Kuantum Kriptolojisi ve Siber Güvenlik

Literatür Makalesi/Review Article

Sadullah ÇELİK

Ekonometri Bölümü, Aydın Adnan Menderes Üniversitesi, Aydın, Türkiye
ssadullah.celik@gmail.com
(Geliş/Received:06.05.2020; Kabul/Accepted:25.12.2020)
DOI: 10.17671/gazibtd.733309

Özet— Bu çalışmanın amacı gelişen kuantum teknolojilerinin siber güvenlik sisteminde kullanılan şifreleme sistemlerini nasıl etkileyeceğini kuantum algoritmalarıyla açıklamaktır. Bu amaçla, çalışmada öncelikle, modern kriptografi de yaygın olarak kullanılan bazı algoritmalar verilmektedir. Daha sonra, kuantum bilgisayarlarda kullanılan Shor ve Grover algoritmalarının modern kriptografide kullanılan algoritmaları nasıl etkileyeceği hakkında bilgiler verilmektedir. Bilişim ve iletişim teknolojilerinde yaşanan son gelişmeler, üretilen ve saklanan bilginin miktarında ve hızında büyük artışa sebep olmuştur. Bilgi miktarındaki bu artış beraberinde birtakım güvenlik sorunlarını da ortaya çıkarmıştır. İşletmeler, bankalar, devlet kurumları ve diğer kuruluşların güvenlik sistemleri, zor matematiksel problemlerin çözülmesi esasına dayanmaktadır. Bu problemlerin çözülmesi, en güçlü bilgisayarlar ve modern algoritmalar kullanılsa bile çok uzun zaman almaktadır. Literatürde yapılan çalışmalarda bugün için kuantum bilgisayarların güvenlik açısından çok büyük tehlikeler oluşturmadığını göstermektedir. Ancak bilim insanları, kuantum hesaplamanın beklenenden daha hızlı gelişeceğini ve büyük güvenlik zafiyetlerini ortaya çıkaracağını ön görüyor. Bu nedenle yakın gelecekte birçok kuruluşun şifreleme sistemleri ciddi siber güvenlik sorunlarıyla karşı karşıya kalacaktır. Gerek devletlerin gerekse özel sektörün bu tehlikeleri bugünden ön görerek gelecekte ortaya çıkabilecek güvenlik sorunlarına şimdiden hazır olmaları gerekir.

Anahtar Kelimeler— kuantum kriptolojisi, siber güvenlik, Shor algoritması, Grover algoritması

Quantum Cryptology and Cyber Security

Abstract— This study aims to explain how developing quantum technologies will affect the encryption systems used in the cyber security system with quantum algorithms. For this purpose, first of all, some algorithms commonly used in modern cryptography are given. Then, information is given about how Shor and Grover algorithms used in quantum computers will affect the algorithms used in modern cryptography. Recent developments in information and communication technologies have caused a great increase in the amount and speed of information produced and stored. This increase in the amount of information has also brought about some security problems. The security systems of businesses, banks, government agencies and other organizations are based on solving difficult mathematical problems. These problems take a long time to solve, even with the most powerful computers and modern algorithms. Studies in the literature show that quantum computers do not pose great security threats today. However, scientists predict that quantum computing will evolve faster than expected and reveal major security vulnerabilities. For this reason, the encryption systems of many organizations will face serious cyber security problems shortly. Both states and the private sector should anticipate these dangers today and be ready for security problems that may arise in the future.

Keywords— quantum cryptology, cyber security, Shor's algorithm, Grover's algorithm

1. GİRİŞ (INTRODUCTION)

Teknolojideki gelişmeler ve özellikle elektronik iletişim, modern çağın ana teknolojik dayanaklarından biri haline gelmiştir. Veri aktarımı ve veri depolamada gizlilik, bütünlük, özgünlük ve itiraz edilmeme ihtiyacı, kriptografi bilimini bilgi teknolojisindeki en önemli disiplinlerden biri haline getirmiştir. Yunanca gizli ve yazma sözcüklerinden türetilen kriptoloji, aktarılan verilerin veya üçüncü taraf düşmanlardan saklanan verilerin güvenliğini sağlama

sürecidir [1]. Bu güvenlik, kriptoloji sayesinde verilerin şifrelenmesiyle gerçekleştirilir. Veri şifreleme, bilgi güvenliğini sağlamak ve birçok uyumluluk gereksinimi için gerekli olabilecek özelliklerden birisidir. Oracle, Microsoft SQL ve MySQL gibi modern veritabanlarının çoğu, verilerin şifrelenmesi ve şifrelerin çözülmesi için birtakım işlemler içermektedirler. Bu platformların çoğunun veritabanında veri sağlama işlevleri bulunmaktadır [2].

Siber güvenlik temel olarak, bir bilgisayar veya bilgisayar grubunu, bir sisteme veya ağa girme ve bilgileri çalma, değiştirme veya yok etme girişimlerinden korumak anlamına gelmektedir. Bu siber saldırılar, izlenmesi zor kaynaklardan gelmekte ve genellikle, virüsleri, solucanları, botları veya yazılımları, nasıl enfekte ettiklerine, çoğaldıklarına ve zarar verdiklerine bağlı olarak oluşmaktadır. Siber güvenlik, genellikle iyi yürütülen bir stratejiyi ve rakiplerin bir sonraki hamlelerini tahmin etme yeteneğini ödüllendiren satranç, futbol veya diğer oyunlara benzetmek mümkündür. San Francisco Körfez Bölgesi'nde bir siber güvenlik uzmanı Markus Jakobsson, "İnsanların beni nasıl yenebileceğini ve yenilmeden önce nasıl durduracağını bulmak istiyorum" diyor. En iyi siber güvenlik uzmanları, zor problemleri çözme konusunda meraklı, şüpheci, akıllı ve tutkulu kişilerdir [3].

Bilgi güvenliği, siyaset, askeri ilişkiler, diplomasi, e-ticaret ve iletişim sistemlerinin güvenliğinin merkezinde yer almakta ve günlük hayatımızda giderek artan bir endişeye neden olmaktadır. Kriptografi, kötü niyetli taraflardan korunmak için güvenli kanallara dayalı temel bilgileri gizlemeyi amaçlayarak bilgi güvenliği için oldukça önemlidir [4]. Yakın alan iletişimi ve daha fazlası güvenli kriptografik işlemlere dayanmaktadır. Buradaki kullanılan "güvenli" kelimesi, altta yatan şifreleme işleminin rakip tarafından (kullanılan anahtarı bilmeden) kırılamayacağı anlamına gelir. Şifreleme yöntemlerini kıran bilime ise kriptanaliz denir. Kriptanaliz matematiksel bilgiye ve büyük hesaplama gücüne dayanmaktadır [5].

Bilgisayar Bilimi ve Yapay Zeka'nın büyük başarısı, son yıllardaki teknolojik ilerlemelerle ilişkilidir. Moore yasasına göre, bilgisayarın gücü 1970 yılından itibaren her iki yılda bir iki katına çıkmaktadır [6]. 20. yüzyılda kuantum hesaplama, Bilgi Teorisi ve Kuantum Mekaniğini birleştirmiştir [6]. Kuantum hesaplama, dünyanın en karmaşık problemlerinin bazılarını çözmemize yardımcı olacağını vaat etmektedir. Kuantum sistemler muhtemelen, en güçlü süper bilgisayarları aşan yeteneklere sahip olacaktır. Daha şimdiden malzeme tasarımı, finansal risk yönetimi ve MRI teknolojisinde ilk kuantum adımları atılmaya başlandı. Kuantum araştırmacıları, bilim adamları, mühendisler ve iş dünyası liderleri kuantum ekosistemini ilerletmek için işbirliği yapmaya devam ettikçe, tüm sektörlerde kuantum etkisi daha hızlı görülecektir. Diğer yandan, karmaşık zor problemlerin çözülmesini sağlayacak olan kuantum bilgi işlem gücü, gelecekte bugün ki en gelişmiş şifreleme sistemlerini bile çözebilecek kapasiteye sahip olabilir [7].

Bu çalışmanın amacı kuantum bilgisayarların siber güvenlik sistemlerinde kullanılan güvenlik şifreleri üzerine etkilerini araştırmaktır. Bu bağlamda, ikinci bölümünde kuantum alanında yaşanan gelişmeler, üçüncü bölümde modern kriptoloji de kullanılan şifreleme yöntemleri, dördüncü bölümde kuantum bilgisayarlar ile Shor ve Grover algoritmaları, beşinci bölümde ise kuantum bilgisayarların ortaya çıkışıyla ne gibi güvenlik zafiyetlerinin yaşanacağı anlatılmıştır. Sonuç bölümünde ise kuantum bilgisayarların siber güvenlik üzerine etkileri tartışılmıştır.

2. LİTERATÜR İNCELEMESİ (LITERATURE REVIEW)

Kuantum kriptolojisinin temelinde kuantum teorisi bulunmaktadır. Kuantum teorisi, modern fiziğin madde ve enerjinin doğasını ve davranışlarını atom ve atom altı (elektron, proton ve nötron) düzeyde açıklamaktadır [8]. Bugün ki kuantum bilgisayarların çalışma yapısı kuantum mekaniğine dayanmaktadır. 20. yüzyılın başlarında Max Planck, Albert Einstein, Louis de Broglie, Neils Bohr, Werner Heinsenberg, Erwin Schrodinger, Max Born, Paul Dirac gibi bilim insanları kuantum mekaniğinin gelişmesine katkı sağlamışlardır [9].

Kuantum bilgi teknolojisi, ikinci kuantum devriminin öncü koruyucusudur ve bir zamanlar az bilinen ve kuantum teorisi tarafından öngörülen 'ikinci dereceden' etkilere dayanmaktadır. Bu etkiler en erken 1935'te Einstein, Podolsky ve Rosen (EPR) tarafından yazılan ve dikkatle hazırlanmış bazı kuantum sistemlerinin aralarında yerel olmayan, dolaşık, klasik olmayan korelasyonlara sahip olduğuna dikkat çeken bir makalede tanıtılmıştır [10]. Einstein, Podolsky ve Rosen korelasyonları sadece olağan dalga-parçacık ikiliğinin bir tezahürü değil, aynı zamanda kendisini yalnızca hassas bir şekilde tasarlanmış insan yapımı kuantum mimarilerinde gösteren yeni bir tür yüksek düzey kuantum etkisidir.

1981 yılında Richard Feynman Massachusetts Teknoloji Enstitüsü'nde yaptığı konuşma ile ilk kez kuantum bilgisayar fikrini ortaya atmıştır [11]. Feynman'a göre; kuantum fiziği yasaları tasarlanan bir bilgisayarda kullanılabilecektir. Feynman, kuantum mekanik sistemlerin klasik bir bilgisayarda doğru bir şeklide uygulanamayacağını, fakat üretilen yeni bir makine türünün (kuantum bilgisayarlar) gelecekte bir molekülü tam olarak simüle edebileceğini söylemiştir [12]. 1989 yılında IBM'deki bilim insanları, bir nikel üzerinde 35 xenon atomu kullanarak şirketin adını hecelemeyi başardı [13]. 1994 yılında Peter Shor, şifreleme sistemlerini kırabilmek için kuantum bilgisayar gücünde bir algoritma geliştirdi [14]. Shor'un algoritması, büyük sayıların çarpanlarına ayrılmasına dayanan kriptografik anahtarları kırabilme kapasitesine sahiptir. Bu buluş kuantum kriptolojisi açısından bir dönüm noktası kabul edilir.

2013 yılında IBM'deki bilim insanları, kısa film oluşturmak için tek karbon monoksit moleküllerinin manipüle edildiği bir "stop-motion" animasyonu olan "A Boy and his Atom" adlı dünyanın en küçük filmini yayınladılar [13]. 2016 yılından sonra kuantum teknolojisinde büyük gelişmeler yaşandı. Tablo 1'de 2016-2020 yılları arasında kuantum teknolojilerinde yaşanan gelişmeler verilmiştir.

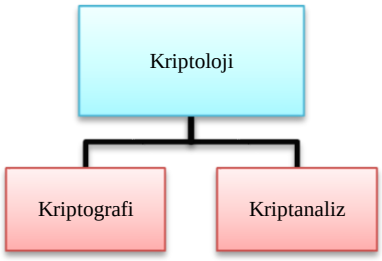
Tablo 1. 2016-2020 dönemlerinde kuantum teknolojisinde yaşanan gelişmeler
(Developments in quantum technology between 2016-2020)

Yıl	Kuantum Teknolojisinde Yaşanan Gelişmeler
2016	IBM, tartışmasız en kapsamlı platform olan Q Experience'ı piyasaya sürdü [15].
2017	Temmuz 2017'de Çinli bilim adamları Tibet'ten yörüngedeki bir uyduya, Dünya yüzeyinin 870 mil (1.400 kilometre) yukarısına kadar bir bilgi paketi gönderdiler. Daha spesifik olarak, bilim adamları bir fotonun kuantum halini (nasıl polarize olduğu hakkında bilgi) yörüngeye ışınladılar [16].
2017	Ağustos 2017'de Çinli bilim adamları ilk özel kuantum iletişim ağını kurduklarını duyurdular [17].
2018	2018 yılında Rigetti's Forest, Google'ın Cirq'i ve Çin Bilimler Akademisi ile işbirliği içinde bir kuantum bulut bilişim hizmeti başlatan Alibaba'nın Aliyun'u geliştirdi [15].
2018	Ekim 2018'de D-Wave Systems, kuantum tavlayıcı donanımına kendi gerçek zamanlı bulut erişimi olan Leap'i piyasaya sürdü [15].
2019	IBM, 53 kübitlik bir model olan en büyük kuantum bilgisayarını çalıştırmayı başardı [18].
2019	Amazon Web Services, Braket adlı araştırmacı odaklı kuantum bilişim hizmetini altyapısına kattı [18].
2019	Kuantum bilgisayarlarının Amazon'un Braket hizmetinde IonQ ve D- Wave'den gelen bilgisayarlara katıldığı Rigetti Computing, 32 kübitlik bir kuantum bilgisayarı tanıttı [18].
2019	Microsoft , "topolojik" kübitlere dayalı kuantum hesaplama teknolojisini güçlendirmeye neredeyse hazır olduğunu söyledi [18].
2019	Azure Quantum bulut bilişim hizmetini başlattı [18].
2019	Intel, kübitleri barındıran kuantum işlemcilerle iletişim kurmak için gereken donanımı küçültmek ve basitleştirmek için tasarlanmış Horse Ridge adlı bir kuantum bilgi işlem denetleyici çipini ürettiğini duyurdu [18].
2019	Google, en hızlı süper bilgisayarın 10.000 yılını alan belirli bir görevi 53 kübitlik bir kuantum bilgi işlem yongasında 200 saniyede gerçekleştirerek kuantum üstünlüğüne ulaştığını duyurdu [18].
2020	IBM, 2023 yılına kadar 1000 kübit içeren bir bilgisayar inşa etme hedefi koydu [18].
2020	Şubat 2020 de Çinli bilim insanları birbirinden 50 kilometre uzaklıktaki iki kuantum bellek arasında fiber optik kablolarla dolanıklık oluşturdular ve bu uzaklık önceki rekorun 40 katıydı. Elde edilen bu başarı ile gelecekte süper hızlı ve süper güvenli kuantum internet"in kurulabileceğine olan inanç daha da arttı [19].
2020	Eylül 2020'de IBM 65 kübit içeren en büyük kuantum bilgisayarı inşa ettiğini duyurdu [20].

Sonuç olarak tüm bu gelişmeler ve şu an ki bilimsel ilerlemeler kuantum teknolojisinin daha hızlı gelişeceğini göstermektedir. Daha şimdiden Avustralya, Kanada, Çin, AB, Japonya, Hollanda, Rusya, Singapur, Birleşik Krallık ve ABD gibi birçok ülke milyarlarca dolarlık kuantum teknoloji programları başlattı. Aynı zamanda, Google, IBM, Microsoft, Intel, Atos, Baidu, Alibaba, Tencent gibi çok sayıda küçük ve daha büyük kuantum start-upları kuantum donanım ve yazılım geliştiren laboratuvarları başlattı [21].

3. KRİPTOLOJİNİN MİMARİ YAPISI (ARCHITECTURAL STRUCTURE OF CRYPTOLOGY)

Matematikteki sayılar teorisi üzerine kurulu olan kriptoloji, güvenli iletişim bilimidir [22]. Kriptoloji, iletilerin sistematik olarak şifrelenmesi, mesajların güvenli iletilmesi ve iletilen mesajların deşifre edilmesini kapsamaktadır. Kriptoloji, kriptografi ve kriptanaliz bilimlerini içermektedir (Bkz. Şekil 1). Bu nedenle kriptolojiyi iyi anlamak için kriptografi ve kriptanalizin iyi bilinmesi gerekir.



Şekil 1. Kriptoloji bileşenleri
(Cryptology components)

3.1. Kriptografi (Cryptography)

Kriptografi, bilgi biliminde gizli iletişim anlamına gelmektedir. Bir iletinin, istenmeyen kişiler/taraflar (kulak misafirleri) tarafından deşifre edilemeyecek şekilde kodlanması (şifreleme) veya kodunun çözülmesi (şifre çözme) sanatıdır [23]. Kriptografi, güvensiz iletişim ortamları üzerinde gizli iletişim sağlayan şemaların tasarlanması ve analiz edilmesi problemiyle ilişkilidir. Güvenli olmayan medya üzerinden gizli iletişim sağlama sorunu, kriptografinin en temel sorunudur. Kriptografide ortam, güvensiz medya üzerinden iletişim kuran iki taraftan oluşmaktadır. Şifreleme şeması, bu tarafların birbirleriyle gizlice iletişim kurmalarına izin veren bir protokoldür [24]. Kriptografi, bilişsel bilgi işleme yaklaşımlarını kullanarak, akıllı kriptografik algoritmalar ve güvenlik protokolleri oluşturmaya odaklanan hesaplama yöntemleri ve güvenlik sistemleri oluşturmaktadır. Bu tür sistemler şifrelenmiş verilerin anlamsal değerlendirilmesi için tasarlanmış ve şifrelemede en uygun tekniklerin seçilmesine izin vermektedir.

3.2. Kriptanaliz (Cryptanalysis)

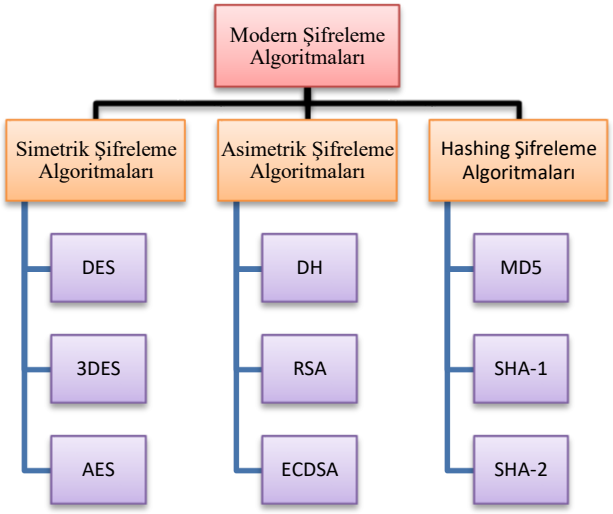
Kriptanaliz, şifrelenmiş mesajları kırma bilimidir [22]. Kriptanaliz, zayıflıkları veya bilgi sızıntılarını aramak için kriptografik sistemleri incelemekte ve kriptografik sistemin temel matematiksel zayıflıklarını bulmaktadır [25]. Bununla birlikte kriptanaliz, yan kanal saldırıları ve zayıf entropi girdileri gibi uygulamalardaki zayıflıkların aranmasını da sağlamaktadır [25]. Örneğin, Amerika Birleşik Devletleri istihbarat teşkilatı olan Federal

Soruşturma Bürosu (FBI), kriminal veya terörist faaliyetlerin tanımlanmasına yardımcı olmak için şifrelenmiş kayıtların ve belgelerin incelenmesinden sorumlu bir kriptanalize sahiptir. Kriptanaliz ajanı, yazılı iletişim, e-posta ve kayıtlardaki her türlü şifreyi ve kodu incelemekten sorumludur. Buradaki temel amaç yasadışı faaliyetleri tespit etmektir. Buradaki kodlar, mahkûmlar, uluslararası teröristler, şiddet suçluları ve yabancı istihbarat ajanları tarafından yaygın olarak kullanılmaktadır [26].

3.3. Modern Şifreleme Algoritmaları (Modern Encryption Algorithms)

Kriptografi, verileri koruyan en eski sistemlerden biridir. Kriptografinin MÖ 2000 yıllarında Mısır'da başladığına inanılıyor. Eski Çinliler eserlerinin anlamını gizlemek için kodlar kullanmıştır. Yıllar içinde, harflerin veya sayıların basit bir şekilde değiştirilmesi ve karmaşık matematiksel teoremler gibi çeşitli sistemler kullanılmıştır. Kriptografinin en basit biçimlerinden biri, sayıların yerine harflerin kullanılmasıdır [27].

Modern şifreleme algoritmaları, çeşitli uygulama alanları için veri iletişim sistemlerinde büyük öneme sahiptir. Özellikle Yapay Zekâ ve Nesnelerin İnterneti'nin gelişmesi, bilgisayar saldırılarının artmasına sebep olmuştur. Bilgisayar saldırıları arttıkça, güvenliğe olan talepte de artış yaşanmıştır. Bugüne kadar, güvenlik sorunlarına çözüm üretmek için çok sayıda şifreleme sistemi geliştirilmiştir. Geliştirilen bu şifrelerin bazıları eski olmalarına rağmen günümüzde çoğu hala aktif olarak kullanılmaktadır. Modern kriptografi, bilgi güvenliğini sağlamak için simetrik, asimetrik ve Hashing şifreleme algoritmaları üzerinde çalışmaktadır (Bkz. Şekil 2). Burada kullanılan yöntemlerin klasik tekniklerle çok fazla ortak noktası yoktur ve genellikle daha matematikseldirler.



Şekil 2. Modern şifreleme algoritmaları
(Modern encryption algorithms)

Şekil 2'de simetrik, asimetrik ve Hashing şifrelemede en yaygın kullanılan bazı algoritmalar verilmiştir. Bu algoritmalardan farklı olarak kullanılan birçok algoritma daha vardır.

3.4. Simetrik Şifreler (Symmetric Cryptography)

Simetrik şifrelemede, gönderen ve alıcı verileri şifrelemek ve şifresini çözmek için aynı gizli anahtarı ve aynı şifreleme algoritmasını kullanır [1]. Simetrik bir şifreyi kullanmak isteyen tarafların, şifreyi kullanmadan önce aynı gizli anahtar üzerinde anlaşmaları gerekir. Örneğin, sır (ileti veya mesaj), taraflarca toplandığında taraflarca paylaşılabilir veya anahtar farklı bir güvenlik protokolü güvenilir bir üçüncü taraf kullanılarak değiştirilebilir [28].

Simetrik şifreleme de Alice ve Bob olarak bilinen iki kişi bir anahtarı paylaşır. Alice, Bob'a gönderilecek bir mesajı kodlamak istediğinde, gizli anahtarı ve mesajı parametre olarak kullanarak simetrik bir algoritma uygular. Bob mesajı aldığında, parametre ile aynı anahtarı kullanarak, karşılık gelen şifre çözme algoritmasını kullanır. Simetrik şifrelemede, şifreleme fonksiyonunu, E olarak kabul edelim. Bu durumda E'ye karşılık gelen şifre çözme fonksiyonu E^{-1}'dir [29]. En iyi bilinen simetrik şifreleme algoritmaları: DES (Data Encryption Standard), 3DES (Triple DES) ve AES (Advanced Encryption Standard)'dir [30]. Bu şifreleme algoritmalarının temel amacı, şifrelenmiş metnin çözülmesini geciktirerek değersiz hale getirmektir. Örneğin 2019 yılında askeri amaçla şifrelenerek gizlenmiş bir metin eğer 100.000 yıl sonra çözülüyorsa bu güvenlik açısından herhangi bir tehlike oluşturmayacaktır.

DES: DES, 1970 yılında ilk olarak IBM'deki [31] araştırmacılar tarafından tasarlandı. DES veri şifrelemede kullanılan eski bir simetrik anahtar yöntemidir. DES bir mesajı şifrelemek ve şifresini çözmek için aynı anahtarı kullanarak çalışır. Bu nedenle hem gönderen hem de alıcı aynı özel anahtarı bilmeli ve kullanmalıdır [31]. DES güçlü şifreleme ihtiyacının yüksek olduğu finansal hizmetlerde hızlı bir şekilde kullanılmaya başlandı. DES sadeliği sayesinde, çok çeşitli gömülü sistemlerde, akıllı kartlarda, SIM kartlarda ve modemlerde kullanılmaktadır. DES bugün için ömrünün sonuna gelmiş olmasına rağmen kriptografi veri şifreleme algoritmalarının geliştirilmesini desteklemektedir [31].

3DES: Üçlü Veri Şifreleme Standardı olarak da bilinen 3DES, 1974 yılında bir IBM ekibi tarafından geliştirilen DES algoritmasına dayanmaktadır. Üçlü DES başlangıçta özel donanımda çalışmak üzere tasarlanmıştır. Bu nedenle genel amaçlı işlemcilerde hesaplama maliyeti yüksektir [32]. Üçlü DES üç adımda çalışmaktadır. Bu adımlar: Şifrele-Şifreyi Çöz-Şifrele (Encrypt-Decrypt-Encrypt-EDE)'dir. Üçlü DES üç adet 56 bit anahtar (K_1, K_2 *ve* K_3) alır ve önce K_1 ile şifrelemekte, daha sonra K_2 ile şifresini çözer ve son olarak K_3 ile şifreleyerek çalışır. Üçlü DES'in iki tuşlu ve üç tuşlu sürümleri vardır. İki tuşlu sürümde, aynı algoritma üç kez çalışır, ancak ilk ve son adımlar için K_1'i kullanır. Başka bir

deyişle, $K_1 = K_2$ ise $K_1 = K_2 = K_3$ olur ve 3DES algoritması DES haline gelir [33].

AES: Gelişmiş Şifreleme Standardı veya AES, ABD hükümeti tarafından gizli bilgileri korumak için seçilen simetrik bir blok şifredir. AES, hassas verileri şifrelemek için dünya çapında yazılım ve donanımda kullanılmaktadır [34]. AES hem yazılımda hem de donanımda hızlı olmasına rağmen, büyük miktardaki verileri şifrelemede oldukça yavaştır. Bu nedenle bu sorunu kalıcı çözmek için AES operasyonlarının hızlandırılması gerekmektedir [35]. AES, 128 bitlik veri bloklarını şifrelemek için 128 bit (10 tur şifreleme ile), 192 bit (12 tur şifreleme ile) veya 256 bit (14 tur şifreleme ile) anahtarları kullanır. AES, beklemedeki verileri korumak için yaygın olarak kullanılır. AES uygulamaları arasında kendi kendini şifreleyen disk sürücüleri, veritabanı şifrelemesi ve depolama şifrelemesi bulunur [34].

3.5. Asimetrik Şifreleme (Asymmetric Encryption)

Asimetrik şifreleme veya genel açık (ortak) anahtarlı şifreleme, anahtarların çift halinde olduğu bir şifreleme şeklidir. Asimetrik şifrelemede her bir kişinin çift anahtarı (kendine özel ve ortak anahtarı) vardır [1]. Bu anahtarların biri mesajın şifrelenmesinde diğeri şifre çözmede kullanılır [36]. Örneğin, Alice, Bob'a şifrelenmiş bir mesaj göndermek isterse, şifreleme için Bob'un ortak anahtarını kullanır. Ardından, Bob, şifrelenmiş mesajı, kendi özel şifresiyle çözer [29]. Böylece, mesaj ortak bir anahtarla şifrelenir ve yalnızca özel anahtara sahip olan kişi mesajın şifresini çözebilir [1].

Asimetrik şifreleme algoritmaları, simetrik şifreleme algoritmaları kadar hızlı değildir. Bunun temel sebebi, asimetrik şifreleme algoritmalarının daha karmaşık fonksiyon ve algoritmalar kullanmasıdır [36]. Bu nedenle asimetrik şifreleme simetrik şifreleme kadar yaygın kullanılmaz. Dijital imzalar için ek olarak asimetrik şifreleme kullanılır. Örneğin, Alice bir belgeyi özel anahtarıyla dijital olarak imzalayabilir ve Bob imzayı Alice'in bilinen genel anahtarıyla doğrulayabilir. Asimetrik şifrelemenin güvenliği, büyük asal sayıları çarpanlarına ayırma zorluğu ve ayrık logaritma problemi gibi hesaplama problemlerine dayanmaktadır.

Bu tür asimetrik algoritmalara tek yönlü fonksiyonlar denir. Çünkü bu algoritmaların tek yönlü hesaplanması kolay olmasına rağmen, tersine çevrilmeleri zordur [37]. DH (Diffie-Hellman), RSA (Rivest, Shamir, Adelman) ve ECDSA (Elliptic Curve Digital Signature Algorithm) [38] en çok kullanılan asimetrik anahtar algoritmalarıdır. Bu algoritmalar, tamsayı çarpanlarına ayırma ve ayrık log problemlerinin sürdürülemezliğine dayanmaktadır. Klasik bilgisayarların bu problemleri çözmesi zordur, ancak kuantum bilgisayarların çözmesi kolaydır [38].

DH: DH, Whitfield Diffie ve Martin Hellman tarafında 1976 yılında [39] geliştirilmiş ve bilinen en eski asimetrik anahtar uygulamalarından biridir. DH algoritması genellikle anahtar değişimi için kullanılır. Simetrik anahtar algoritmaları hızlı ve güvenli olmasına rağmen, anahtar değişimi her zaman sorunludur. Bu nedenle tüm sistemlere özel anahtarı almanın bir yolunun bulunması gerekir. DH algoritması bu konuda yardımcı olur. DH algoritması güvenli bir iletişim kanalı oluşturmak amacıyla kullanılır. Bu kanal, sistemler tarafından özel bir anahtar alışverişi yapmakta kullanılır. Daha sonra bu özel anahtar, iki sistem arasında simetrik şifreleme yapmak için kullanılır [36]. Örneğin, Curve25519, 128 bit güvenlik sağlayan ve anahtar değişim protokolü için tasarlanan bir DH fonksiyonudur [40].

RSA: RSA, birçok akıllı karta gömülü en iyi bilinen ve kullanılan açık anahtar algoritmasıdır [41]. 1978 yılında geliştirilen RSA, imzalama ve şifreleme için yaygın olarak kullanılan asimetrik bir algoritmadır [36]. RSA algoritması, $N = p.q$ $(p \neq q)$ olmak üzere p ve q gibi iki büyük rassal asal sayıyı kullanır. Asal sayı büyüdükçe gizlilik ve güvenlik sistemleri için kullanım da artmaktadır. RSA algoritması üç parçalı bir işlem kullanır. İlk bölümde RSA algoritmasında kullanılan tuşlar, asal sayılara dayalı matematiksel işlemler kullanılarak anahtar üretilir. Sürecin ikinci bölümü şifrelemedir. Bu şifreleme, anahtar çiftindeki anahtarlardan biri kullanılarak yapılır. Sürecin üçüncü bölümü şifre çözmedir. Şifre çözme, anahtar çiftindeki diğer anahtar kullanılarak yapılır [36]. RSA, e-postaları, kredi kartlarını ve diğer pek çok elektronik sistemi güvenli hale getirmek için kullanılan bir şifreleme türüdür [42].

ECDSA: ECDSA, çoğu blok zincirindeki işlemleri imzalamak için kullanılan açık anahtar şifreleme sistemi altında anahtarlar oluşturmada standart haline gelmiştir. Bu sistem, herhangi bir üçüncü tarafla paylaşabileceğimiz rassal bir 256 bitlik özel anahtar ve türetici bir açık anahtar oluşturmamızı sağlar. Daha sonra, açık anahtarı oluşturan özel anahtarı bulmak neredeyse imkânsızdır. Ancak kuantum bilgisayarlar bir açık anahtar ile özel anahtar arasındaki matematiksel ilişkiyi çözmek için bir algoritma kullanarak özel anahtarı ortaya çıkarabilir ve güvenliği tehlikeye atabilirler. Çok yakın bir zamanda güçlü kuantum bilgisayarlar, Bitcoin ve Ethereum gibi ECDSA'ya dayanan tüm blok zincirleri için bir tehdit haline gelebilir [43].

3.6. Hashing Şifreleme (Hashing Encryption)

Kriptografik hash fonksiyonları, anahtarsız şifreleme olarak adlandırılan üçüncü bir şifreleme türüdür [44]. Hash fonksiyonu, kriptolojide kullanılan bir matematik fonksiyonudur [45]. Bu fonksiyon sabit boyutlu bir bit (veri) dizesi değeri hesaplayan bir algoritmadır. Örneğin, elimizde bulunan bir dosyanın temel olarak veri bloklarını içeriğini varsayalım. Hash bu verileri, orijinal dizeyi temsil eden çok daha kısa sabit uzunluklu bir değere veya anahtara dönüştürür. Hash fonksiyonundaki temel mantık, elde bulunan veri sistematik olarak dosyaya nasıl yerleştirilmelidir ki, arandığında doğrudan adrese bakılsın şeklindedir. Hash fonksiyonları, mesajların bütünlüğünü

kontrol etmek ve bilgileri doğrulamak için bilgi işlem sistemlerinde yaygın olarak kullanılan veri yapılarıdır. Bununla birlikte hash fonksiyonları, polinom zamanda çözülebildiği için kriptografik olarak "zayıf" kabul edilmekte, fakat kolayca deşifre edilemezler. Kriptografik hash fonksiyonları, tipik hash fonksiyonlarına güvenlik özellikleri ekleyerek bir iletinin içeriği veya alıcılar ve göndericiler hakkında bilgi almayı zorlaştırmaktadır. Bu fonksiyonlar, işlem bilgilerini güncel olarak iletmek için kripto para birimlerinde yaygın olarak kullanılmaktadır. Örneğin, kripto para birimi olan Bitcoin, algoritmasında SHA-256 kriptografik hash fonksiyonunu kullanmaktadır [46]. Bugün için birçok hashing algoritması vardır: MD5 (Message-Digest 5), SHA-1 (Secure Hashing Algorithm-1) [30] ve SHA-2 (Secure Hashing Digest-2) [47] bunlardan bazısıdır.

MD5: MD5 hash algoritması, herhangi bir uzunluktaki bir iletiyi giriş olarak kabul eden ve çıkış olarak orijinal iletinin kimliğini doğrulamak için kullanılacak sabit uzunluklu bir çıktı değerine dönüştüren tek yönlü bir şifreleme fonksiyonudur [48]. Bir MD5 hash değeri, dosya veya mesaj gibi bir veri parçasına bağlı olarak 32 basamaklı onaltılık sayı olarak ifade edilir. MD5, dijital imzaların oluşturulması ve doğrulanması ile dosyaların bütünlüğünü kontrol etmek için kullanılır [49].

SHA-1: SHA-1, sonsuz miktarda giriş verisini destekleyen ve sabit bir çıkış uzunluğu sağlayan popüler bir hash algoritmasıdır [50]. SHA-1, mesaj özeti (message digest) adı verilen bir mesajın yoğunlaştırılmış bir gösterimini oluşturmak için kullanılabilir. SHA-1, Dijital İmza Standardında belirtilen Dijital İmza Algoritması ile ve federal uygulamalar için güvenli bir hash algoritması gerektiğinde kullanılmaktadır. SHA-1, bir dijital imzanın hesaplanmasında ve doğrulanmasında bir iletinin hem vericisi hem de amaçlanan alıcısı tarafından kullanılır [51].

SH-2: SH-2, dijital verileri korumada kullanılan bir kriptografik hash fonksiyonudur. SH-2, SH-1'in daha gelişmiş bir sürümü olup SH-1'e benzer çalışır [52]. SH-2 birkaç farklı algoritma içerebilmektedir. Örneğin, SHA-2, SHA-224, SHA-256, SHA-384, SHA-512, SHA-512/224 ve SHA-512/256'yı içeren bir hash fonksiyon ailesidir. Tüm bu hash fonksiyonları benzer olmakla birlikte, algoritmanın belirli bir girdiden bir özet (digest) veya çıktı oluşturma biçiminde biraz farklılıklar vardır. Ayrıca bu algoritmalar ürettikleri özetin sabit uzunluğunda da farklılıklar gösterirler [53]. SHA-2, SHA-1 veya MD5 ile karşılaştırıldığında daha iyi güvenlik sağlar [54].

4. KUANTUM KRİPTOGRAFİ (QUANTUM CRYPTOGRAPHY)

Kuantum kriptografi, kuantum hesaplama, kuantum ölçümleri ve kuantum ışınlanma içeren kuantum bilgi işlemenin bir dalıdır. Kuantum hesaplama ve kuantum bilgisi, kuantum mekanik sistemler kullanılarak gerçekleştirilebilecek bilgi işleme görevlerinin incelenmesidir [55]. Kuantum mekaniği, fiziksel teorilerin inşası için matematiksel bir çerçeve sunmaktadır. Kuantum mekaniğinin kuralları basittir, ancak uzmanlar bile onları mantık dışı bulmaktadır. Fizikçiler kuantum mekaniğini daha iyi anlamak için uzun zamandır kuantum dolanıklık ilkesi üzerinde çalışmaktadırlar. Dolanıklık, kuantum hesaplama ve kuantum bilgisinin en ilginç uygulamalarının çoğunda kilit rol oynamaktadır. Son yıllarda bilim insanları, dolanıklığın özelliklerini daha iyi anlamak için yoğun çalışmalar başlattılar. Henüz tam bir dolanıklık teorisi olmamasına rağmen, kuantum mekaniğinin bu garip özelliğini anlama konusunda bazı ilerlemeler kaydedildi. Birçok araştırmacı tarafından, dolanıklık üzerine daha fazla çalışmanın yapılmasının, kuantum hesaplama ve kuantum bilgisinde yeni uygulamaların geliştirilmesini kolaylaştıracak öngörüler sağlayacağı düşünülmektedir [55].

Kriptografi, siber güvenlik için en önemli unsurlardan biridir ve bilgi çağında giderek daha önemli hale gelmektedir. Klasik kriptosistemlerde, kriptografi algoritmaları çoğunlukla sayı teorisindeki klasik çözülmesi zor problemlere dayanmaktadır. Bununla birlikte, kuantum bilgisayar ve Shor algoritmasının geliştirilmesi [56], sayı teorisindeki zor problemlerin çözülebilmesini sağlayarak (RSA şifreleme sistemi gibi) kripto sistemlerin güvenliği üzerinde büyük bir tehdit oluşturmaktadır. Bu nedenle, hem kuantum hem de klasik bilgisayarlara karşı güvenli olan kuantum kriptografisi önemli bir ihtiyaç haline gelmiştir [57]. Kuantum bilgisayarlar çevrimiçi hale geldiğinde, bazı yaygın ve önemli şifreleme yöntemleri kullanılmayacaktır. Kuantum bilgisayarlar atom altı parçacıkları yöneten yasalardan yararlanarak mevcut şifreleme yöntemlerini kolayca kırabilirler [58].

Maryland'deki Kuantum Enstitüsü'nde deneysel kuantum fizikçisi olan Chris Monroe, "Bilgi güvenliği temel fizik yasaları tarafından garanti edilmektedir." demektedir [59]. Kriptografi bugün tüm elektronik iletişim sistemlerinde önemli bir rol oynamaktadır. Örneğin, e-postaların, şifrelerin, finansal işlemlerin ve hatta elektronik oylama sistemlerinin güvenliği, gizlilik ve dürüstlük gibi aynı güvenlik hedeflerini gerektirir. Kriptografi, yalnızca anahtar değişimi olan tarafların şifreli mesajı okuyabilmesini sağlar [60]. Kuantum bilgisayarlar, klasik bilgisayarların yapamayacağı hesaplamaları yapabildikleri için güvenli ve özgün iletişimi tehdit etmektedir. Sonuç olarak, kuantum bilgisayarlar tüm gizli anahtarları kapsamlı bir şekilde hesaplayarak veya arayarak kriptografik anahtarları hızlı bir şekilde kırabilir, mesaj gönderen veya alıcı arasındaki iletişim kanalını kesebilir. Bu işlemler geleneksel bir bilgisayar tarafından hesaplanamaz [61].

4.1. Kuantum Algoritmaları (Quantum Algorithms)

Algoritma, her adımı bilgisayarda gerçekleştirebilecek bir hesaplama veya bir sorunu çözmek için uygulanacak bir dizi talimatı gerçekleştirmek için izlenecek adım adım bir prosedürdür. Bu nedenle, bir algoritma, bir kuantum bilgisayarda gerçekleştirildiğinde bir kuantum algoritmasıdır. Genel olarak tüm klasik algoritmaları bir kuantum bilgisayarda çalıştırmak mümkündür. Bununla

birlikte, kuantum algoritması terimi, adımlardan en az biri, süperpozisyon veya dolanıklık kullanılarak belirgin bir şekilde "kuantum" olan algoritmalara uygulanır [62].

Kuantum hesaplamanın nihai uygulamaları, kriptografik sistemleri kırmaktan yeni ilaçların tasarımına kadar uzanmaktadır. Bu uygulamalar, bir kuantum bilgisayarda çalışan ve olası herhangi bir klasik algoritma üzerinde bir hızlanma veya başka bir verimlilik artışı sağlayan kuantum algoritma veya algoritmalarına dayanmaktadır. Bugün için büyük ölçekli kuantum bilgisayarlar henüz mevcut olmasa da, kuantum algoritmaları teorisi 20 yılı aşkın bir süredir aktif olarak üzerinde çalışılan bir alandır [63]. Çalışmanın bu kısmında, kuantum bilgisayarların zor problemleri polinom zamanda çözmesini sağlayan Shor ve Grover algoritmalarına genel bir bakışın sunulması amaçlanmıştır.

4.2. Shor Algoritması (Shor's Algorithm)

1994 yılında matematikçi Peter Shor [64], açık anahtarlı kriptografi ile ilgili gruplarda tamsayı çarpanlarına ayırma problemini ve ayrık logaritma problemini çözen polinom zamanlı kuantum bilgisayar algoritmalarını keşfetti. Shor'un algoritması bir pozitif N tamsayısının asal çarpanlarını bulmak için kullanılan bir kuantum algoritmasıdır [65]. Shor (1994), yaptığı çalışmada büyük tamsayıları çarpanlarına ayırmanın kuantum bilgisayarlarla temelde değişeceğini kanıtladı [64]. Bu algoritma kriptoloji açısından büyük önem taşımaktadır. Çünkü bugün kullanılan şifreleme sistemleri çok büyük sayıların klasik bilgisayarlar kullanılarak istenilen makul zamanda faktörlerine ayrılmasının mümkün olmadığı varsayımı üzerine çalışmaktadır. Bu nedenle, şu anda uygulamada kullanılan tüm açık anahtarlı kriptografi sistemleri, yeterince büyük kuantum bilgisayarlar piyasaya çıktığında güvensiz hale gelecektir [64]. Kuantum bilgisayarlardaki algoritmaların bu etkinliği kuantum mekaniğindeki dolanıklık ve paralellik sayesindedir [6].

Shor'un algoritması çok büyük sayıları hesaba katmak için oluşturulmuş bir algoritmadır. Klasik bilgisayarlarda, bu algoritmayla bile, RSA şifrelemesini kırmak için bir sayıyı hesaplamak çok uzun zaman (binlerce yıl gibi) almaktadır. Bununla birlikte, bu büyük tam sayılar kuantum bilgisayar kullanarak, sadece birkaç dakikada çarpanlarına ayrılabilir. Shor algoritması, RSA şifrelemesini kıracak ve siber güvenlik alanında devrim yaratacaktır [42]. Örneğin, bugün kullanılan güvenlik sistemlerinin çoğu şu prensibe göre çalışmaktadır: p ve q iki asal sayı $(p \neq q)$ ve $\mathrm{N} = \mathrm{pq}$ ise N küçük olduğunda hesaplanması kolay bir değerdir. Örneğin, $\mathrm{N} = 21$ ise $\mathrm{p} = 3$ ve $\mathrm{q} = 7$ olur. Ancak $N, 500$ basamaklı iki asal sayının çarpımı ve çok büyük olduğu zaman N'i iki asal sayının çarpımı olarak bulmak zordur. Bu sorunu klasik bilgisayar kullanarak çözmek mümkün değildir. Ancak kuantum bilgisayarlar Shor algoritması sayesinde, bu asal çarpanları hızlı bir şekilde bulabilmekte ve bu tür sorunları kolayca çözebilmektedir.

4.2.2. Grover Algoritması (Grover's Algorithm)

Kuantum işlem birimleri kuşkusuz hesaplama analizi hakkındaki düşünme şeklimizi değiştirecektir. Kuantum hesaplama kavramı yarım yüzyılı aşkın bir süredir var olsa da, son zamanlarda mevcut teknolojiler onu somut bir gerçeklik haline getirmiştir. Bununla birlikte, yıllar boyunca insanlar, sanki varmış gibi, kuantum bilgisayarların ilginç uygulamalarını geliştiriyor ve keşfediyorlar; kuantum kapılarını tanımlayan matematik uygun bir şekilde tanımlanıyor. Bu nedenle mekanikler gerçekte bunları uygulamak için yerinde olmadan algoritmalar keşfedebilir [66].

Grover algoritması 1996 yılında Lov Grover tarafından bulundu ve birçok kriptografik sistemi etkilemektedir [67]. Grover algoritması kuantum hesaplama için tanımlanmış pozitif uygulamaların çoğunun temelini oluşturmaktadır [68]. Grover algoritması, belirli bir sorguyu karşılayan belirli bir öğe veya öğeler için öğe listesinde arama yapmanın ustaca bir yoludur [66]. Klasik olarak, sıralanmamış bir veritabanını aramak, zaman içinde $\mathrm{O(N)}$ olan doğrusal bir arama (linear search) gerektirmektedir. Grover algoritmasında bu $O\left(\sqrt{N}\right)$ zamanda yapılmaktadır. Bu sıralanmamış bir veritabanını aramak için mümkün olan en hızlı kuantum algoritmasıdır. Grover algoritması klasik emsalleri üzerinde hız sağlayabilen diğer kuantum algoritmalarının aksine "sadece" ikinci dereceden bir hızlanma sağlar. Bununla birlikte, N büyük olduğunda ikinci dereceden hızlanma bile önemlidir. Tüm kuantum bilgisayar algoritmalarında olduğu gibi Grover algoritması da olasılıkla çalışmaktadır. Çünkü yüksek olasılıkla doğru sonucu vermektedir. Ayrıca, hata olasılığını, algoritmanın tekrarlanmasıyla azaltmak da mümkündür [69].

5. KUANTUM SONRASI SİBER GÜVENLİK (CYBER SECURITY AFTER QUANTUM)

Günümüzde kullanılan kriptografik şemaların çoğu, Shor'un kuantum saldırı algoritmasına karşı dayanıklı olmayan sayı teorisine dayanmaktadır [70]. Shor (1994), geliştirdiği algoritma sayesinde ayrık algoritma ve hesaplanması zor problemler kuantum bilgisayarlar sayesinde polinom zamanda çözülebilmektedir. Shor algoritması sayesinde bugün kullanılan açık anahtarlı kriptosistemlerin temelini oluşturan çarpanlarına ayırma ve ayrık algoritmalar gibi çözülmesi zor problemlerin çözülebilecek olması asimetrik sitemlerde büyük bir tehdit oluşturmaktadır [14].

Kriptografi güvenliği, belirli "zor" problemlere dayanmaktadır. Bu nedenle güvenliğin doğru şifreleme anahtarıyla yapılması kolaylık sağlamaktadır. Ancak güvenlik doğru olmayan şifreleme anahtarıyla yapılırsa kolay olmayan zor hesaplamalar gerektirmektedir. "Zor" bir problem, mevcut en iyi bilgisayarlarla milyarlarca yılda çözülebilirken "kolay" bir problem çok çabuk çözülebilen bir problemdir. Şifreleme sistemlerinin güvenliğini ölçmek için "güvenlik bit"leri kullanılır. Güvenlik bitleri, bir sistemi en etkili saldırı ile kırmak için gereken adım

sayısının bir fonksiyonu olarak düşünülebilir. Örneğin, 112 bit güvenlikli bir sistemi kırmak için 2^{112} adımın atılması gerekmektedir. Bu da bugün için mevcut olan en iyi bilgisayarla milyarlarca yıl sürecektir [38].

Şifreleme güvenliği, anahtarın uzunluğuna ve kullanılan şifreleme sistemine bağlıdır. Kripto sistemlerin güvenliğini Shor ve Grover kuantum algoritmaları etkilemektedir. Shor algoritması RSA, DH ve ECDSA gibi açık anahtarlı şifreleme sistemlerini kırabilmektedir. Grover algoritması ise AES ve SHA gibi simetrik şifreleme sistemlerinin güvenliğini zayıflatmaktadır. Ancak bu, güvenlik sisteminde önemli bir zafiyet oluşturmamaktadır. Tablo 1'de kuantum bilgisayarlar sonrasında bazı şifreleme sistemlerinde yaşanacak güvenlik riskleri verilmiştir.

Tablo 2. Kuantum sonrası bazı kriptografik sistemlerde yaşanacak güvenlik seviyelerine ilişkin örnekler
(Examples of security levels in some post-quantum cryptographic systems)

Kriptosistem	Fonksiyon	Kuantum Öncesi Güvenlik Seviyesi	Kuantum Sonrası Güvenlik Seviyesi
Simetrik Şifreleme			
AES-128 [71]	Simetrik şifreleme	128-bit	64-bit (Grover)
AES-192 [72]	Simetrik şifreleme	128-bit	64-bit (Grover)
AES-256 [71]	Simetrik şifreleme	256-bit	128-bit (Grover)
Salsa20 [73]	Simetrik şifreleme	256-bit	128-bit (Grover)
GMAC [74]	MAC	128-bit	128-bit (Etkilenmez)
Poly1305 [75]	MAC	128-bit	128-bit (Etkilenmez)
Hashing Şifreleme			
SHA-224 [53]	Hash fonksiyonu	256-bit	128-bit (Grover
SHA-256 [76]	Hash fonksiyonu	256-bit	128-bit (Grover)
SHA3-256 [54]	Hash fonksiyonu	256-bit	128-bit (Grover)
SHA-384 [53]	Hash fonksiyonu	256-bit	128-bit (Grover)
SHA-512 [53]	Hash fonksiyonu	256-bit	128-bit (Grover)
Açık Anahtarlı Şifreleme			
RSA-2048 [77]	Şifreleme	128-bit	0-bit Kırılır (Shor)
RSA-3072 [78]	Şifreleme	128-bit	0-bit Kırılır (Shor)
RSA-3072 [78]	İmzalama	128-bit	0-bit Kırılır (Shor)
RSA-4096 [77]	Şifreleme	128-bit	0-bit Kırılır (Shor)
DH-128 [36]	Anahtar Değişimi	128-bit	0-bit Kırılır (Shor)
DH-3072 [79]	İmzalama	128-bit	0-bit Kırılır (Shor)
DSA-3072 [80], [81]	Anahtar Değişimi	128-bit	0-bit Kırılır (Shor)
256-bit ECDH [82], [83], [84]	Anahtar Değişimi	128-bit	0-bit Kırılır (Shor)
256-bit ECDSA [85], [86] , [43]	İmzalama	128-bit	0-bit Kırılır (Shor)
Curve25519 [40]	Anahtar Değişimi	128-bit	0-bit Kırılır (Shor)

* Bu tablo Bernstein ve Lange (2017) çalışmasında kullandıkları tablo baz alınarak oluşturulmuştur [68].

Tablo 2 dikkate alındığında, kübit işlemleri yeterince küçük ve hızlıysa, Grover'ın algoritması 128 bit AES anahtarları gibi 2^{128} güvenliği amaçlayan birçok şifreleme sistemini tehdit edecektir. Sadece 256 bit AES anahtarlarına geçilmesi tavsiye edilir. Ayrıca, GMAC ve Poly1305 gibi "Bilgi teorisi" MAC'ları, herhangi bir değişiklik yapmadan kuantum bilgisayarlara karşı koruma sağlamaktadır.

Kuantum kriptografi, veri güvenliğinde büyük öneme sahiptir. Bugün için kuantum bilgisayarların ortak şifreleme algoritmalarının sağladığı güvenliği ortadan kaldırma potansiyelini savunan çok sayıda görüş vardır. Bazı görüşlere göre, bugün ki şifreleri kırabilecek kuantum bilgisayarlar önümüzdeki birkaç yıl içinde kullanılabilecektir. Ancak gerçeklere daha yakından bakıldığında, bunun henüz böyle olmadığı görülebilir. Günümüz standartlarının gerektirdiği gibi 2.048 bitlik bir RSA anahtarını kırmak için bir kuantum bilgisayarın, en az 2.048 dolanık kübite ihtiyacı vardır. Bugün mevcut olandan çok uzaktayız. Ayrıca daha fazla dolaşma yaratmada mevcut ilerleme oranının önümüzdeki birkaç yıl içinde bunu mümkün kılması pek de olası görünmemektedir. Bu nedenle, önümüzdeki birkaç yıl içerisinde bugün kullanılan şifreleme sisteminin kuantum bilgisayarlarına karşı savunmasız kalacağı tahmin edilmektedir. Bilim insanlarının kuantum durumlarını tam olarak kontrol edebildikleri durumlar vardır. Ancak bu gelişmeler bugünün şifrelemesini kırmak için yeterince büyük bir kuantum bilgisayarının üretilmesi için hala yeterli görünmüyor. Bu noktaya ulaşmak için hala çok sayıda temel araştırmaya ihtiyaç vardır. Bugün için şifrelemenin kuantum bilgisayarlı rakiplere karşı savunmasız hale gelmesinden endişe etmek zor görünüyor [87]. Diğer taraftan Google gibi kuruluşlar, kafes tabanlı algoritmalardan yararlanan kuantum sonrası kriptografi yöntemlerini test etmeye çoktan başladı bile. NSA, NIST (Amerikan Ulusal Standartlar ve Teknoloji Enstitüsü - National Institute of Standards and Technology) ve diğer devlet kurumları da gelişimlerine aktif olarak yatırım yapıyorlar. NIST, bu yeni algoritmaları değerlendirmek için sistemler geliştirmektedir ve bulgularını 2022-2024 yılları arasında yayınlamayı planlamaktadır [88].

5. SONUÇ (CONCLUSION)

Son yıllarda, klasik bilgisayarlar ile zor olan matematiksel problemleri çözmek için kuantum mekaniği üzerine birçok araştırma yapılmıştır. Bu araştırmalara göre büyük ölçekli kuantum bilgisayarlar şimdiye kadar üretilmiş olsaydı, bugün kullanılan açık anahtarlı şifreleme sistemleri kırılmış olacaktı. Bu şifreleme sistemlerinin kırılması, internet ve dijital iletişim güvenliğini ve bütünlüğünü büyük ölçüde tehlikeye atacaktır. Kuantum sonrası kriptografinin amacı, hem kuantum hem de klasik bilgisayarlara karşı güvenli olan ve mevcut iletişim protokolleri ve ağlarıyla birlikte çalışabilen kriptografik sistemler geliştirmektir [89]. Kuantum bilgisayarlar piyasaya çıktığında kriptografi alanında yaşanacak en önemli sorun, güvenilirlik olacaktır. Bugün için henüz herhangi bir sorun yoktur. Fakat kuantum bilgisayarlar

hayatımıza girdiğinde kriptografi, 5G, dijital dönüşüm ve siber güvenlik alanlarında ciddi güvenlik sorunları ile karşı karşıya kalınacaktır. Diğer taraftan bugün için bu tehlikelerden korunma çabaları hala devam ediyor. Ancak sorunun hak ettiği aciliyette ele alınıp alınmadığı tartışmaya açıktır. Bu nedenle bu çalışma kuantum kriptolojisinin önemini vurgulamak açısından oldukça önemlidir.

Kuantum kriptografi tekniği çok güvenli bir protokole sahip olsa da bugün için maliyeti oldukça yüksektir. Bu nedenle şu an da sadece askeri amaçlarla kullanılmaktadır. Bugün için büyük ölçekli bir kuantum bilgisayarın ne zaman üretileceği sorusu hala belirsizliğini korumaktadır. IBM, 2021 ve 2022 yılında sırasıyla 127 ve 433 kübitlik orta büyüklükteki bilgisayarlar ve daha sonra da milyon kübitlik bilgisayaralar inşa etmeyi planlıyor [20]. Bazı bilim insanları, önümüzdeki 20 yılda bugün kullanılan tüm ortak anahtar programlarını kırabilecek kuantum bilgisayarların inşa edilebileceğini söylüyor [89]. Geçmişe baktığımızda modern ortak anahtar şifreleme altyapısının oluşmasının neredeyse 20 yılı bulduğu görülüyor. Bu nedenle kuantum hesaplamaya ne zaman ulaşılacağımız aslında belirsizdir. Dolayısıyla bu günden kuantum hesaplamaya dayanıklı bilgi güvenliği sistemlerini çalışmaya başlamamız gelecekte karşımıza çıkabilecek birçok soruna karşı önceden hazırlıklı olmamızı sağlayacaktır.

Günümüzde farklı şifreleme sistemleri kullanılsa da asıl gelişmeler süper bilgisayarların icat edildiği son yıllara dayanmaktadır. Bugün için kullanımı kolay fakat çözülmesi imkansız olan bir şifreleme tekniği henüz geliştirilemedi. Diğer taraftan RSA, 3DES, DH ve AES gibi yaygın kullanılan şifreleme algoritmalarının matematiksel olarak çözülmesi mümkündür. Fakat bu insan ömrünün yetmeyeceği bir zamanı dilimin almaktadır. Şu an kullanılan şifreleme algoritmalarının amacı şifrelemeyi geciktirmek ve bu sayede değersiz hale getirmektir. Son dönemlerde sadece anahtarlı iletim için çok sayıda algoritma geliştirilmiştir. Üretilen bu algoritmaların güvenliği tam olarak sağladığı söylenemez, fakat kuantum kriptografinin bugün için güvenliği sağladığını söyleyebiliriz.

Sonuç olarak bu çalışmada kuantum bilgisayarların hayatımıza girmesiyle kuantum algoritmalarının şifreleme sistemlerini nasıl etkileyeceği ve hangi anahtar sistemlerinde güvenlik sorunlarını ortaya çıkacağı verilmiştir. Çalışma sonucunda elde edilen bulgulardan Shor ve Grover algoritmalarının güvenlik sistemlerinde ciddi sorunlara neden olacağı sonucuna varılmıştır. Shor algoritması RSA, DH ve ECDSA gibi açık anahtarlı şifreleme sistemleri üzerinde, Grover algoritması ise AES ve SHA simetrik şifreleme sistemleri üzerinde birtakım güvenlik sorunlarına neden olacaktır. Bugün için henüz mevcut şifreleme protokollerini kıracak kadar güçlü bir kuantum bilgisayar inşa etmenin mümkün olup olmayacağı hala belirsizliğini koruyor. Ayrıca bilim insanları, kuantum bilgi bilimi ile ne tür keşifler yapacaklarından veya en yararlı uygulamaların ne olacağından hala emin değiller. Ancak güvenlik alanında riskler yüksek ve uluslardan şirketlere kadar herkes bu oyuna dahil olmak için çalıyor. Diğer taraftan bugün için Türkiye de kuantum alanında kayda değer bir gelişme henüz olmadı. Bu nedenle Türkiye'nin gerek içerden gerekse dışarıdan gelebilecek siber saldırılardan korunmak ve savunma sistemlerini güçlendirmek için kuantum teknolojisine daha fazla yatırım yapması ve en kısa zamanda bir kuantum araştırma merkezi kurması gerekir.

KAYNAKLAR (REFERENCES)

[1] V. Mavroeidis, K. Vishi, M. D. Zych, A. Jøsang, "The impact of quantum computing on present cryptography", arXiv preprint arXiv:1804.00200, 2018.

[2] C. S. Wright, **The IT Regulatory and Standards compliance Handbook: How to Survive Information Systems Audit and Assessments**, Elsevier. 2018.

[3] B. Nelson, B. "Computer science: Hacking into the cyberworld", *Nature*, 506(7489), 517-519, doi: 10.1038/nj7489-517a, 2014.

[4] F. Hu, L. Lamata, M. Sanz, X. Chen, X. Chen, C. Wang, E. Solano, "Quantum computing cryptography: Finding cryptographic Boolean functions with quantum annealing by a 2000 qubit D-wave quantum computer", *Physics Letters A*, 126214, doi: 10.1016/j.physleta.2019.126214, 2020.

[5] F. J. Furrer, "Roger A. Grimes. Cryptography Apocalypse: Preparing for the Day When Quantum Computing Breaks Today's Crypto", *Springer*, 2020.

[6] M. Clixto, "Quantum computation and cryptography: an overview", *Natural Computing*, *8*(4), 663, 2009.

[7] Internet: Cryptography in the era of quantum computers, https://cloudblogs.microsoft.com/quantum/2020/02/26/cryptography-quantum-computers/, 25.04.2020.

[8] Internet: M. Rouse, Quantum Theory. https://whatis.techtarget.com/definition/quantum-theory, 25.01.2020.

[9] N. Gürsakal, S. Çelik, "Kuantum Bilgisayarlar Teknolojik Anlamda Ne Getirecek?", **Küresel Ekonomiye Yön Veren Yeni Teknolojiler**, Ed: Pakdemirli, B., Gürsakal, N., Bayraktar, Z., & Takmaz S., 23-48, Akçağ Yayınları, Ankara, 2020.

[10] A. Einstein, B. Podolsky, N. Rosen, "Can quantum-mechanical description of physical reality be considered complete?", *Physical review*, *47*(10), 777, 1935.

[11] R. P. Feynman, "Simulating physics with computers", *Int. J. Theor. Phys*, *21*(6/7), 1999.

[12] J. Preskill, "Quantum Computing in the NISQ era and beyond", *Quantum*, *2*, 79. 2018.

[13] Internet: A brief history of quantum. https://pursuit.unimelb.edu.au/articles/a-brief-history-of-quantum, 10.12.2020.

[*14*] L. Chen, S. Jordan, Y. K. Liu, D. Moody, R. Peralta, R. Perlner, D. Smith-Tone, **Report on post-quantum cryptography,** Vol. 12, US Department of Commerce, National Institute of Standards and Technology, 2016.

[15] Internet: The next decade in quantum computing—and how to play, 2018, November 15. https://www.bcg.com/publications/2018/next-decade-quantum-computing-how-play, 10.12.2020.

[*16*] Internet: J. Emspak, Chinese scientists just set the record for the farthest quantum teleportation, 2017, July 15. https://www.space.com/37506-quantum-teleportation-record-shattered.html, 10.12.2020.

[17] Internet: G. Zhe, Not only satellite: China's quantum network connects Beijing, Shanghai and the space. https://news.cgtn.com/news/7a49544d33557a6333566d54/share_p.html, 05.12.2020.

[18] Internet: S. Shankland, Quantum computing leaps ahead in 2019 with new power and speed. https://www.cnet.com/news/quantum-computing-leaps-ahead-in-2019-with-new-power-and-speed/, 25.11.2020.

[19] Y. Yu, F. Ma, X. Y. Luo, B. Jing, P. F. Sun, R. Z. Fang, W. J. Zhang, W. J. "Entanglement of two quantum memories via fibres over dozens of kilometers", *Nature*, *578*(7794), 240-245. https://doi.org/10.1038/s41586-020-1976-7, 2020.

[20] Internet: A. Cho, IBM promises 1000-qubit quantum computer—a milestone—by 2023. https://www.sciencemag.org/news/2020/09/ibm-promises-1000-qubit-quantum-computer-milestone-2023, 19.11.2020.

[21] J. P. Dowling, G. J. Milburn, "Quantum technology: the second quantum revolution", *Philosophical Transactions of the Royal Society of London*. Series A: Mathematical, Physical and Engineering Sciences, 361(1809), 1655-1674, 2003.

[22] E. Conrad, S. Misenar, J. **Feldman, Eleventh Hour CISSP: Study Guide.** Syngress, 77-93, 2014.

[23] N. Chandra, S. Parida, "Quantum Entanglement in Photon-Induced Electron Spectroscopy of Atoms and Molecules: Its Generation, Characterization, and Applications", In *Advances in Imaging and Electron Physics*, 196, 1-164, 2016.

[24] O. Goldreich, "Foundations of cryptography: volume 1, basic tool", *Cambridge university press*, 2007.

[25] T. W. Edgar, D. O. Manz, "Research methods for cyber security", *Syngress*, 2017.

[26] Internet: What is cryptanalysis?, Security Degree Hub. https://www.securitydegreehub.com/what-is-cryptanalysis/, 26.04.2020.

[*27*] T. Speed, J. Ellis, **Internet Security,** Elsevier, Digital Press, 2003.

[28] D. Serpanos, T. Wolf, **Architecture of network systems.** Elsevier. 2011.

[29] C. Kiennert, S. Bouzefrane, P. Thoniel, "Authentication Systems", **In Digital Identity Management,** Elsevier, 95-135, 2015.

[30] N. A. Hassan, R. Hijazi, **Data hiding techniques in Windows OS: a practical approach to investigation and defense**. Syngress, 2017.

[31] Internet: M. Rouse, What is Data Encryption Standard (DES)? - Definition from WhatIs.com. https://searchsecurity.techtarget.com/definition/Data-Encryption-Standard, 11.03.2020.

[32] Internet: R. Gamby, Is the 3DES encryption algorithm the best choice for S/MIME protocol?, https://searchsecurity.techtarget.com/answer/Is-the-3DES-encryption-algorithm-the-best-choice-for-S-MIME-protocol, 12.03.2020.

[*33*] Internet: J. Callas, Triple DES: How strong is the data encryption standard?. https://searchsecurity.techtarget.com/tip/Expert-advice-Encryption-101-Triple-DES-explained, 20.03.2020.

[34] Internet: M. Rouse, What is AES encryption and how does it work? SearchSecurity. https://searchsecurity.techtarget.com/definition/Advanced-Encryption-Standard, 25.03.2020.

[35] L. Li, J. Fang, J. Jiang, L. Gan, W. Zheng, H. Fu, G. Yang, "Efficient AES implementation on Sunway TaihuLight supercomputer: A systematic approach", *Journal of Parallel and Distributed Computing*,138, 178-189, doi: 10.1016/j.jpdc.2019.12.013, 2020.

[36] D. Rountree, **Security for Microsoft Windows System Administrators Introduction to Key Information Security Concepts**, Elsevier, Pages 29-69. ISBN 978-1-59749-594-3. 2011.

[37] M. Dušek, N. Lütkenhaus, M. Hendrych, "Quantum cryptography", *Progress in Optics*, 49, 381-454, 2006.

[38] Internet: K. Martin, Waiting for quantum computing: Why encryption has nothing to worry About, https://techbeacon.com/security/waiting-quantum-computing-why-encryption-has-nothing-worry-about, 28.03.2020.

[39] Internet: M. Chapple, Diffie-Hellman key exchange, https://searchwindowsserver.techtarget.com/tip/Diffie-Hellman-key-exchange, 25.03.2020.

[40] D. J. Bernstein, "Curve25519: New Diffie-Hellman Speed Records", **Public Key Cryptography - PKC 2006, PKC 2006**, Eds: Yung, M., Dodis, Y., Kiayias, A., Malkin, T., Lecture Notes in Computer Science, vol 3958. Springer, Berlin, Heidelberg, 2006.

[41] W. Atkins, (2004). **The Smart Card Report,** Elsevier, 2004.

[42] Internet: K. FIlali, Shor's algorithm in c++. Retrieved from https://medium.com/@kfila1/shors-algorithm-in-c-52920e8f4f1c, 20.03.2020.

[43] Internet: How the Crypto World Is Preparing for Quantum Computing, Explained. Retrieved from https://cointelegraph.com/explained/how-the-crypto-world-is-preparing-for-quantum-computing-explained, 25.02.2020.

[44] J. Andress, **The basics of information security: understanding the fundamentals of InfoSec in theory and practice.** Syngress, 2014.

[45] Internet: Cryptographic hash functions definition. Investopedia. https://www.investopedia.com/news/cryptographic-hash-functions/, 17.03.2020.

[46] Internet: What is hashing? Benefits, types and more, https://www.2brightsparks.com/resources/articles/introduction-to-hashing-and-its-uses.html, 12.02.2020.

[47] Internet: D. Danyal, Kuantum Hesaplamanın Günümüz Şifrelemesine https://medium.com/@devrimdanyal/kuantum-hesaplaman%C4%B1n-g%C3%BCn%C3%BCm%C3%BCz-%C5%9Fifrelemesine-etkisi-cb42eb8516bc, 14.03.2020.

[48] Internet: M. Rouse, What is MD5? - Definition from WhatIs.com. SearchSecurity, https://searchsecurity.techtarget.com/definition/MD5, 15.04.2020.

[49] Internet: M. Cobb, *MD5 security: Time to migrate to SHA-1 hash algorithm?*. SearchSecurity. https://searchsecurity.techtarget.com/answer/MD5-security-Time-to-migrate-to-SHA-1-hash-algorithm, 10.03.2020.

[50] Internet: M. Bohm, What is SHA-1?, https://www.quora.com/What-is-SHA-1, 07.03.2020.

[51] FIPS PUB, **Secure hash standard**, Public Law, 1995.

[52] Internet: U. Mathew, What is SHA-256, SHA2, and why is it used?, https://www.quora.com/What-is-SHA-256-SHA2-and-why-is-it-used, 23.03.2020.

[53] Internet: Cryptographic hash functions explained: A beginner's guide, https://komodoplatform.com/cryptographic-hash-function/, 25.03.2020.

[54] Internet: J. Adley, S. Evangelist, What is the SHA-256 fingerprint?, https://www.quora.com/What-is-the-SHA-256-fingerprint, 16.03.2020.

[55] X. Q. Tan, "Introduction to quantum cryptography", **Theory and Practice of Cryptography and Network Security Protocols and Technologies**, Ed: Sen, J., 2013.

[56] C. Yu, F. Gao, S. Lin, W. Jingbo, "Quantum data compression by principal component analysis", *Quantum Inf Process*, 18, 249, doi: 10.1007/s11128-019-2364-9, 2019.

[57] J. Shi, S. Chen, Y. Lu, Y. Feng, R. Shi, Y. Yang, J. Li, "An Approach to cryptography Based on continuous-Variable Quantum neural network", *Scientific Reports*, 10(1), 1-13, doi: 10.1038/s41598-020-58928-1, 2020.

[58] Internet: Chris Cesare, Nature magazine, Cryptographers Brace for Quantum Revolution, https://www.scientificamerican.com/article/cryptographers-brace-for-quantum-revolution, 27.03.2020.

[59] Internet: D. Powell, The Race To Prove 'Spooky' Quantum Connection May Have a Winner, https://www.popsci.com/race-prove-spooky-quantum-connection-may-have-winner/, 13.03.2020.

[60] M. Campagna, L. Chen, O. Dagdelen, J. Ding, J. Fernick, N. Gisin, B. Neill, "Quantum Safe Cryptography and Security: An introduction, benefits, enablers and challenges", *European Telecommunications Standards Institute*, 1-64, 2015.

[61] W. Buchanan, A. Woodward, "Will quantum computers be the end of public key encryption?", *Journal of Cyber Security Technology*, 1(1), 1-22. 2017.

[62] Internet: D. Voorhoede, What is a quantum algorithm?, https://www.quantum-inspire.com/kbase/what-is-a-quantum-algorithm/, 11.04.2020.

[63] A. Montanaro, "Quantum algorithms: an overview", *npj Quantum Information*, *2*(1), 1-8, doi: 10.1038/npjqi.2015.23., 2016.

[64] P. W. Shor, "Algorithms for quantum computation: discrete logarithms and factoring," **Proceedings 35th Annual Symposium on Foundations of Computer Science**, Santa Fe, NM, USA, pp. 124-134, 1994.

[65] Internet: P. Hacker, How does Shor's algorithm work in Layman's terms?, https://www.quora.com/How-does-Shors-algorithm-work-in-laymans-terms, 14.03.2020.

[66] Internet: S. Wehner, Quantum computing: An intuitive explanation of GROVER's Algorithm, https://www.linkedin.com/pulse/quantum-computing-intuitive-explanation-grovers-algorithm-sam-wehner, 16.03.2020.

[67] L. K. Grover, "Quantum mechanics helps in searching for a needle in a haystack", *Physical review letters*, 79(2), 325, 1997.

[68] D. J. Bernstein, T. Lange, "Post-quantum cryptography", *Nature*, 549(7671), 188-194, doi:10.1038/nature23461, 2017.

[69] Internet: Grover's Search Algorithm, https://www.quantiki.org/wiki/grovers-search-algorithm, 12.04.2020.

[70] P. Zeng, S. Chen, K. K. R. Choo, "An IND-CCA2 secure post-quantum encryption scheme and a secure cloud storage use case", *Human-centric Computing and Information Sciences*, *9*(1), 1-15. doi: 10.1186/s13673-019-0193-6, 2019.

[71] J. Daemen, V. Rijmen, "The design of Rijndael: AES-the advanced encryption standard", *Springer Science & Business Media*, 2013.

[72] A. Beşkirli, D. Özdemir, M. Beşkirli, "Şifreleme Yöntemleri ve RSA Algoritması Üzerine Bir İnceleme", *Avrupa Bilim ve Teknoloji Dergisi*, 284-291, 2019.

[73] M. Robshaw, O. Billet, **New stream cipher designs: the eSTREAM finalists,** Springer, 2008.

[74] D. A. McGrew, J. Viega, "The security and performance of the Galois/Counter Mode (GCM) of operation", **International Conference on Cryptology**, Springer, Berlin, Heidelberg, 2004.

[75] D. J. Bernstein, "The Poly1305-AES message-authentication code", **International Workshop on Fast Software Encryption**, Springer, Berlin, Heidelberg, 32-49, 2005.

[76] Q. H. Dang, "Secure hash standard (No. Federal Inf. Process. Stds.(NIST FIPS)-180-4)", doi: 10.6028/NIST.FIPS.180-4, 2015.

[77] Internet: How many qubits are required to break RSA 2048 or 4096 with a universal quantum computer?, https://crypto.stackexchange.com/questions/35137/how-many-qubits-are-required-to-break-rsa-2048-or-4096-with-a-universal-quantum#, 19.03.2020.

[78] R. L. Rivest, A. Shamir, L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems", *Communications of the ACM*, 21(2), 120-126, 1978.

[79] W. Diffie, M. Hellman, "New directions in cryptography", *IEEE transactions on Information Theory*, 22(6), 644-654, 1976.

[80] T. ElGamal, "A public key cryptosystem and a signature scheme based on discrete logarithms", *IEEE transactions on information theory*, *31*(4), 469-472, 1985.

[81] C. P. Schnorr, "Efficient identification and signatures for smart cards", **Conference on the Theory and Application of Cryptology,** 239-252, Springer, New York, NY, 1989.

[82] V. S. Miller, "Use of elliptic curves in cryptography", **Conference on the theory and application of cryptographic techniques,** 417-426, Springer, Berlin, Heidelberg, 1985.

[83] N. Koblitz, "Elliptic curve cryptosystems", *Mathematics of computation*, 48(177), 203-209, 1987.

[84] E. T. Campbell, B. M. Terhal, C. Vuillot, "Roads towards fault-tolerant universal quantum computation", *Nature*, 549(7671), 172-179, 2017.

[85] D. Johnson, A. Menezes, S. Vanstone, "The elliptic curve digital signature algorithm (ECDSA)", *International journal of information security*, *1*(1), 36-63, 2001.

[86] D. J. Bernstein, N. Duif, T. Lange, P. Schwabe, B. Y. Yang, "High-speed high-security signatures", *Journal of cryptographic engineering*, *2*(2), 77-89, 2012.

[87] Internet: L. Martin, Is the newest quantum breakthrough an encryption killer?, https://techbeacon.com/security/newest-quantum-breakthrough-encryption-killer, 15.04.2020.

[88] Internet: S. Sham, "The impact of quantum computing on cybersecurity", https://www.okta.com/security-blog/2019/07/the-impact-of-quantum-computing-on-cybersecurity/, 11.04.2020.

[89] Internet: Post-quantum cryptography | CSRC, https://csrc.nist.gov/Projects/post-quantum-cryptography, 28.04.2020.