşmesi muhtemel kuantum siber saldırılardan korunabilmek amacıyla yeterli bilgi işlem seviyesine ulaşmış kuantum bilgisayarlar henüz oluşturulmadan geliştirilen yerli ve milli kripto sistemin, kuantum bilgisayarların bilgi işlem gücünün artırılması veya geliştirilen kripto sistemlerde zaman içerisinde güvenlik zafiyetlerinin ortaya çıkması gibi sebeplerle daha dayanıklı hale getirilmesi, performansının geliştirilmesi veya yeni teknolojik trendlere daha iyi uyum sağlamasını teminen güncellenmesi/geliştirilmesi gerekeceği göz önünde bulundurularak etkin ve yetkin personel yetiştirilmesinin, kurum içi, kurum dışı, yurt içi, yurt dışı eğitimlerine gönderilerek bilgilerinin güncel ve eğitim seviyelerinin yüksek tutulmasının önem arz ettiği değerlendirilmektedir. Bu kapsamda, etkin ve yetkin insan kaynağının oluşturulabilmesi için;

- Üniversiteler ve araştırma kurumlarıyla iş birliği yapılarak kuantum kriptografi alanında eğitim programlarının oluşturulması ve katılımın teşvik edilmesi,
- Araştırma ve geliştirme projeleri kapsamında gerçekleştirilecek projelerin desteklenmesi,
- Kuantum hesaplama ve kuantum kriptografi alanında çalışabilmek için gerekli laboratuvar altyapısının oluşturulması ve güncel teknolojilere erişim için laboratuvarların finansal olarak desteklenmesi,
- İlgili kamu kurum ve kuruluşlarının kuantum teknolojileri ve kuantum kriptografi alanında seminerler ve konferanslar düzenlemesini sağlayarak farkındalık oluşturulması, güncel gelişmelerin paylaşılmasının sağlanması ve potansiyel kariyer fırsatlarına yönelik bilgilendirmenin yapılması

hususlarının önem arz ettiği değerlendirilmektedir.

- **Mevzuatta yer verilen kriptografik algoritmaların kuantum güvenli kriptografik algoritmalar baz alınarak güncellenmesi ve/veya kuantum güvenli olmasına yönelik çalışmaların takip edilmesi önerilmektedir.**

Ülkemiz mevzuatı incelendiğinde ikincil düzenlemelerde yer verilen bazı kriptografik algoritmaların kuantum hesaplama teknolojilerinin gelişmesi ile birlikte savunmasız kalabileceği görülmüştür. Bu kapsamda;

- Kamu kurum ve kuruluşlarının "Gizlilik Dereceli Belgelerde Uygulanacak Usul ve Esaslar Hakkında Yönetmelik" kapsamında yer alan ve kritik önemi haiz verileri içeren hizmete özel belgelerine ilişkin işlemlerin yerli ve milli kuantum güvenli kripto sistemler aracılığıyla gerçekleştirilmesi,
- 06.01.2005 tarihli ve 25692 sayılı Resmi Gazete'de yayımlanarak yürürlüğe giren Elektronik İmza Kanununun Uygulanmasına İlişkin Usul ve Esaslar Hakkında Yönetmelik ile 25.08.2011 tarihli ve 28036 sayılı Resmi Gazete'de yayımlanarak yürürlüğe giren Kayıtlı Elektronik Posta Sistemine İlişkin Usul ve Esaslar Hakkında Yönetmelik altyapısında kullanılan:
    - Asimetrik anahtarlı algoritma sınıfında yer alan ve kuantum hesaplama teknolojilerine karşı savunmasız olduğu ifade edilen imza oluşturma ve doğrulama mekanizmalarının kuantum güvenli kriptografik algoritmalar ile değiştirilmesinin,

- Anahtarsız algoritma sınıfında yer alan ve güvenliği anahtar boyutuna bağlı olan özetleme algoritmalarında ise kuantum hesaplama teknolojilerine dirençli olduğu belirtilen SHA-2 ile SHA-3 şifreleme algoritmalarının kullanılmasının

gerekli güvenlik kriterlerinin sağlanmasında yeterli olacağı değerlendirilse dahi söz konusu sistemlerin uluslararası geçerliliğe sahip olmasını teminen 06.01.2005 tarihli ve 25692 sayılı Resmi Gazete'de yayımlanarak yürürlüğe giren Elektronik İmza ile İlgili Süreçlere ve Teknik Kriterlere İlişkin Tebliğ uyarınca ETSI TS 119 312 standardına uygun olması gerektiğinin hükme bağlanması sebebiyle ETSI tarafından söz konusu algoritmaların kuantum güvenli olarak güncellenmesi akabinde gerekli değişikliklerin iç mevzuata aktarılması,

tedbirlerinin alınmasının uygun olacağı düşünülmektedir. Diğer yandan, "Kamu Kurum ve Kuruluşları ile Gerçek ve Tüzel Kişilerin Elektronik Haberleşme Hizmeti İçinde Kodlu veya Kriptolu Haberleşme Yapma Usul ve Esasları Hakkında Yönetmelik" kullanılan kriptografik yöntemden bağımsız olarak düzenlenmiş olsa da söz konusu Yönetmelik kapsamında yer alan ve mevcut kodlu veya kriptolu haberleşme sistemlerinden farklı olarak iletişimde kullanılacak şifrenin anlık ve kuantum kanalları vasıtasıyla oluşturulabildiği kuantum anahtar dağıtımına dayalı kriptolu haberleşme cihazlarına ilişkin gelişmelerin BTK'de muhafaza edilen kripto anahtarlarına ilişkin teknik teçhizat yönüyle takip edilmesinin önem arz ettiği değerlendirilmektedir.

- **Ulusal kuantum kriptografi stratejisi ve eylem planı oluşturulması önerilmektedir.**

Ülke uygulamaları incelendiğinde gerek kuantum anahtar dağıtımı yönteminin gerek kuantum güvenli kriptografik algoritmaların ülkelerin kritik önemi haiz verilerini koruması için kullanıldığı ve bu alanda çeşitli hedefler konularak planlamalar yapıldığı görülmektedir. Ülkemizde ise TÜBİTAK ve Aselsan'ın kuantum teknolojileri ile kuantum güvenli iletişim alanındaki çalışmalarının henüz başlangıç aşamasında olduğu ve düzenleyici bir yaklaşımın mevcut olmadığı görülmektedir.

Bu kapsamda yerli ve milli kuantum güvenli kripto sistemlerin oluşturulmasının akabinde ABD tarafından oluşturulan Kuantum Güvenli Kriptografi Girişimine benzer şekilde ülkemizin kuantum güvenli kriptografik algoritmalara geçişi için gerekli planlamaların yapılmasının ve bir yol haritasının oluşturulmasının elzem olduğu değerlendirilmektedir.

5809 sayılı Elektronik Haberleşme Kanunu'nun 5'inci maddesinde yer alan *"Ulusal siber güvenliğin sağlanması amacıyla politika, strateji ve hedefleri belirlemek, kamu kurum ve kuruluşları ile gerçek ve tüzel kişilere yönelik siber güvenliğin sağlanmasına ilişkin usul ve esasları belirlemek, eylem planlarını hazırlamak, ..."* hükmü ile Ulaştırma ve Altyapı Bakanlığına siber güvenliğin sağlanmasında politika ve strateji belirlemek görevi verilmiş olup söz konusu strateji ve eylem planının Ulaştırma ve Altyapı Bakanlığı tarafından hazırlanabileceği, gerekli eylemlerin ise ülkemizin siber güvenliğine karşı siber ortamda ortaya çıkan tehditlerin belirlenmesi, muhtemel siber saldırı ve olayların etkilerini azaltılması veya ortadan kaldırılmasına yönelik önlemlerin geliştirilmesi ve belirlenen aktörlerle paylaşılması amacıyla BTK bünyesinde oluşturulan USOM önderliğinde ve USOM ile işbirliği halinde koordineli çalışmalar gerçekleştiren kamu kurum ve kuruluşları bünyesinde faaliyet gösteren Siber Olaylara Müdahale Ekipleri (Kurumsal SOME, Sektörel SOME) aracılığıyla gerçekleştirilebileceği değerlendirilmektedir.

Bu doğrultuda kamu kurum ve kuruluşlarının;

- Kuantum siber güvenlik tehditlerine karşı savunmasız olduğu ifade edilen kriptografik algoritmalarına yönelik tespit çalışmalarını gerçekleştirmesinin,
- Savunmasız olduğu değerlendirilen kriptografik algoritmaların hangi sistemlerde ve ne amaçla kullanıldığının analiz edilmesinin, (örneğin anahtar depoları, parolalar, kişisel bilgiler vb.)
- Sistemin kritik altyapı sektörlerini destekleyip desteklemediğinin, hangi sistemlerle iletişim halinde olduğunun, sistemde yer alan verilerin saklanması gerektiği sürelerin ve diğer kuruluşlarla ne oranda bilgi paylaşımı gerçekleştirdiğinin belirlenmesinin,

sağlanarak herhangi bir işlev için kriptografik teknolojileri kullanan tüm sistemlerin bir envanterinin oluşturulması gerekmektedir. Akabinde, kurumların bilgi teknolojileri

sistemlerini kuantum bilgisayarlardan gelen saldırılara karşı dayanıklı olan kuantum güvenli kriptografi algoritmalarına geçirebilmeleri için;

- USOM tarafından risk altında olan sistemlerin yer aldığı envanterin, envanterin önceliklendirilmesini sağlayacak kriterlerin ve raporlanması talep edilen bilgilere ilişkin açıklamanın yer aldığı bir kılavuzun yayımlanmasının,
- Yerli ve milli olarak geliştirilen kuantum güvenli kripto sistemlerin oluşturulmasının ardından ivedilikle her kurumun önceliklendirilmiş bilgi teknolojileri sistemlerinden başlamak üzere kuantum güvenli algoritmalara geçişe ilişkin USOM tarafından yayınlanacak kılavuz doğrultusunda bir plan belirlemesinin ve zaman çizelgesi bilgisi ile birlikte SOME'ler vasıtasıyla USOM'a iletmesinin,
- Süreklilik arz edecek şekilde kurumların kuantum güvenli kriptografik algoritmaları benimseme ve ilerlemelerine yönelik raporlamalarının devam etmesinin,
- Sürecin yerli ve milli kripto sistemlerin belirlenmesinden itibaren en geç 5 yıl içerisinde nihayetlendirilmesinin,

önem arz ettiği değerlendirilmektedir.

- **Kuantum iletişim teknolojilerine yönelik araştırma geliştirme ve ürün geliştirme faaliyetlerinin gerçekleştirilebilmesi için bir test ortamı oluşturulması önerilmektedir.**

Kuantum iletişim, kuantum mekaniği yasalarının kullanılarak; bilginin ve kuantum kaynaklarının güvenli bir şekilde iletilebilmesi amacıyla kuantum bilgisayarların, simülatörlerin ve sensörlerin birbirine bağlandığı bir iletişim ağını ifade etmektedir. Kuantum iletişim teknolojileri ile uzun vadede ulaşılmak istenen nihai hedef ise hataya dayanıklı kuantum bilgisayarlar geliştirmek, aynı zamanda bu bilgisayarları birbirine bağlamak ve aralarında kuantum bilgi alışverişi yapmak; aslında hem kuantum hesaplama hem de kuantum iletişim yeteneklerinden yararlanarak bir 'kuantum interneti' geliştirmektir. Kuantum iletişim teknolojilerini gerçekleştirmedeki ilk basamak ise kuantum anahtar dağıtım yönteminin uygulanmasıdır.

Bu doğrultuda, 5G ve Ötesi teknolojilerin araştırma geliştirme, ürün geliştirme ve testlerinin yapılabileceği açık bir test sahası olan "5G Vadisi Açık Test Sahası"na benzer şekilde kamu-üniversite-işletmeci-sanayi iş birliği ile kuantum iletişim teknolojilerine yönelik akademisyenler, araştırmacılar, doktora öğrencileri ve şirketlerin etkili araştırmalar ve projeler yürütmesine imkan tanıyacak bir platform oluşturulmasının, bu alanda yetiştirilecek nitelikli insan kaynağı ile dünya pazarlarında yer alacak yerli ve milli katma değeri yüksek ürün ve teknolojilerin geliştirilmesinin teşvik edilmesinin ülkemizin kuantum teknolojilerinde yaşanan gelişmeleri ve fırsatları yakalaması ile söz konusu teknolojilerin yerli ve milli olarak geliştirilmesinde önem arz ettiği değerlendirilmektedir.

KAYNAKLAR

A. Aguado, V. L.-M. (2018). VPN service provisioning via virtual router deployment and quantum key distribution. *Optical Fiber Communication Conference.* San Diego, USA.

A. I. Nurhadi, N. R. (2018). Quantum Key Distribution (QKD) Protocols: A Survey. *2018 4th International Conference on Wireless and Telematics (ICWT)*, s. 1-5. doi:10.1109/ICWT.2018.8527822

A. K. Pandey, A. B. (2023). Cryptographic Challenges and Security in Post Quantum Cryptography Migration: A Prospective Approach. *2023 IEEE International Conference on Public Key Infrastructure and its Applications (PKIA)*, s. 1-8. doi:10.1109/PKIA58446.2023.10262706

A. Sharma, S. K. (2013). Authentication in online banking systems through quantum cryptography. *International Journal of Engineering Technologies, 5*(3), s. 2696-2700.

A. Singh, K. D. (2021). Quantum Internet—Applications, Functionalities, Enabling Technologies, Challenges, and Research Directions. *IEEE Communications Surveys & Tutorials, 23*(4), s. 2218-2247. doi:10.1109/COMST.2021.3109944

A. Singh, K. D. (2021). Quantum Internet—Applications, Functionalities, Enabling Technologies, Challenges, and Research Directions. *IEEE Communications Surveys & Tutorials, 23*(4), s. 2218-2247. doi:10.1109/COMST.2021.3109944

Al-Ehwany, A. F. (1961). *Al-Kindi" in A History of Muslim Philosophy.* New Delhi: Low Price Publication.

Amer, O., & vd. (2020). Efficient Routing for Quantum Key Distribution Networks. *2020 IEEE International Conference on Quantum Computing and Engineering (QCE)*, (s. 137-147). doi:10.1109/QCE49297.2020.00027

Andres, J. (2014). *The Basics of Information Security.*

Armengol, J. M. (2008). Quantum communications at ESA: Towards a space experiment on the ISS. *Acta Astronautica, 63*, s. 165-178.

ASELSAN. (2022). *Kripto ve Bilgi Güvenliği Çözümlerimiz*. https://www.aselsan.com/tr/blog/detay/319/kripto-ve-bilgi-guvenligi-cozumlerimiz

ASELSAN. (2023). *Aviyonik Siber Güvenlik*. https://www.aselsan.com/tr/blog/detay/377/aviyonik-siber-guvenlik

ASELSAN. (2023). *Hakkımızda*. https://www.aselsan.com/tr/hakkimizda

ASELSAN. (2023). *Kuantum Teknolojileri*. https://www.aselsan.com/tr/arge/kuantum-teknolojileri

Aslan, F. (2020). Nesnelerin İnterneti Uygulamalarının Güvenliği İçin Hafif Sıklet Kriptografik Algoritmaların Analizi ve Güvenli Akıllı Bir Platform Uygulaması. *Yükseköğretim Kurulu*, s. 44.

Aspect, A. (2015). Closing the Door on Einstein and Bohr's Quantum Debate. *Physics*. https://physics.aps.org/articles/v8/123

Avrupa Komisyonu. (2021). 2030 Digital Compass: the European way for the Digital Decade. https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A52021DC0118

Avrupa Komisyonu. (2022). *A Secure Quantum Communications Infrastructure for Europe:Technical background for a policy vision.* https://publications.jrc.ec.europa.eu/repository/handle/JRC129425

Avrupa Komisyonu. (2023). *Commission Recommendation on critical technology areas for the EU's economic security for further risk assessment with Member States,C(2023) 6689 final.* https://defence-industry-space.ec.europa.eu/system/files/2023-10/C_2023_6689_1_EN_ACT_part1_v8.pdf

Avrupa Komisyonu. (2023). *European Economic Security Strategy, JOIN(2023) 20 final.* https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52023JC0020

Avrupa Komisyonu. (2023). *European Quantum Communication Infrastructure-EuroQCI Initiative*. https://digital-strategy.ec.europa.eu/en/policies/european-quantum-communication-infrastructure-euroqci

AvrupaBirliği. (2023). EU secure connectivity programme)-EU 2023/588. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32023R0588

AvrupaKomisyonu. (2020). *Strategic Research Agenda.* https://digital-strategy.ec.europa.eu/en/news/new-strategic-research-agenda-quantum-technologies

AvrupaKomisyonu. (2021). 2030 Digital Compass: the European way for the Digital Decade. https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A52021DC0118

AvrupaKomisyonu. (2023). *European Declaration on Quantum Technologies.* https://digital-strategy.ec.europa.eu/en/library/european-declaration-quantum-technologies

AvrupaKomisyonu. (2023). *Quantum Technologies Flagship*. https://digital-strategy.ec.europa.eu/en/policies/quantum-technologies-flagship

AvrupaKomisyonu. (2023). *The Digital Europe Programme*. https://digital-strategy.ec.europa.eu/en/activities/digital-programme

AWS, A. (2023). *Searchable encryption*. https://docs.aws.amazon.com/database-encryption-sdk/latest/devguide/searchable-encryption.html

Babaoğlu, A. (2009). Kriptolojinin Geçmişi. *Bilim ve Teknik*(500), s. 24-27.

BAE. (2023). *What is Quantum Sensing?* 09 28, 2023 tarihinde BAE Systems: https://www.baesystems.com/en-us/definition/what-is-quantum-sensing#:~:text=Quantum%20Sensing%20is%20an%20advanced,collected%20at%20the%20atomic%20level

Bennett, C. (1992). Quantum Cryptography using any two Nonorthogonal Sates. *Physical review letters, 68*, s. 3121-3124.

Bikku, T., Praveen, P., & Sirisha, U. (2024). Enhancing Real Time Malware Analysis with Quantum Neural Networks. *Journal of Intelligent Systems and Internet of Things*. doi:10.54216/JISIoT.120105

Boaron, A. (2018). Secure quantum key distribution over 421 km of optical fiber. *Physical Review Letters, 121*(19).

Bouwmeester, P., Mattle, K., & Zeilinger, A. (1997). Experimental quantum teleportation. *Nature*, s. 575-579. doi:10.1038/37539

Britannica. (2023). *Playfair Cipher*. 05 18, 2023 tarihinde https://www.britannica.com/topic/Playfair-cipher

Britannica. (2024). *Colossus.* https://www.britannica.com/technology/Colossus-computer

Britannica. (2024). *Enigma.* https://www.britannica.com/topic/casualties-of-World-War-II-2231003

C.H. Bennett, G. B. (2014). Quantum cryptography: Public key distribution and coin tossing. *Theoretical Computer Science, 560*(7-11).

Caceres, M., Robichaux, T., & D., F. (2009). *Next Generation SSH2 Implementation: Securing Data in Motion.* Syngress. doi:10.1016/B978-1-59749-283-6.X0001-3

Camilo, B., Couto, R., & Costa, H. (2017). Assessing the impacts of IPsec cryptographic algorithms on a virtual network embedding problem. *Computers and Electrical Engineering*, s. 1-16. doi:10.1016/j.compeleceng.2017.06.025

C-DOT. (2021). *Secretary Telecom Shri K. Rajaraman visits C-DOT*. https://pib.gov.in/PressReleaseIframePage.aspx?PRID=1762590

Chen, Y. (2018). Large-scale quantum network: From intra-city to intercity to global. *8th International Conference on Quantum Cryptography*, s. 1-14.

Chen, Y. Z. (2021). An integrated space-to-ground quantum communication network over 4,600 kilometres. *Nature*(589), s. 214-219. doi:https://doi.org/10.1038/s41586-020-03093-8

Chen, Y.-A. (2018). Large-scale quantum network: From intra-city to intercity to global. *8th International Conference on Quantum Cryptography*, s. 1-14.

Chen, Y.-A. (2021). An integrated space-to-ground quantum communication network over 4,600 kilometres. *Nature, 589*(7841), s. 214-219.

CISA. (2021). *Preparing for Post-Quantum Cryptography.* https://www.dhs.gov/sites/default/files/publications/post-quantum_cryptography_infographic_october_2021_508.pdf

CISA. (2022). *Post-Quantum Cryptography Initiative*. https://www.cisa.gov/news-events/news/cisa-announces-post-quantum-cryptography-initiative

Clauser, J., Shimony, A., Holt, R., & Horne, M. (1969). Proposed Experiment to Test Local Hidden-Variable Theories. *Physical Review Letters, 23*(15).

CNAS. (2018). *China's Quantum Future*. Center for a New American Security: https://www.cnas.org/publications/commentary/chinas-quantum-future

Cohen, F. (1995). *A shor History of Cryptography.* http://all.net/edu/curr/ip/Chap2-1.htm

Colvin, D. P. (2005). Current status of the DARPA quantum network. *Quantum Information and Computation, 3*(5815), s. 138–150.

Congress.gov. (2022). *Public Law 117-260, H.R.7535.* https://www.congress.gov/117/plaws/publ260/PLAW-117publ260.pdf

CRYPTEC. (2023). *CRYPTREC Ciphers List*. https://www.cryptrec.go.jp/en/list.html

CRYPTEC. (2023). *Organization of CRYPTREC*. https://www.cryptrec.go.jp/en/system.html

CRYPTREC. (2023). *Interviews-CRYPTREC Project.* NICT. https://sfl.nict.go.jp/en/interview/cryptrec.html

CSA, S. (2024). Transport Layer Security (TLS): https://www.csa.gov.sg/Tips-Resource/internet-hygiene-portal/information-resources/tls

CSET. (2021). *Outline of the People's Republic of China 14th Five-Year Plan for National Economic and Social Development and Long-Range Objectives for 2035*. Center for Security and Emerging Technology: https://cset.georgetown.edu/wp-content/uploads/t0284_14th_Five_Year_Plan_EN.pdf

D.J. Bernstein, J. B. (2009). Post-Quantum Cryptography. *Springer*.

Das, M. L., & Samdaria, N. (2014). On the security of SSL/TLS-enabled applications. *Applied Computing and Informatics*, s. 68-81. doi:10.1016/j.aci.2014.02.001

Dhanush, C. S., & Jain, K. (2023). Comparison of Post-Quantum Cryptography Algorithms for Authentication in Quantum Key Distribution Classical Channel. *2023 Second International Conference on Augmented Intelligence and Sustainable Systems (ICAISS)* (s. 1219-1225). IEEE. doi:10.1109/ICAISS58487.2023.10250627

DST. (2020). *Budget 2020 announces Rs 8000 cr National Mission on Quantum Technologies & Applications*. Department of Science & Technology: https://dst.gov.in/budget-2020-announces-rs-8000-cr-national-mission-quantum-technologies-applications

Dubrawsky, I. (2007). *Security+ Study Guide.* Syngress.

Ekert, A. (1991). Quantum cryptography based on Bell's theorem. *Physical review letters, 67*, s. 661-663.

ENISA. (2021). *Post-Quantum Cryptography Current State and Quantum Mitigation.* ENISA. https://www.enisa.europa.eu/publications/post-quantum-cryptography-current-state-and-quantum-mitigation

ENISA. (2021). *Post-Quantum Cryptography: Current state and quantum mitigation.*

ENISA. (2022). *Post-Quantum Cryptography: Integration study.* https://www.enisa.europa.eu/publications/post-quantum-cryptography-integration-study

ENISA. (2023). *About ENISA.* https://www.enisa.europa.eu/about-enisa

ESA. (2023). *European Space Agency*. https://www.esa.int/

ETSI. (2010). *ETSI GS QKD 002-Quantum Key Distribution (QKD); Use Cases.* 12 11, 2023 tarihinde https://www.etsi.org/deliver/etsi_gs/qkd/001_099/002/01.01.01_60/gs_qkd002v010101p.pdf

ETSI. (2010). *ETSI GS QKD 004-Quantum Key Distribution Application Interface.* 12 10, 2023 tarihinde https://www.etsi.org/deliver/etsi_gs/QKD/001_099/004/01.01.01_60/gs_QKD004v010101p.pdf

ETSI. (2010). *ETSI GS QKD 005- Quantum Key Distribution; Security Proofs.* 12 11, 2023 tarihinde https://www.etsi.org/deliver/etsi_gs/QKD/001_099/005/01.01.01_60/gs_QKD005v010101p.pdf

ETSI. (2010). *ETSI GS QKD 008-Quantum Key Distribution; QKD Module Security Specification.* 12 11, 2023 tarihinde https://www.etsi.org/deliver/etsi_gs/QKD/001_099/008/01.01.01_60/gs_QKD008v010101p.pdf

ETSI. (2015). *Quantum Safe Cryptography and Security- An introduction, benefits, enablers and challenges.*

ETSI. (2016). • *ETSI GS QKD 011- Quantum Key Distribution (QKD) Component Characterization: Characterizing Optical Components for QKD Systems.* 12 11, 2023 tarihinde https://www.etsi.org/deliver/etsi_gs/QKD/001_099/011/01.01.01_60/gs_QKD011v010101p.pdf

ETSI. (2017). *ETSI GR QSC 006-Quantum-Safe Cryptography.* https://www.etsi.org/deliver/etsi_gr/QSC/001_099/006/01.01.01_60/gr_QSC006v010101p.pdf

ETSI. (2018). *ETSI GR QKD 003-Quantum Key Distribution; Components and Internal Interfaces.* 12 11, 2023 tarihinde alındı

ETSI. (2018). *ETSI GR QKD 007- Quantum Key Distribution (QKD); Vocabulary.* 12 11, 2023 tarihinde https://www.etsi.org/deliver/etsi_gr/QKD/001_099/007/01.01.01_60/gr_QKD007v010101p.pdf

ETSI. (2018). *Implementation Security of Quantum Cryptography: Introduction, challenges, solutions.* ETSI White Paper No.27. https://www.etsi.org/images/files/ETSIWhitePapers/etsi_wp27_qkd_imp_sec_FINAL.pdf

ETSI. (2019). *ETSI GS QKD 012- Quantum Key Distribution; Device and Communication Channel Parameters for QKD Deployment.* 12 11, 2023 tarihinde https://www.etsi.org/deliver/etsi_gs/QKD/001_099/012/01.01.01_60/gs_QKD012v010101p.pdf

ETSI. (2019). *ETSI GS QKD 014-Quantum Key Distribution; Protocol and data format of REST-based key delivery API.* 12 11, 2023 tarihinde https://www.etsi.org/deliver/etsi_gs/QKD/001_099/014/01.01.01_60/gs_QKD014v010101p.pdf

ETSI. (2020). *ETSI GS QKD 004-Quantum Key Distribution(QKD); Application Interface.* 12 11, 2023 tarihinde https://www.etsi.org/deliver/etsi_gs/QKD/001_099/004/02.01.01_60/gs_QKD004v020101p.pdf

ETSI. (2021). *ETSI GS QKD 015- Quantum Key Distribution; Control Interface for Software Defined Networks.* 12 11, 2023 tarihinde https://www.etsi.org/deliver/etsi_gs/QKD/001_099/015/01.01.01_60/gs_QKD015v010101p.pdf

ETSI. (2022). *ETSI GS QKD 018- Quantum Key Distribution; Orchestration Interface for Software Defined Networks.* 12 11, 2023 tarihinde https://www.etsi.org/deliver/etsi_gs/QKD/001_099/018/01.01.01_60/gs_QKD018v010101p.pdf

ETSI. (2023). *ETSI GS QKD 016-Quantum Key Distribution; Common Criteria Protection Profile - Pair of Prepare and Measure Quantum Key*

Distribution Modules. 12 11, 2023 tarihinde https://www.etsi.org/deliver/etsi_gs/QKD/001_099/016/01.01.01_60/gs_QKD016v010101p.pdf

EuropenCommission. (2016). *Quantum Manifesto-A New Era of Technology.* http://qurope.eu/system/files/u7/93056_Quantum%20Manifesto_WEB.pdf

F. Mallouli, A. H. (2019). A Survey on Cryptography: Comparative Study between RSA vs ECC Algorithms, and RSA vs El-Gamal Algorithms. *2019 6th IEEE International Conference on Cyber Security and Cloud Computing (CSCloud)/ 2019 5th IEEE International Conference on Edge Computing and Scalable Cloud (EdgeCom)*. doi:10.1109/CSCloud/EdgeCom.2019.00022

Fernández-Caramés, T. M. (2020). From pre-quantum to post-quantum IoT security: A survey on quantum-resistant cryptosystems for the Internet of Things. *IEEE Internet of Things Journal, 7*(7), s. 6457-6480.

Freedman, S., & Clauser, J. (1972). Experimental Test of Local Hidden-Variable Theories. *Physical Review Letters, 28*(14).

Georgescu, I., Ashhab, S., & Nori, F. (2014). Quantum simulation. *Reviews of Modern Physics*, s. 153-185. doi:10.1103/revmodphys.86.153

Grimes, R. A. (2020). *Cryptography Apocalypse: Preparing for the Day When Quantum Computing Breaks Today's Crypto.* John Wiley & Sons.

Grindlay, B. ,. (2003). *Quantum Cryptography; A study into the present technologies and future applications.* Next Generation Security Software: https://research.nccgroup.com/wp-content/uploads/2020/07/quantum_cryptography_-_a_study_into_present_technologies_and_future_applications.pdf

Grover, L. (1996). *A Fast Quantum Mechanical Algorithm For Database Search.* Teknik Rapor, Bell Labs, New Jersey.

GSMA. (2023). *About us*. https://www.gsma.com/aboutus/

GSMA. (2023). *Guidelines for Quantum Risk Management for Telco.* https://www.gsma.com/get-involved/working-groups/wp-content/uploads/2023/09/Guidelines-for-Quantum-Risk-Management-for-Telco-v1.0.pdf

GSMA. (2023). *Post Quantum Telco Network Impact Assessment Whitepaper.* https://www.gsma.com/newsroom/wp-content/uploads//PQ.1-Post-Quantum-Telco-Network-Impact-Assessment-Whitepaper-Version1.0.pdf

Guo , H., & Yu, X. (2022). A survey on blockchain technology and its security. *Blockchain: Research and Applications*. doi:10.1016/j.bcra.2022.100067

H.B. Pasquinucci, N. G. (1999). Incoherent and coherent eavesdropping in the six-state protocol of quantum cryptography. *Physical Review Letter, A59*, s. 4238-4248.

He-Liang Huang, D. W. (2020). Superconducting Quantum Computing: A Review.

IBM. (2023). *7.5 Security Cryptography.* https://www.ibm.com/docs/en/ssw_ibm_i_75/pdf/rzajcpdf.pdf

IBM. (2023). *How to quantum computers work?* 10 5, 2023 tarihinde https://www.ibm.com/topics/quantum-computing#Where+are+quantum+computers+used%3F%09%09%09%09%09%09%09

IBM. (2023). *How to quantum computers work?* 10 5, 2023 tarihinde https://www.ibm.com/topics/quantum-computing

IBM. (2024). *Know about the Caesar Cipher, one of the earliest known and simplest ciphers.* https://community.ibm.com/community/user/ibmz-and-linuxone/blogs/subhasish-sarkar1/2020/07/04/caesar-cipher

IDB, I.-A. (2019). *Quantum Technologies; Digital transformation, social impact and cross-sector disruption.* IDB.

IDQ, S. Q. (tarih yok). Securing Data Transfer for Elections: Ethernet Encryption with Quantum Key Distribution. https://marketing.idquantique.com/acton/attachment/11868/f-020f/1/-/-/-/-/Geneva%20Govt_%20DCI%20QKD%20Use%20Case.pdf

IEC. (2023). *Who we are.* https://iec.ch/who-we-are

İlter, M. B., & Çetin, S. (2020, 8). *ASELSAN*(106), s. 73. https://wwwcdn.aselsan.com/api/file/AselsanDergi106_1276.pdf

ISO. (2023). *About us.* https://www.iso.org/about-us.html

ISO. (2023). *ISO/IEC 23837-1 Information security- Security requirements, test and evaluation methods for quantum key distribution, Part 1: Requirements.* https://www.iso.org/standard/77097.html

ISO. (2023). *ISO/IEC 23837-1 Information security- Security requirements, test and evaluation methods for quantum key distribution, Part 2: Evaluation and testing methods.* https://www.iso.org/standard/77309.html

ISRO. (2023). *Department of Space demonstrates entanglement based quantum communication over 300m free space along with real time cryptographic applications*. Indian Space Research Organisation: https://www.isro.gov.in/DeptofSpace.html

Kaaniche, N., & Laurent, M. (2017). Data security and privacy preservation in cloud storage environments based on cryptographic mechanisms. *Computer Communications*, s. 120-141.

Kara, O. (2009). 2. Dünya Savaşından Günümüze Kriptoloji: Enigma'dan AES'e Şifreleme. *Bilim ve Teknik*.

Kessler, G. C. (2015). An Overview of Cryptography. https://www.cs.princeton.edu/~chazelle/courses/BIB/overview-crypto.pdf

Kiktenko, E. O. (2018). Quantum-secured blockchain. *Quantum Science and Technology, 3*(3).

Kleppner, D., & Jackiw, R. (2000). One Hundred Years of Quantum Physics. *Science, 289*(5481), s. 893-898. https://www.ifi.unicamp.br/~mtamash/f689_mecquant_i/science289_893.pdf

Kohlios, C. P., & Hayajneh, T. A. (2018). A Comprehensive Attack Flow Model and Security Analysis for Wi-Fi and WPA3. *Electronics*. doi:10.3390/electronics7110284

KPN. (2016). *KPN to Implement Quantum Encrypted Connection (QKD).* https://www.overons.kpn/nieuws/en/kpn-to-implement-quantum-encrypted-connection-qkd

Kumar, M. (2022). Post-quantum cryptography Algorithm's standardization and performance analysis. *Array, 15*(100242). doi:10.1016/j.array.2022.100242

L. Huang, H. Z. (2021). Quantum random number cloud platform. *NPJ Quantum Information, 7*, s. 107.

Liao, S.-K. (2017). Satellite-to-ground quantum key distribution. *Nature, 549*(7670), s. 43-47.

LibreTexts. (2023). *Atoms and Photons: Origin of Quantum Theory.* LibreTexts Chemistry: https://chem.libretexts.org/Bookshelves/Physical_and_Theoretical_Chemistry_Textbook_Maps/Supplemental_Modules_(Physical_and_Theoretical_Chemistry)/Quantum_Mechanics/01._Waves_and_Particles/Chapter_1%3A_Atoms_and_Photons%3A_Origin_of_Quantum_Theory

M. Ajtai, C. D. (1997). A public-key cryptosystem with worstcase/average-case equivalence. *ACM Symposium on Theory of Computing (STOC 97)*.

M. Niemiec, P. M. (2016). Authentication in virtual private networks based on quantum key distribution methods. *Multimedia Tools and Applications, 75*(17), s. 10691-10707.

M3 LAB. (2023). *Biz Kimiz?* https://ma3.bilgem.tubitak.gov.tr/biz-kimiz/

Mermin, N. (1992). Quantum cryptography without Bell's theorem. *Physical review letters, 68*, s. 557-559.

Microsoft. (2018, 09). *Micdosoft Azure Quantum Blog*. 10 09, 2023 tarihinde https://cloudblogs.microsoft.com/quantum/2018/09/06/developing-a-topological-qubit/

MoD. (2021). *Indian Army Establishes Quantum Laboratory at Mhow*. Ministry of Defence: https://pib.gov.in/PressReleasePage.aspx?PRID=1786012

Mohamed, K. S. (2020). *New Frontiers in Cryptography.* doi:10.1007/978-3-030-58996-7_2

Moissinac, K., Ramos, D., Elleithy, A., & Rendon, G. (2021). Wireless Encryption and WPA2 Weaknesses. *2021 IEEE 11th Annual Computing and Communication Workshop and Conference (CCWC)*, s. 1007-1015. doi:10.1109/CCWC51732.2021.9376023

National Security Agency. (2023). *QUANTUM KEY DISTRIBUTION (QKD) AND QUANTUM CRYPTOGRAPHY QC*. https://www.nsa.gov/Cybersecurity/Quantum-Key-Distribution-QKD-and-Quantum-Cryptography-QC/

NIST. (2021). *Getting Ready for Post-Quantum Cryptography: Exploring Challenges Associated with Adopting and Using Post-Quantum Cryptographic Algorithms.* doi:10.6028/NIST.CSWP.04282021

NIST. (2021). *Introduction to Public Key Technology and the Federal PKI Infrastructure.* https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-32.pdf

NIST. (2022). *NIST IR 8413 Status Report on the Third Round of the NIST Post-Quantum Cryptography Standardization Process.* doi:https://doi.org/10.6028/NIST.IR.8413-upd1

NIST. (2022). *Post-Quantum Cryptography, Security*. https://csrc.nist.rip/projects/post-quantum-cryptography/post-quantum-cryptography-standardization/evaluation-criteria/security-(evaluation-criteria)

NIST. (2023). *Digital Signature Standard (DSS).* doi:10.6028/NIST.FIPS.186-5

NIST 800-131A, N. I. (2015). *Special Publication (SP) 800-131A Revision 1, Transitions: Recommendation for Transitioning the Use of Cryptographic Algorithms and.* doi:http://dx.doi.org/10.6028/nist.sp.800-131ar1

NQCO, N. Q. (2023). *About the National Quantum Initiative*. https://www.quantum.gov/about/#LEGISLATION

O. Elmabrok, M. R. (2018). Wireless quantum key distribution in indoor environments. *Journal of the Optical Society of America B, 35*(2), s. 197-207.

Pirandola, S., Andersen, U., & Banchi, L. (2020). Advances in quantum cryptography. *Advences in Optics and Photonics*, s. 1012-1236.

Poppe, A. (2004). Practical quantum key distribution with polarization entangled photons. *Optics Express, 12*(16), s. 3865-3871.

Princy, M. J. (2015). A COMPARISON OF SYMMETRIC KEY ALGORITHMS DES, AES, BLOWFISH, RC4, RC6: A SURVEY. https://api.semanticscholar.org/CorpusID:61177706

Q. Zhang, F. X. (2019). Quantum information research in China. *Quantum Science and Technology, 4*(4).

QApp. (2023). *CACR post-quantum competition*. 12 18, 2023 tarihinde https://en.qapp.tech/help/cacr

Qin, H. (2019). Towards large-scale quantum key distribution network and its applications. *ITU Workshop on Quantum Information Technology Networks.* Shanghai, China.

QuantERA. (2023). *About QuantERA*. https://quantera.eu/about/

Raggo, M., & Hosmer, C. (2013). *Data Hiding.* Syngress. doi:10.1016/B978-1-59-749743-5.00001-8

S. Akyelek, M. (2019). Kuantum Bilgisayarlar ile Kriptoanaliz ve Kuantum Sonrası Güvenilir Kripto Sistemleri. *Siber Güvenlik ve Savunma*, s. 137-168.

S. F. Al-Janabi, A. K. (2012). Development of Certificate Authority services for web applications. *2012 International Conference on Future Communication Networks*. doi:10.1109/ICFCN.2012.6206857

S. Ghernaouti-Hélie, M. A. (2005). Guaranteerring security of financial transaction by using quantum cryptography in banking environment. *International Conference on E-Business and Telecommunication Networks, 3*, s. 139-149. doi:10.1007/978-3-540-75993-5_12

Sahinaslan, E. &. (2019). Cryptographic methods and development stages used throughout history. *AIP Conference Proceedings, 2086*(1).

Salva, R. P. (2023). Annealing Quantum Computing: An Overview. doi:https://dx.doi.org/10.2139/ssrn.4501788

Settia, N. (2010). Cryptanalysis of Modern Cryptographic Algorithms. *International Journal of Computer Science and Technology, 1*(2).

Shara, J. (2023). Quantum Machine Learning and Cybersecurity. *International Journal of Engineering Inventions*. https://www.researchgate.net/publication/371367309

Shor, P. W. (1994). Algorithms for quantum computation: discrete logarithms and factoring. *Proceedings of the 35th Annual Symposium on Foundations of Computer Science*, s. 124-134.

Shor, P. W. (1994). Algorithms for Quantum Computation: Discrete Logarithms and Factoring. *Proceedings 35th annual symposium on foundations of computer science* , s. 124-134.

Singh, A., & Patro, K. (2019). Security of Low Computing Power Devices: A Survey of Requirements, Challenges & Possible Solutions. *Cybernetics and Information Technologies*. doi:http://dx.doi.org/10.2478/cait-2019-0008

Singh, P., & Chauhan, R. (2017). A Survey on Comparisons of Cryptographic Algorithms Using Certain Parameters in WSN. *International Journal of Electrical and Computer Engineering (IJECE)*. doi:10.11591/ijece.v7i4.pp2232-2240

Singh, S. (2000). *The code book: the science of secrecy from ancient Egypt to quantum cryptography.* Anchor Books.

Stallings, W. (2011). *Cryptography and Network Security.* Boston: Prentice Hall.

T. M. Fernández-Caramès, P. F.-L. (2020). Towards post-quantum blockchain: A review on blockchain cryptography resistant to quantum. *IEEE Access, 8*, s. 21091-21116.

Tattersall, J. (1999). *Elementary Number Theory in Nine Chapters.* Cambridge: Cambridge University Press. doi:10.1017/CBO9780511756351

TÜBİTAK. (2023). *Biz Kimiz?* https://www.tubitak.gov.tr/tr/kurumsal/hakkimizda/icerik-biz-kimiz

TÜBİTAK. (2023). *Test ve Değerlendirme Direktörlüğü Laboratuvarları*. TÜBİTAK BİLGEM: https://bilgem.tubitak.gov.tr/laboratuvarlar/tdd-laboratuvarlari/

TÜBİTAK BİLGEM. (2022). *Kuantum Bilgisayarların Güvenli İletişim Üzerine Olumsuz Etkileri ve Alınacak Önlemler*. https://bilgem.tubitak.gov.tr/kuantum-bilgisayarlarin-guvenli-iletisim-uzerine-olumsuz-etkileri-ve-alinacak-onlemler/

TürkNet. (2023). *Dark Fiber Nedir?* https://turk.net/blog/dark-fiber-nedir/

UEKAE. (2023). *Biz Kimiz?* https://bilgem.tubitak.gov.tr/uekae-kurumsal/

UEKAE. (2023). *Kuantum Teknolojileri*. https://bilgem.tubitak.gov.tr/kuantum-teknolojileri/

V. Scarani, A. A. (2004). Quantum cryptography protocols robust against photon number splitting attacks for weak laser pulse implementations. *Physical Review Letters, 92*.

Vasileios, K. V. (2018). The Impact of Quantum Computing on Present Cryptography. *International Journal of Advanced Computer Science and Applications (IJACSA), 9*(3). doi:https://doi.org/10.48550/arXiv.1804.00200

Vazirani, U. (1998). On The Power of Quantum Computation. *Philosophical Transactions of the Royal Society of London A: Mathematical, Physical and Engineering Sciences, 356*(1743), s. 1759-1768.

Wang, L., Yang, J., & Wan, P.-J. (2020). Educational modules and research surveys on critical cybersecurity topics. *International Journal of Distributed Sensor Networks*. doi:10.1177/1550147720954678

Wang, Y. (2020). Analysis on the Mechanism of Superconducting Quantum Computer. *Journal of Physics: Conference Series*.

Wikipedia. (2024). *Alberti Cipher.* https://en.wikipedia.org/wiki/Alberti_cipher

Wikipedia. (2024). *One-time pad.* https://en.wikipedia.org/wiki/One-time_pad

Wikipedia. (2024). *Scytale.* https://en.wikipedia.org/wiki/Scytale

Wikipedia. (2024). *Vigenere Cipher.* https://en.wikipedia.org/wiki/Vigen%C3%A8re_cipher

X. Sun, M. S. (2019). Towards quantum-secured permissioned blockchain: Signature, consensus, and logic. *Entropy, 21*(9), s. 887.

Y. Cao, Y. Z. (2022). The Evolution of Quantum Key Distribution Networks: On the Road to the Qinternet. *IEEE Communications Surveys & Tutorials, 24*(2), s. 839-894. doi:10.1109/COMST.2022.3144219

Yang, S., Piao, H., & Zhang, L. (2007). An Improved IDEA Algorithm Based on USB Security Key. *Third International Conference on Natural Computation*. doi:10.1109/ICNC.2007.214

Yang, Y. (2021). All optical metropolitan quantum key distribution network with post-quantum cryptography authentication. *Optics Express, 29*(16), s. 25859-25867.

Yang, Z., Zolanvari, M., & Jain, R. (2023). A Survey of Important Issues in Quantum Computing and Communications. *IEEE COMMUNICATIONS SURVEYS & TUTORIALS, 25*(2).

Yi, X., Paulet, R., & Bertino, E. (2014). Homomorphic Encryption. *Homomorphic Encryption and Applications*. doi:https://doi.org/10.1007/978-3-319-12229-8_2

Z. Yang, M. Z. (2023). A Survey of Important Issues in Quantum Computing and Communications. *IEEE Communications Surveys & Tutorials, 25*(2), s. 1059-1094. doi:10.1109/COMST.2023.3254481.

Zhang, Q. (2015). Quantum network in China. *Updating Quantum Cryptography and Communications (UQCC 2015)*.

Zhang, Q., & Xu, F. (2018). Large scale quantum key distribution: Challenges and solutions. *Optics Express, 26*(18), s. 24260-24273.

Zhang, Q., He, Y., Lai, R., Hou, Z., & Zhao, G. (2023). A survey on the efficiency, reliability, and security of data query in blockchain systems. *Future Generation Computer Systems* , s. 303-320.

ÖZGÜNLÜK BİLDİRİMİ

Uzmanlık tezi olarak sunduğum bu çalışmayı, bilimsel ahlak ve geleneklere aykırı düşecek bir yol ve yardıma başvurmaksızın yazdığımı, yararlandığım eserlerin kaynakçada gösterilenlerden oluştuğunu, bunlardan her seferinde değinme yaparak yararlandığımı ve Bilgi Teknolojileri ve İletişim Kurumu Meslek Personeli Yönetmeliğine uygun olarak hazırladığımı belirtir, bunu onurumla doğrularım.

Bilgi Teknolojileri ve İletişim Kurumu tarafından belli bir zamana bağlı olmaksızın, tezimle ilgili yaptığım bu beyana aykırı bir durumun saptanması durumunda, ortaya çıkacak tüm ahlaki ve hukuki sonuçlara katlanacağımı bildiririm.

Elif YILDIRIMLI AYDINLI

ÖZGEÇMİŞ

1994 yılında İzmir'de doğdu. İlk öğrenimini İzmir Hakimiyet-i Milliye İlkokulu'nda, orta öğrenimini İzmir Misak-ı Milli Ortaokulu'nda, lise öğrenimini İzmir Buca Anadolu Lisesi'nde tamamladı. 2018 yılında Gazi Üniversitesi Endüstri Mühendisliği Bölümü'nden mezun oldu. 2020 yılının Eylül ayında Bilgi Teknolojileri ve İletişim Kurumu Bilgi Teknolojileri Dairesi Başkanlığı'nda Bilişim Uzman Yardımcısı olarak çalışmaya başladı. 2023 yılı Ekim ayından itibaren Gazi Üniversitesi Bilişim Sistemleri Bölümü'nde Yüksek Lisans eğitimine devam etmektedir.