T.C.
HARRAN ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

YÜKSEK LİSANS TEZİ

BB84 YÖNTEMİ KULLANILARAK KUANTUM ŞİFRELEME BENZETİM ORTAMI GELİŞTİRİLMESİ

İdris TÜRKER

ELEKTRİK ELEKTRONİK MÜHENDİSLİĞİ ANABİLİM DALI

ŞANLIURFA
2018

T.C.
HARRAN ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

YÜKSEK LİSANS TEZİ

BB84 YÖNTEMİ KULLANILARAK KUANTUM ŞİFRELEME BENZETİM ORTAMI GELİŞTİRİLMESİ

İdris TÜRKER

ELEKTRİK ELEKTRONİK MÜHENDİSLİĞİ ANABİLİM DALI

ŞANLIURFA
2018

Dr. Öğr. Üyesi Mehmet Akif NACAR danışmanlığında, İdris TÜRKER'in hazırladığı "**BB84 Yöntemi Kullanılarak Kuantum Şifreleme Benzetim Ortamı Geliştirilmesi**" konulu bu çalışma 30/10/2018 tarihinde aşağıdaki jüri tarafından oy birliği ile Harran Üniversitesi Fen Bilimler Enstitüsü Elektrik Elektronik Mühendisliği Anabilim Dalı'nda YÜKSEK LİSANS TEZİ olarak kabul edilmiştir.

İmza

Danışman: Dr. Öğr. Üyesi Mehmet Akif NACAR ……

Üye: Dr. Öğr. Üyesi İbrahim Berkan AYDİLEK ……

Üye: Dr. Öğr. Üyesi Faruk KÜRKER ……

Bu Tezin Elektrik Elektronik Mühendisliği Anabilim Dalında Yapıldığını ve Enstitümüz Kurallarına Göre Düzenlendiğini Onaylarım.

Prof. Dr. Halil Murat ALĞIN
Enstitü Müdürü

Not: Bu tezde kullanılan özgün ve başka kaynaktan yapılan bildirişlerin, çizelge, şekil ve fotoğrafların kaynak gösterilmeden kullanımı 5846 sayılı Fikir ve Sanat Eserleri Kanunundaki hükümlere tabidir.

İÇİNDEKİLER

Sayfa No

ÖZET i
ABSTRACT ii
TEŞEKKÜR iii
ŞEKİLLER DİZİNİ iv
ÇİZELGELER DİZİNİ vi
1. GİRİŞ 1
2.ÖNCEKİ ÇALIŞMALAR 6
2.1.Klasik Şifreleme Teknikleri 6
2.1.1.Yerine koyma yöntemi 6
2.1.1.1.Tek alfabetik yerine koyma metodu 7
2.1.1.2.Çok alfabeli yerine koyma metodu 8
2.1.2.Yer değiştirme yöntemi 11
2.2.Modern Şifreleme Teknikleri 13
2.2.1.Simetrik şifreleme 14
2.2.1.1.Blok şifreleme 14
2.2.1.2.Akış şifreleme 16
2.2.2.Asimetrik şifreleme 16
2.3.Kuantum Şifreleme 19
3.MATERYAL ve YÖNTEM 25
3.1.Kuantum Kriptolojisi 25
3.2.Kuantum Kriptolojisinin Amacı 25
3.3.Kuantum Anahtar Dağıtım Yöntemi 25
3.3.1.BB84 protokolü 26
3.3.2.B92(Bennet 1992) protokolü 30
3.3.3.SARG04(Scarani&Acin&Ribordy&Gisin) protokolü 32
3.3.4.E91 protokolü 34
3.4.Yapılan Çalışmalar 35
3.4.1.BB84 protokolü algoritması 35
3.4.2.CASCADE (Hata Tespit ve Düzeltme) protokolü algoritması 40
3.4.3.Vernam şifreleme algoritması 47
3.5.Uygulama 52
3.5.1.BB84 protokol uygulaması 52
3.5.2.CASCADE protokol uygulaması 61
3.5.3.Vernam şifreleme uygulaması 66
4.SONUÇLAR ve ÖNERİLER 71
4.1.Sonuçlar 71
4.2.Öneriler 72
KAYNAKLAR 74
ÖZGEÇMİŞ 76

ÖZET

Yüksek Lisans Tezi

BB84 YÖNTEMİ KULLANILARAK KUANTUM ŞİFRELEME BENZETİM ORTAMI GELİŞTİRİLMESİ

İdris TÜRKER

Harran Üniversitesi
Fen Bilimleri Enstitüsü
Elektrik Elektronik Mühendisliği Anabilim Dalı

Danışman: Dr. Öğr. Üyesi Mehmet Akif NACAR
Yıl: 2018, Sayfa: 76

Aynı kurum içerisinde güvenlik politikaları sebebi ile ayrı network sistemlerinin kullanıldığı alanlarda dış ataklara karşı güvenli bir veri iletişimi gerçekleştirile bilmesi gerekmektedir. Bunun için anahtarlı şifreleme tekniği içersinde en ciddi güvenlik problemi olan tahmin edilmesi zor anahtarın belirlenmesi ve belirlenen anahtar üzerinden veri iletişim işleminin başlamasıdır. Bu gerekçelerle veri iletişim sırasında hattın dinlenmesi anlaşılabilir bir ortam ve öngörülen bir anahtarın kullanılması gerekmektedir. Bu sebep dolayısıyla kuantum şifreleme tekniğinde anahtar belirleme işlemi fiber optik hat içerisindeki fotonların davranışları ile gerçekleşmektedir. Bu teknik kullanılarak Gönderici olarak tanımlanan taraf ile Alıcı olarak tanımlanan taraf arasında ortak bir anahtar oluşturma işlemi yapılmaktadır. Gönderici, düz ve köşegen tipte iki filtre kullanarak dört farklı foton polarizasyonu elde etmektedir. Gönderici tarafından üretilen fotonlar Alıcı tarafından düz ya da köşegen tipteki rastgele üretilen filtreden geçirilir. Gönderici ve Alıcı tarafından eşleşen filtrelerle ortak anahtar üretimi gerçekleşmektedir. Fiber optik hattında bir gürültü varsa veya bir Gizli Dinleyici söz konusuysa, Gönderici ve Alıcı tarafından üretilen ortak anahtarda benzerlik olmayacaktır. Fiber optik hattan geçen fotonların hata oranı % 27,6 veya daha az olmalıdır. Belirtilen oran bu değerin üzerindeyse, iletişim gerçekleştirilmez. Yapılan çalışma, belirlenen senaryo ve çevrimiçi ortam ile BB84 Kuantum anahtar dağıtım protokolünü kullanarak gürültülü ortamdaki anahtar üretimini simüle etmektir. Gönderici ve Alıcı arasında oluşan ortak anahtarda eşleşmeyen bitler için CASCADE Protokolü olarak kabul edilen teknik kullanılır. Hata tespit ve düzeltme bu protokol ile gerçekleştirilir. Kullanılan yöntem, gerçek ortamda önemli bir maliyet gerektirdiğinden, test ve yorumlama için bir ortam oluşturmuştur.

ANAHTAR KELİMELER: Kuantum Şifreleme, Kuantum Anahtar Dağıtımı, BB84 Algoritması, Cascade Protokolü,

ABSTRACT

MSc Thesis

DEVELOPMENT OF QUANTUM ENCRYPTION SIMULATION ENVIRONMENT USING BB84 METHOD

İdris TÜRKER

Harran University
Graduate School of Natural and Applied Sciences
Department of Electrical Electronics Engineering

Supervisor: Assist. Prof. Dr. Mehmet Akif NACAR
Year: 2018, Page:76

In the same institution, it is necessary to have secure data communication against external attacks in areas where separate network systems are used due to security policies. For this purpose, the most important security problem in the key encryption technique is to determine the hard to guess key and start the data communication process with the specified key. For these reasons, it is necessary to use an understandable environment and an unpredictable key to listen to the line during data communication. For this reason, the key determination process in quantum encryption technique is realized by the behavior of photons in the fiber optic line. By using this technique, a common key creation is made between Alice, defined as the sender side and Bob, defined as the receiving side. Alice uses flat and diagonal two type filter to obtain four different photon polarizations. The photons produced by Alice are filtered by a flat or diagonal type randomly produced by Bob. Alice and Bob's a common key generation by matching the filter is realized. If there is a noise in the fiber optic line or a listener (Eva), there will be no similarity in the common key produced by Alice and Bob. The error rate of photons passing through the fiber optic line should be 27.6% or less. If the specified ratio is above this value, communication is not performed. The work done is simulating the production of key in the noisy environment using the online environment and the BB84 Quantum key distribution protocol. The common key that is formed between Alice and Bob use the technique that is considered as CASCADE Protocol for non-matching bits. Error detection and correction is performed with this protocol. The method used has created an environment for testing and interpretation as it requires a significant cost in the real environment.

KEY WORDS: Encryption, Quantum Encryption, Quantum Key Distribution, BB84 Algorithm, Cascade Protocol

TEŞEKKÜR

Bu çalışmanın gerçekleştirilmesinde, değerli bilgilerini bizlerle paylaşan, kullandığı her kelimenin hayatıma kattığı önemini asla unutmayacağım saygıdeğer danışman hocam; Dr. Öğr. Üyesi Mehmet Akif NACAR'a, çalışmam boyunca benden bir an olsun yardımlarını esirgemeyen değerli hocam Araştırma Görevlisi Mehmet Emin TENEKECİ'ye, bilgi paylaşımlarından dolayı değerli arkadaşım Bahadır DEMİRCİOĞLU'na, katkılarından dolayı değerli jüri hocalarım Dr. Öğr. Üyesi İbrahim Berkan AYDİLEK ile Dr. Öğr. Üyesi Faruk KÜRKER'e ve çalışma süresince tüm zorlukları benimle göğüsleyen ve hayatımın her evresinde bana destek olan değerli aileme sonsuz teşekkürlerimi sunarım.

ŞEKİLLER DİZİNİ

Sayfa No

Şekil 1.1. Harran Üniversitesi Araştırma Hastanesi ile Harran Üniversitesi Arasındaki Veri İletişimi 1
Şekil 1.2. Mısır Hiyeroglifi 3
Şekil 1.3. Şifreleme Türleri 4
Şekil 2.1. Şifreleme Teknikleri Diyagramı 6
Şekil 2.2. Üç Harf Atlamalı Sezar Şifresi 7
Şekil 2.3. Alberti Şifreleme Diski 8
Şekil 2.4. Jefferson'un Disk Şifresi 9
Şekil 2.5. Enigma 10
Şekil 2.6. Eniac 11
Şekil 2.7. Bir Scytale 12
Şekil 2.8. ADFGVX Şifreleme 13
Şekil 3.1. BB84 Protokolünde Polarizasyon Kubit Değeri Eşleşmesi 26
Şekil 3.2. Kuantum Anahtar Dağıtımı Modeli 27
Şekil 3.3. Anahtar Bitlere Karar Verilmesi 28
Şekil 3.4. Hattın Dinlenmesi ve Sonuçları 29
Şekil 3.5. B92 Protokolünde Polarizasyon-Kubit Değeri 31
Şekil 3.6. B92 Protokolünde Okuma Basamağındaki Polarizasyon-Kubit Değeri 31
Şekil 3.7. SARG Protokolü İçin Polarizasyon-Kubit Değeri Eşleşmesi 33
Şekil 3.8. Gönderici - Kuantum Kanal Üzerindeki İletişim Diyagramı 35
Şekil 3.9. Gönderici Foton Oluşturma Diyagramı 36
Şekil 3.10. Alıcı - Kuantum Kanal Üzerindeki İletişim Diyagramı 37
Şekil 3.11. Alıcı Foton Oluşturma Diyagramı 38
Şekil 3.12. Gönderici - Alıcı Klasik Kanal Üzerinden İletişim 39
Şekil 3.13. CASCADE Hata Bulma Diyagramı 42
Şekil 3.14. Diziyi Karıştırmak için Kullanılan Algoritmanın Diyagramı 43
Şekil 3.15. Bloklara Ayrılmış Dizinin Parity Değerini Hesaplama Algoritması Diyagramı 44
Şekil 3.16. Gönderici - Alıcı Parity Değerlerin Karşılaştırma Algoritma Diyagramı 45
Şekil 3.17. Hatalı Bit Bulmak için Kullanılan Algoritma Diyagramı 46
Şekil 3.18. Hata Toleransı Hesaplamak için Kullanılan Algoritma Diyagramı 47
Şekil 3.19. Vernam Encrypt Algoritması Akış Diyagramı 49
Şekil 3.20. Vernam Decrypt Algoritması Akış Diyagramı 50
Şekil 3.21. Vernam Algoritması Akış Diyagramı 51
Şekil 3.22. BB84 Simülasyonun Foton Sayısı 50, Kayıp ve Dinleme Olmadan Çalıştırması 52
Şekil 3.23. Foton Sayısı 50, Kayıp ve Dinleme Olmadan Gönderici Tarafından Oluşan Simülasyon Sonucu 52
Şekil 3.24. Foton Sayısı 50, Kayıp ve Dinleme Olmadan Alıcı Tarafından Oluşan Simülasyon Sonucu 53
Şekil 3.25. Simülasyonun Foton Sayısı 50, Kaybın Olup ve Dinlemenin Olmadığı Şekilde Çalıştırması 54
Şekil 3.26. Foton Sayısı 50, Kaybın Olup ve Dinlemenin Olmadığı Ortamda Gönderici Tarafından Oluşan Simülasyon Sonucu 54
Şekil 3.27. Foton Sayısı 50, Kaybın Olup ve Dinlemenin Olmadığı Ortamda Alıcı Tarafından Oluşan Simülasyon Sonucu 55
Şekil 3.28. Simülasyonun Foton Sayısı 50, Kaybın Olmadığı ve Dinlemenin Olduğu Şekilde Çalıştırması 56
Şekil 3.29. Foton Sayısı 50, Kaybın Olmadığı ve Dinlemenin Olduğu Ortamda Gönderici Tarafından Oluşan Simülasyon Sonucu 56
Şekil 3.30. Foton Sayısı 50 Gizli Dinleyici Tarafından Oluşan Simülasyon Sonucu 57
Şekil 3.31. Foton Sayısı 50, Kaybın Olmadığı ve Dinlemenin Olduğu Ortamda Alıcı Tarafından Oluşan Simülasyon Sonucu 57

Şekil 3.32. Simülasyonun Foton Sayısı 50, Kayıp ve Dinlemenin Olduğu Şekilde Çalıştırması 59
Şekil 3.33. Foton Sayısı 50, Kayıp ve Dinlemenin Olduğu Ortamda Gönderici Tarafından Oluşan Simülasyon Sonucu 59
Şekil 3.34. Sayısı 50 Gizli Dinleyici Tarafından Oluşan Simülasyon Sonucu 60
Şekil 3.35. Foton Sayısı 50, Kayıp ve Dinlemenin Olduğu Ortamda Alıcı Tarafından Oluşan Simülasyon Sonucu 60
Şekil 3.36. Foton Sayısı 50, Kayıp ve Dinleme Olmadan Oluşan Simülasyonda CASCADE İşlemini Uygulanması 62
Şekil 3.37. Foton Sayısı 50, Kaybın Olup ve Dinleme Olmadan Oluşan Simülasyonda CASCADE İşlemini Uygulanması 63
Şekil 3.38. Foton Sayısı 50, Kaybın Olmayıp ve Dinlemenin Olup Oluşan Simülasyonda CASCADE İşlemini Uygulanması 64
Şekil 3.39. Foton Sayısı 50, Kayıp ve Dinleme Olup Oluşan Simülasyonda CASCADE İşlemini Uygulanması 65
Şekil 3.40. Gönderici Vernam Şifreleme Uygulaması 66
Şekil 3.41. Alıcı Vernam Şifre Çözme Uygulaması 67
Şekil 3.42. Vernam Uygulaması ile Oluşturulan Dosyalar 67
Şekil 3.43. Foton Sayısı 50, Kayıp ve Dinleme Olmadan Simülasyonda Gönderici ve Alıcı Tarafından Üretilen Anahtar Dosyaları 68
Şekil 3.44. Foton Sayısı 50, Kaybın Olup ve Dinleme Olmadan Simülasyonda Gönderici ve Alıcı Tarafından Üretilen Anahtar Dosyaları 69
Şekil 3.45. Foton Sayısı 50, Kaybın Olmayıp ve Dinlemenin Olduğu Simülasyonda Gönderici ve Alıcı Tarafından Üretilen Anahtar Dosyaları 69

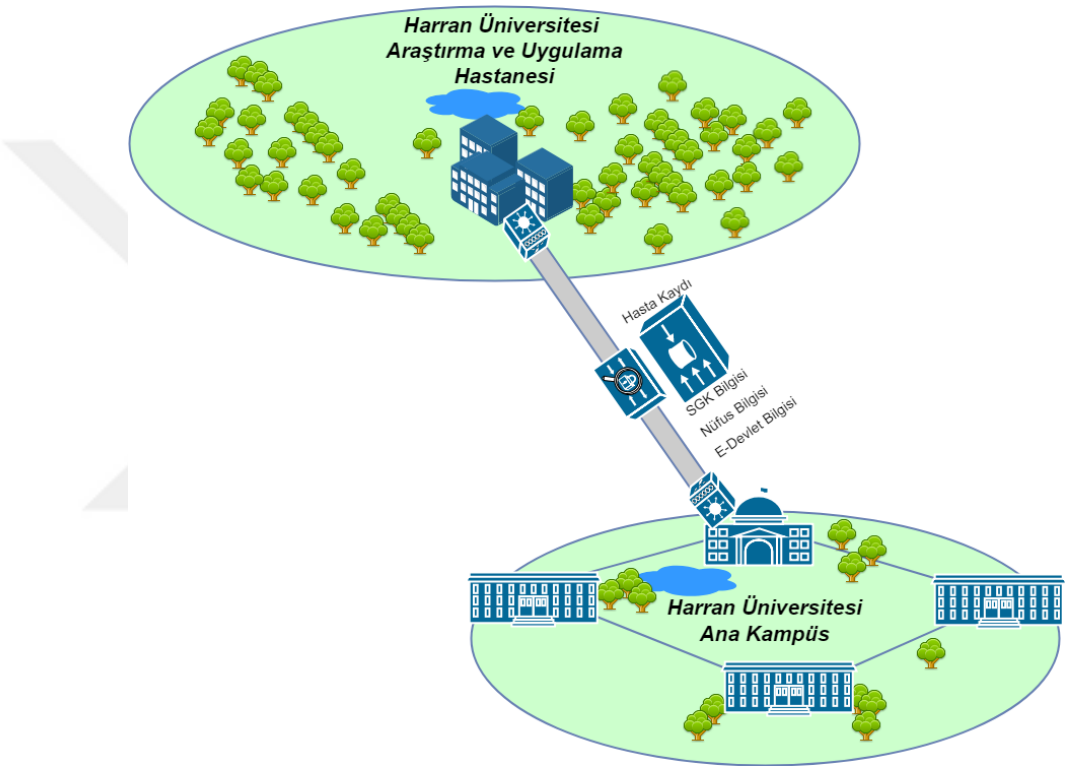
ÇİZELGELER DİZİNİ

Sayfa No

Çizelge 3.1. B92 Protokolü iletimi ile Yapılan Altı Kubitte Olası Okuma Sonuçları 32
Çizelge 3.2. B92 Protokolü iletimi ile Yapılan Altı Kubitte Olası Okuma Sonuçları 32
Çizelge 3.3. 0 Derece Açı ile Polarizasyona Sahip Bir Fotonun Olası İhtimallerinde SARG Protokolü ile Altı Farklı İletimi 34

1. GİRİŞ

Harran Üniversitesi Ana Kampüsü ile Harran Üniversitesi Araştırma ve Uygulama Hastanesi arasında kanuni olarak gizliliği zorunlu olan hasta bilgilerinin, güvenli bir veri iletişim ortamı oluşturup bu ortamdan işlemlerin gerçekleştirilip simüle edilmesi hedeflenmektedir.



Şekil 1.1. Harran Üniversitesi Araştırma ve Uygulama Hastanesi ile Harran Üniversitesi Ana Kampüs Arasındaki Veri İletişimi

Şekil 1.3.'de görüldüğü üzere üniversite ile üniversite hastanesi arasındaki bilgi alışverişi için kullanılan hattaki hasta bilgilerinin mahremiyeti önem taşımaktadır. Bu konu ile ilgili;

- 2016 yılında kabul edilen **Kişisel Verilerin Korunması Kanunu**
- 1980 tarihli **Mahremiyetin Korunması ve Kişisel Verilerin Sınır Ötesi Akışına İlişkin Rehber İlkeleri**

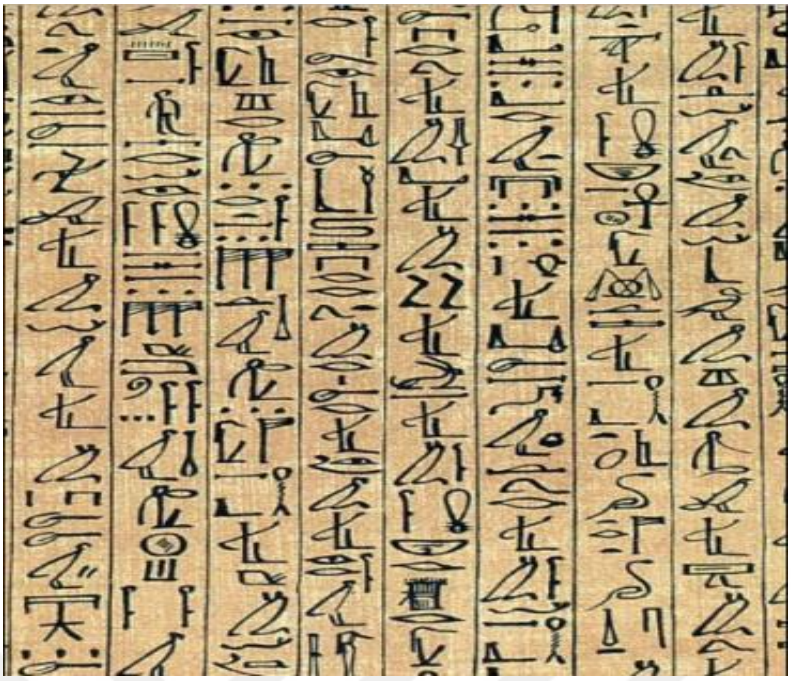
- 1981 tarihinde Avrupa Konseyi tarafından hazırlanan **Kişisel Nitelikteki Verilerin Otomatik İşleme Tabi Tutulması Karşısında Şahısların Korunmasına Dair 108 Sayılı Sözleşme**
- 1990 tarihinde Birleşmiş Milletler tarafından hazırlanan **45/95 sayılı Kişisel Veri Dosyalarının Bilgisayar Aracılığıyla İşlenmesinde Genel İlkeler**

gibi ulusal ve uluslar arası alanda kişisel verilerin korunması ile ilgili düzenlemeler yapılmaktadır.

Harran Üniversitesi Araştırma ve Uygulama Hastanesi, hasta kayıt bilgilerinde doğrulama işlemi için Harran Üniversitesi Ana Kampüsünün kullanmış olduğu sistem üzerinden tanımlı olan yetki işlemini kullanarak işlemlerini gerçekleştirmektedir. Güvenlik politikaları gereği aynı kurum içerisinde olmalarına rağmen farklı network sistemlerine sahip olan bu iki yapı arasında hasta mahremiyetinden dolayı hasta bilgilerinin taşıma işlemi sırasındaki güvenlik, önem arz etmektedir. Ayrıca bu iki yapı arasındaki senkronize çalışan Elektronik Belge Yönetim Portali ve Personel Bilgi Portali gibi sistemlerdeki veri iletişimindeki gizlilik, ciddi önem gerektiren durumlardandır.

Kriptoloji ilk başlarda bir sanat yapıtı olarak 4000 yıl önce yaşamış bir kâtip'in efendisinin hayatının anlatırken hiyeroglifleri şifrelenmiş bir şekilde oluşturmuştu ve bazı hiyeroglifler daha önce hiç kullanılmamıştı.

Hiyeroglifler birbirinden kolaylıkla ayırt edilebilecek yüzlerce sembolden oluşur. Her işaret belli bir sesi veya nesneyi temsil eder. Bu yazı soldan sağa veya sağdan sola ya da yukarıdan aşağı yazılabilir, okumak için ölçüt sembollerdeki insan ya da hayvan figürlerinin baktıkları yöndür. Mısır hiyerogliflerinde 700'den fazla işaret bulunmaktadır (Anonim, 2015a).



Şekil 1.2. Mısır Hiyeroglifi

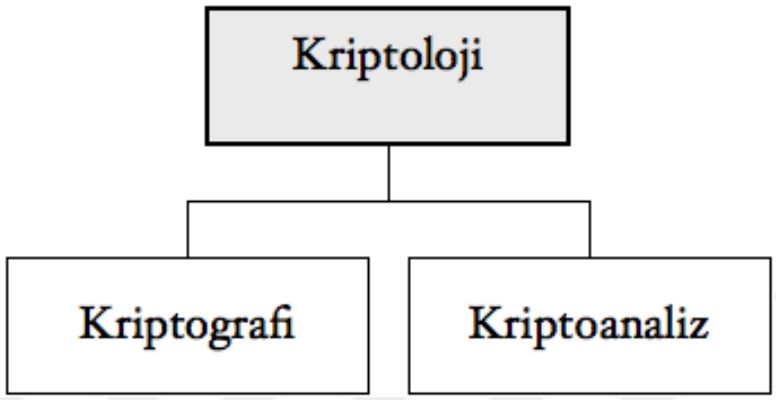
İnsan zekâsının sınırlarını zorlayan bu kavramı (kriptoloji) özellikle savaş dönemlerinde gelişme gösteren bir bilim dalı olarak karşımıza çıkmaktadır.

İkinci Dünya Savaşında savaşan ülkeler şifre bilimine oldukça fazla önem vermiş ve farklı şifreleme türleri bularak bu bilimin ileri düzeyde gelişmesini sağlamışlardır. Bu dönemde ülkelerin stratejik planlarını düzenlenmesinde oldukça önemli bir fonksiyonu bulunan kriptolojiyle birlikte, gönderilmek ve gizli tutulmak istenen iletiler oldukça farklı ve güvenli şifreleme türleriyle birlikte alıcılara ulaşmış ve bir nevi haberleşmenin en önemli noktalarından biri olmayı başarmıştır (Anonim, 2015a).

Şifreleme bilimi ismi ile tabir edilen bu türün, bir verinin saklı tutulması için bir sistem dâhilinde kapsamında belirli teknikler ile şifrelenmesidir. Tabi ki bu bilim için uğraş alanı bundan ibaret değildir. Bununla beraber şifreleme bilimi, şifrelenmiş mesajların deşifre edilmemesinde de çalışmalar içermektedir.

Ayriyeten şifreleme bilimi içerisinde iki türü bulunmaktadır. Bunlara Kriptografi (Şifreleme) ve Kriptoanaliz (Şifre çözme) isimleri ile tabir edilirler.

Anlam olarak şifreleme bilimi olan kriptoloji de kelime analizi gerçekleştirildiğinde, Eski Yunanca dilinde kullanılan kriptos kelimesi yazı'yı, graphi kelimesi ise gizlilik anlamına geldiği görülmektedir. Kriptoloji bu Eski Yunanca kelimelerin bir araya gelmesi ile türetilmiştir.



Şekil 1.3. Şifreleme Türleri

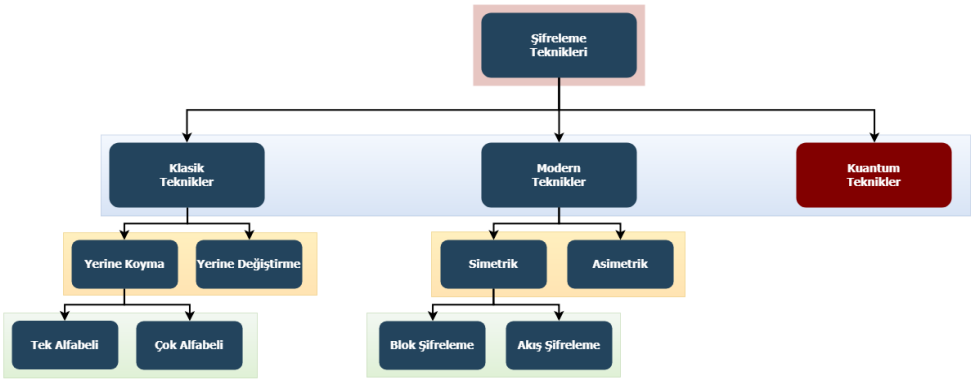
Günümüz çağında kriptoloji bilimi için kullanım alanında artış görülmektedir. Kuantum fiziğinden DNA incelemelerine, kriptografi ile alakalı olan pek çok bilimsel disiplin vardır (ANONİM, 2018). Siber savaşlara maruz kalan uluslar, bilgi güvenliğinde zafiyet yaşayan ülkelerde görülmektedir. Bu duruma sebep olan neden ise, teknolojinin çok hızlı bir şekilde ilerlemesi ve gelişmesidir. İnternet kullanımı, kriptoloji bilimi için kullanım alanını artmasına sebep olan etkenlerdendir. Nedeni ise internet kullanımının çağımızda popüler olması buna bağlı olarak güvenlik açığı problemleri oluşturmasıdır (Anonim, 2015b).

Özdağ (2009), "Enformasyon savaşına hazırlanamayan milletler 21. yüzyılda enformasyon savaşına hazırlanan milletler karşısında kızıl derililerin kovboylar karşısında düştüğü durumdan daha kötü duruma düşeceklerdir." diyor. Öyle görülmektedir ki siber saldırılar, hedef devletlerin birçok alanda stratejik bilgilerinin ele geçirmesi ve kendi menfaatleri doğrultusunda kullanmayı sağlaması için önemli bir konumda yer almaktadır. Bundan dolayı günümüzde ve gelecekte bilgi/veri güvenliği kritik ve önemli bir hale gelmiştir.

Birçok insanın internet bağlantısı sonucunda bilgisi dışında gerçekleşen sunucuya ulaşma talepleri (şifrelenmeden) doğrultusunda arada kullanılan network cihazlarının sistem yöneticisi tarafından izlenebilmesi ve hatta değiştirilebilmesi imkânı bulunmaktadır. Kişisel veya kurumsal çerçevede hassas ve gizlilik arz eden bilgilerin iletiminde bir nebzede olsa tasarlanmış şifreleme standartları/protokolleri mevcuttur. https:// kısaltması ile başlayan sitelere giriş yapıldığında internet tarayıcısındaki SSL uygulaması kullanmaktadır. SSL (Secure Sockets Layer), tarayıcı ve sunucu arasındaki şifrelenmiş iletişim sağlayan standarttır (Kaşkaloğlu, 2016).

Bilgisayar teknolojisi içerisinde beklenmekte olan en büyük yenilik kuantum bilgisayar kullanımının yaygınlaştırılmasıdır. Bu bilgisayarların çalışma mantığında kuantum yasaları görülmektedir. Kuantum bilgisayarlar içerisinde bilgi, atomun farklı iki durumunu kullanılarak saklayabileceği tahmin edilmektedir. Ancak ilginç olan şey atomun aynı zamanda her iki durum için de doğru olmasıdır. Atomik süper pozisyon karşısında kuantum bilgisayarlarında veri işlemek için saklama kapasitesinin ciddi oranlara ulaşılması ile RSA benzeri kırılma ihtimali zor görünen açık anahtarlı algoritmalarını kısa bir süre içerisinde kırılabilmektedir. Kuantum şifreleme Heisenberg belirsizlik ilkesini kullanır. Sistemin güvenliğini sağlamak için, fotonlardaki iki özelliğin aynı zaman içerisinde bilinmeyip ve iletişim sırasında fotonların kopyalanması işlemine izin verilmemesi öngörülebilir (Çimen ve ark., 2007).

2. ÖNCEKİ ÇALIŞMALAR



Şekil 2.1. Şifreleme Teknikleri Diyagramı

2.1. Klasik Şifreleme Teknikleri

Geçmiş yüzyıllarda insanlar bilgiyi saklama adına değişik saklama metotları kullanmıştır. Örneğin Eski Yunanlılar şifreli bir mesajı göndermek için köleleri kullanmışlardır. Mesajı göndermek için kölelerin saçlarını tıraş etmişler, daha sonra da gönderecekleri mesajı kölelerin kafasına yazarak saçlarının uzamasını beklemişlerdir. Birkaç ay sonra da köle hedefine doğru yola çıkmış ve gittiği yerde tekrar saçları tıraş edilerek mesajın okunması sağlanmıştır. Bu ve buna benzer teknikleri içeren klasik şifreleme teknikleri basit olarak tasarlanmış şifrelemelerdir.

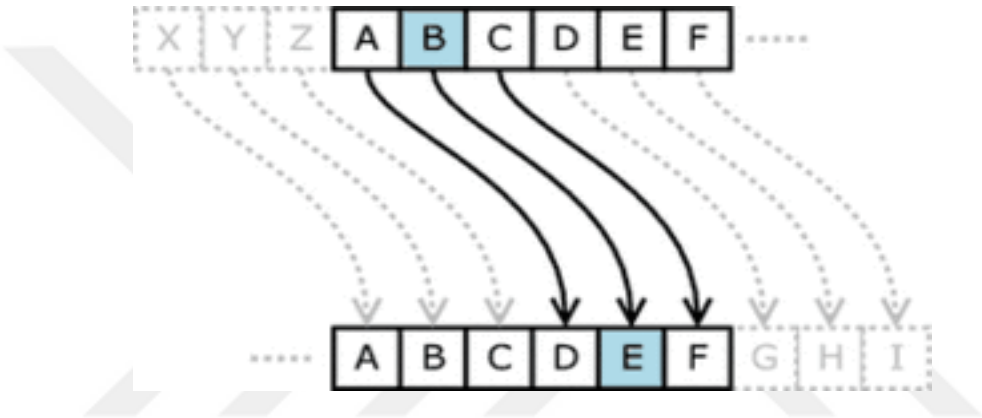
Klasik şifrelemenin tekniğinde iki temel esas bulunmaktadır. Bunlar yerine koyma (substitution) ve yer değiştirme (transposition) teknikleridir.

2.1.1. Yerine koyma yöntemi

Düz bir metindeki harflerin yerine başka harfler, sayılar ya da semboller koyarak yapılan şifreleme türüdür. İki tip yerine koyma metodu vardır. Bunlar Tekli Alfabetik Yerine Koyma ve Çoklu Alfabetik Yerine Koyma metotlarıdır.

2.1.1.1. Tek alfabetik yerine koyma metodu

Tarihteki ilk şifreleme fikir olarak, yer değiştirme ile harf değiştirme yöntemidir. Bu yöntemler ile birinci olarak bir metindeki harflerin yerlerinin değiştirilmesi, ikinci olarak harfleri farklı harfler ile değiştirilmesi ile elde edilmesidir. Sezar Şifresi bu tekniği kullanan en ünlü şifreleme yöntemidir. İlk olarak bu yöntem Sezar'ın generallerine bilgi göndermek işleminde uygulanmıştır. Bu tekniğin temel mantığı, her harf sonrasındaki harfi kullanarak yazılmasıdır (Bahadır ve Özdemir, 2012).



Şekil 2.2. Üç Harf Atlamalı Sezar Şifresi

Tek alfabeli şifre sistemlerinde ilk kripto analiz çalışmaları 9. Yüzyılda yaşamış olan Arap filozofu Al-Kindi tarafından yazılan Kriptografik Mesajların Deşifresi (Risâle fi'stihrâci'l-mu'ammâ) yazısı ile ortaya çıkmıştır. Bu yazıda Al-Kindi ilk olarak frekans analizi terimini öne sürmüştür. Al-Kindi'nin kripto analiz tekniğine göre yazıldığı dil bilinen şifrelenmiş iletiyi çözebilmek için, benzer dil kullanılarak yazılan uzunca bir metin içerisinde harflerin kullanım sıklığı hesaplanmalıdır. Metin içerisinde kullanılmış olan en sık harf, şifreli metin içerisinde de en sık kullanılmakta olan harfe denk gelmelidir. Bu yöntemin keşfedilmesi ile tek alfabeli şifreleme sistemlerinin güvensizliğini ispatlamıştır. Bu nedenle şifreleme tekniğinde birden fazla alfabe kullanılmıştır ve böylece çok alfabeli şifre sistemleri ortaya çıkmıştır (Çeşmeci, 2009; Çimen ve ark., 2008).

2.1.1.2. Çok alfabeli yerine koyma metodu

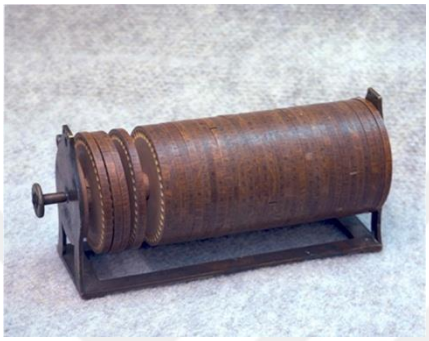
Çoklu alfabe kullanılarak ilk kripto çalışması 1466-1467 yılları arasında Leon Alberti tarafından yapılmıştır. Bu teknik Sezar şifreleme yöntemine benzemektedir. Sezar şifreleme yönteminden farklı olan kısmı ise kaydırma miktarının aynı olmamasıdır. Harflerin kaydırılması sırasında Alberti Diski kullanılmıştır. İç çemberi sabit, dış çemberi hareketli bu disk yardımıyla, her harfin istenilen miktarda ötelenmiş hali görülebilir (Canbek ve Sağıroğlu, 2006; Çeşmeci, 2009).



Şekil 2.3. Alberti Şifreleme Diski

1553 yıllarında Giovan Batista Belaso isimli bir İtalya vatandaşı tarafından geliştirilen çok alfabeli şifre uzun yıllar kırılamamıştır. Bu şifre,1586 yılında Fransız bir diplomat tarafından biraz daha geliştirilerek Vigenére Şifresi adını alan şifreleme tekniğinin orijinal halidir. Bu tekniğe göre açık metindeki her bir harf farklı alfabe şifreleri ile şifrelenir. Alfabe şifrelerinde hangisinin seçileceğine anahtar sözcüklere bakarak karar verir. Bu şekilde şifrelenmemiş metinde bulunan birbirine benzer sözcükler de aynı olmayan şifreli metinler oluşur. Bundan dolayı da frekans analizi yöntemi bu yöntemde tek başına yeterli gelmemektedir. Uzun yıllar kırılamayan bu yöntem 1854 ile 1863 yılları arasında Charles Babbage ve Friedrich Kasiski tarafından çözülmüştür (Canbek ve Sağıroğlu, 2006; Çeşmeci, 2009; Çimen ve ark., 2008).

1790 tarihinde Thomas Jefferson kendi soyadını verdiği Jefferson Diski sistemini yapmıştır. Bu diskin yapımında İngiliz alfabesi kullanılmıştır. İngiliz alfabesindeki tüm harfler 26 diskten oluşan sistemin üzerinde her diskin üzerine rastgele biçimde yerleştirilmiştir. Mesajın alıcısında ve vericisinde aynı özellikleri taşıyan Jefferson Diski bulunmak zorundadır. Şifre metni alan alıcı elindeki Jefferson Diski ile şifre metni oluşturup, geri kalan sıralardaki anlamlı metni çıkarmış olur (Çeşmeci, 2009; Çimen ve ark., 2008).



Şekil 2.4. Jefferson'un Disk Şifresi

Wheatstone-Playfair şifresi olarak bilinen ve Charles Wheatstone ve Baron Lyon Playfair tarafından 5x5'lik matris kullanılarak geliştirilmiş olan sistem 20.yüzyıl başlarına kadar güvenilirliğini korumuştur. Bu sistem de Jefferson Diski sistemi gibi İngiliz alfabesi için tasarlanmıştır. 5x5'lik matrisin her hücresine bir harf gelecek şekilde tasarlanan sistemde bir harf fazla gelmiştir. Bunun için de I ve J harfleri tek harf olarak düşünülmüştür. Bu şekilde tüm alfabe bir matris içine sığdırılmıştır. 20. Yüzyılın başlarında ikili harf frekans analizi ile kriptoanalizi gerçekleştirilmiştir. (Çeşmeci, 2009; Çimen ve ark., 2008).

İkinci Dünya Savaşın sırasında Almanya tarafından Enigma adlı bir kripto cihaz kullanılmıştır. Enigma makinesi temel olarak; klavyesinden girilen karakterlerin makine içerisinde birbiri ile değişik şekillerde algoritma oluşturacak şekillerde yazıları kodlayan üç adet diskten oluşmaktaydı. Polonyalı kripto analistler yapmış oldukları çalışmalarla Enigma ile şifrelenen mesajları çözmeyi başarmıştır. Bunun üzerine 1939 yılında Enigma'nın yapısı daha da karmaşıklaştırılmıştır. Bazı tarihçiler, Alman Enigma kod sisteminin deşifre olması sayesinde Avrupa'da savaşın iki yıl daha önce

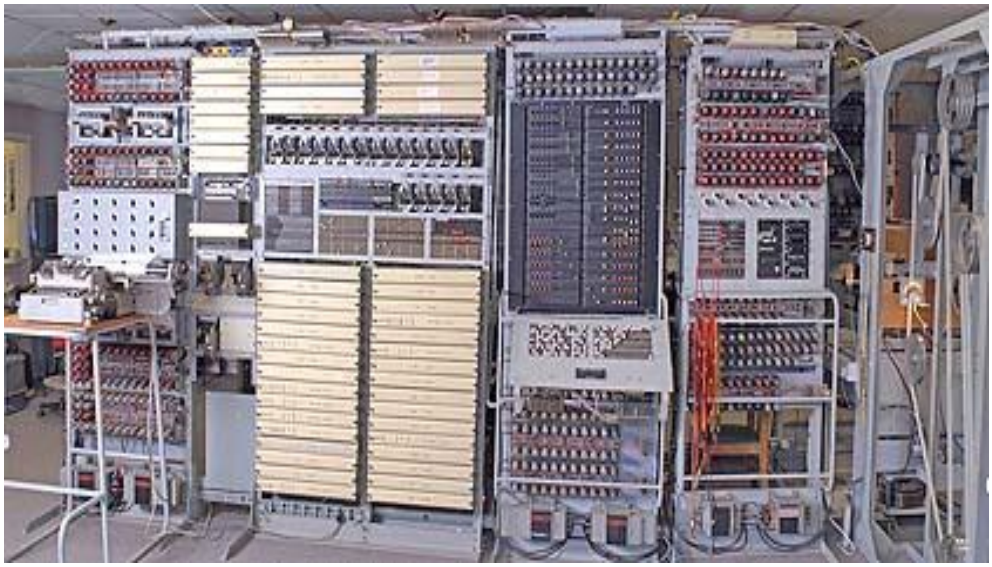
bittiğini ileri sürmektedirler (Canbek ve Sağıroğlu, 2006; Çeşmeci, 2009; Çimen ve ark., 2008; Kara, 2009).



Şekil 2.5. Enigma

Çok alfabeli şifreleme sistemlerinin örneklerinden biri olan Hill şifresi, 1929 yıllarında Leste Hill tarafından keşfedilmiştir. Bu şifreleme tekniği çok alfabeli şifrelerin pratik hale dönüştürülmesi bakımından oldukça önem taşımaktadır. Lester Hill ve ortağı 6x6'lık bloklarla Hill şifresinin uygulanabileceği bir makine geliştirmiştir, fakat bu makineye çok fazla talep olmamıştır (Çeşmeci, 2009; Çimen ve ark., 2008).

Enigma şifrelerini çözmek için 1943 yılında Colossus makinesi geliştirilmiştir. İlk elektronik bilgisayar olarak kabul edilen Colossus'un geliştirilmesi ile bilgisayarın babası denilebilecek Eniac ortaya çıkmıştır. Enigma'yı çözmek için kullanılan Eniac, Avrupa'da Hitler'in gücünü kırmıştır (Çeşmeci, 2009; Çimen ve ark., 2008; Kara, 2009).



Şekil 2.6. Eniac

1960'lı yıllarda ise daha farlı bir yöntem olan mor ötesi boya ile yazı yazılabilen kalemler icat edilerek fiziksel olarak veri aktarılmaya çalışılmıştır. Bu yöntem steganografi'de kullanılan yaygın yöntemlerden biridir (Canbek ve Sağıroğlu, 2006; Çeşmeci, 2009).

2.1.2. Yer değiştirme yöntemi

İlk kripto sistemine ise M. Ö. 400 yıllarında Spartalılar tarafından geliştirilen scytale örnek olarak verilebilir. Bu sistem ilk kriptografi cihazı olarak da anılmaktadır (Çeşmeci, 2009). Bu cihaz uzunca bir papirüsün veya parşömenin silindir olarak tabir edilen bir sopanın çevresine sarılması ile oluşturulmuştur. Şifrelenecek mesajın kelimeleri dikey ve her şerit turu sırasında bir harfin gelebildiği şekilde yazılmasıdır. Sonrasında açılan şerit ile ortaya anlamsız harflerden oluşan bir metin ortaya çıkar. Bu mesajın da çözülebilmesi için şifreleme işleminde kullanılan silindirle aynı çapa sahip bir silindire ihtiyaç vardır. Bu silindirin çağ değeri de kripto anahtarına denk gelir (Çimen ve ark., 2008).



Şekil 2.7. Bir Scytale

20. yüzyıl başlarında teknolojinin ilerlemesi ile beraber şifrelemenin önemi de artmıştır. Bilginin önemi artmasından kaynaklı olarak kullanım alanının artması şifrelemeye verilen önemin artmasından en büyük paya sahip olan etkendir. İtalyan bir fizikçi olan Markoni tarafından icat edilen telsiz ile yeni sorunlar ortaya çıkmaya başlamıştır. Savaş alanından haberleşmeyi kolaylaştıran bu alet bilgi güvenliği olmadığı takdirde büyük sorunların ortaya çıkacağının bir ispatı olmuştur. Buradaki asıl sorun bilginin hedef alıcısının yanında düşmana da kolaylıkla ulaşabilecek haldedir. Bu sebeple telsizle iletişim mesajın güvenli bir şekilde şifrelenmesini gerektirmiştir (Çeşmeci, 2009; Çimen ve ark., 2008).

Birinci Dünya Savaşı sürerken telsiz güvenliğinin önemi iyice anlaşılmıştır. Güvenliğin sağlanabilmesi için çok sayıda şifreleme yöntemi geliştirilmiştir. Dönemin en ünlü yöntemlerinden biri de Almanlar tarafından geliştirilen ADFGVX şifresidir.1918 tarihli büyük Alman saldırısından hemen önce tasarlanmış olan bu yöntem, yer değiştirme ve ters çevirme işlemlerinin karışımından oluşmaktadır. Bu şifreleme yöntemi Fransızlar tarafından kırılmış ve Almanlar savaşı kaybetmiştir (Çeşmeci, 2009; Çimen ve ark., 2008).

	A	D	F	G	V	X
A	d	h	x	m	u	4
D	p	3	j	6	a	o
F	i	b	z	v	9	w
G	1	n	7	0	q	k
V	f	s	l	y	c	8
X	t	r	5	e	2	g

Şekil 2.8. ADFGVX Şifreleme

Birinci dünya savaşında Amerika'nın savaşa dâhil olmasında etkili olan olayın arkasında İngiltere'nin 1917'de Almanya Dışişleri Bakanı Arthur Zimmermann'ın Meksika Başkanı'na çekmiş olduğu telgrafı deşifre etmesi yatmaktadır (Canbek ve Sağıroğlu, 2006; Çeşmeci, 2009; Çimen ve ark., 2008; Kara, 2009).

2.2. Modern Şifreleme Teknikleri

Modern kriptografi, kriptografinin sanat dalından bilim dalına geçişi olarak tanımlanır. Bilgisayar ile iletişim güvenliğinde temel esası olarak görülen modern şifreleme algoritmalarından kısa fakat kompleks yapı barındırırlar. Modern şifreleme yöntemleri içerisinde kullanılmakta olan bütün algoritmalar, şifreleme ve şifre çözme işlemlerinde kontrol amaçlı olarak bir anahtar kullanırlar. Mesaj yalnızca kullanılan anahtarın uyuşması halinde çözülür.

Modern şifreleme tekniklerinde iki temel işleyiş bulunmaktadır. Bu işleyişlerden ilki simetrik anahtarlı sistemler (gizli anahtarlı şifreleme), ikincisi asimetrik anahtarlı sistemler (açık anahtarlı sistemler) olarak ikiye ayrılır.

2.2.1. Simetrik şifreleme

Bu algoritma içerisinde şifreleme ve şifre çözme yöntemlerinde bir adet gizli anahtar kullanılır. Kullanılan anahtar şifreleme işlemi gerçekleştiren taraf ile şifrelemeyi çözecek taraf arasında oluşturulmuş ortak anahtardır. Gönderilmekte olan gizli metin, beraberinde oluşturulan gizli anahtar ile alıcıya gönderilir. Alıcı gizli anahtarı kullanarak metni çözümler.

Bu şifreleme tekniğinin en önemli avantajından biri oldukça hızlı olmasıdır. Bunun ile beraber simetrik algoritmanın içermiş olduğu basit işlemlerin elektronik cihazlar içerisinde uygulanması çok daha zahmetsizdir.

Algoritmaların hızlı ve donanımlarla birlikte kullanılabilir oluşu avantaj olarak görülebilirken güvenli olarak anahtarın dağıtılma zorluğu, hacim problemi ve kimlik doğrulama ilkeleri kullanılarak hizmetlerde güvenilir bir ortam oluşmasındaki zorluklar bu yöntem için dezavantaj olarak görülmektedir.

2.2.1.1. Blok şifreleme

DES (Data Encrytion Standard - Veri Şifreleme Standartı) şifrelemede blok kullanan algoritmalardan biridir. Şifrelemede metin uzunluk değerleri belirli olan bloklarda meydana gelir. DES algoritmasının 64 bit uzunluk değerinde bir anahtara sahip olmasına karşın 56 bitlik uzunlukta simetrik şifreleme tekniğini uygulayan bir yöntemdir. Bununla birlikte her uygulamada kullandığı duruma özgü yeni bir anahtar üretmesi DES algoritmasının güçlü bir yapıya sahip olduğunu gösterir. Günümüzün teknolojisinde algoritması yavaş olması ve 56 bit anahtar uzunluğundaki yetersizliği DES algoritmasının zayıf yönünü belirtir. Teknolojisinin ilerlemesi sonucunda 2000'li yılların başında DES algoritmasının kırılması ile yetersiz kaldığı görülmüş ayrıca itibarını kaybetmesine sebep olmuştur. DES algoritmasındaki bu soruna sebep olan kaynaklar 'TripleDES' veya 'DES-3' adıyla tanınan yeni bir algoritmayla düzeltme işlemi gerçekleşmiştir. Günümüzde kullanılan SSH benzeri birçok uygulama DES-3 algoritmasından faydalanmaktadır. DES şifrelemesinin 3 defa arka arkaya işlenmesi ile oluşan DES-3 algoritması, DES algoritmasının 3 kat kadar daha yavaş

çalışmaktadır. Buna ek olarak DES-3 algoritması ile şifreleme gerçekleştirmek için 24 bayt uzunluğunda anahtar kullanılmaktadır. Her bayt değeri için 1 eşlik biti barındırır. Bundan dolayı anahtar uzunluk değeri 168 bit olarak hesaplanır. AES algoritmasının geliştirilmesi ile popülaritesini kaybetmiştir. Nedeni ise AES şifreleme yönteminin çok gelişmiş olmasından dolayı 6 kat daha hızlı çalışmasıdır.

AES (Advanced Encrytion Standard - Gelişmiş Şifreleme Standartı) DES algoritmasına binaen güvenli sistemlerden biridir. Bazı bilim adamlarının DES algoritmasının çözmesi ile birlikte 2001 yıllarında Vincent Rijmen ve Joan Daemen tarafından geliştirilmiştir. DES algoritmasının zayıf yönlerini matematiksel yöntemler kullanarak tümü ile düzeltilen blok şifreleme algoritmalarından biridir. AES algoritması 128, 192 ve 256 bit olarak aynı olmayan üç anahtar uzunluk değerine ait olabilme durumuna sahiptir. AES algoritmasının DES algoritmasından farklı olması hem donanımsal olarak hem de yazılımsal olarak hızlı olması ayrıca daha kolay uygulanabilir olması buna ek olarak hafızaya gereğinden az ihtiyaç duyması bu algoritmanın güçlü yanlarından biridir. Simetrik şifreleme algoritmasında en yaygın olarak kullanılan bu algoritma, pratik ve doğrudan (bruteforce) saldırılara karşı dayanıklılığı önemli derecede yüksek olduğu düşünülmektedir.

Blowfish, DES algoritmasının eksikliğinin anlaşıldığı zamanlarda onun yerini alması amacı ile tasarlanmış olan bu algoritma 64-bit öbek büyüklüğünde ve 32 bit ile 448 bit arasında anahtar uzunluğuna sahiptir. Bu algoritma en az 4 kilobayt ram boyutuna ihtiyaç duyar. Bundan dolayı akıllı kart olarak adlandırılan hafif sistemlerde kullanımı görülmemektedir. Algoritmanın üstün şifreleme işlemi gerektiren ve e-mail benzeri genel olarak kullanılan uygulamalarda başarılılığı yüksek olarak değerlendirilen bir yöntem olması kullanımını artıran özelliklerinden birisi haline getirmiş olup ve tamamıyla ücretsiz olması bu algoritmasının piyasadaki kullanımını arttırmıştır. İçerdiği kompleks anahtar tablosu ile bu algoritmayla oluşturulan şifrenin kırılmasını zorlaştırmıştır.

2.2.1.2. Akış şifreleme

Matematiğin sistematik olarak kriptografide kullanılması 1917 yılında Amerika'da başlamıştır. Vernam şifresi olarak bilinen ve Vigenére şifreleme sistemini temel alan yeni bir şifreleme tekniği geliştirilmiştir (Çeşmeci, 2009; Çimen ve ark., 2008).

Bu yöntemde düz metin içerisindeki karakter düz metin ile aynı uzunluk değerine sahip, belirtilen gizli anahtar ile karaktere modüler olarak eklenip şifrelenmesidir. Cidden anahtar rastgele olarak üretilmiş ve belirtilen metinden çok büyük ise, kısmen veya tamamen tekrar edilmiyorsa ayrıca gizli tutuluyorsa şifreli metindeki anahtarı bilebile kırılması imkânsızdır. Ancak bu yöntemle şifrelenen metnin kırılmasının imkânsıza yakın olmasına rağmen bu yöntemin pratik olmayışı nedeniyle tek kullanımı yaygın olarak engellemiştir.

Vernam şifreleme yönteminde her şifrelemeden sonra anahtarın değiştirilmesinin sistemi çok daha güvenli hale getireceği düşüncesi tek seferlik şifre(one time pad) yöntemini ortaya çıkarmıştır. Tek seferlik şifre yöntemi günümüzde de kullanılmaktadır (Çeşmeci, 2009; Çimen ve ark., 2008).

Tek seferlik şifre tekniğinin en büyük dezavantajı anahtarın mesaj alıcısına güvenli şekilde iletilmesi zorunluluğudur. Mesaj uzunluğunda bir anahtarın güvenli bir kanaldan iletilmesi gereklidir. Her mesaj iletiminde bu anahtarın değişeceği düşünülürse bu sistemin pahalı ve pratik olmayan bir sistem olduğu görülür. Buna rağmen Amerika ile Rusya devlet başkanları arasındaki kırmızı hatta tek seferlik şifreyle iletişim yapıldığı bilinmektedir (Canbek ve Sağıroğlu, 2006; Çeşmeci, 2009; Çimen ve ark., 2008).

2.2.2. Asimetrik şifreleme

Anahtar dağıtımı, simetrik şifreleme algoritmalarındaki en büyük problemlerden biridir. Çok kullanıcılı bir sistemde simetrik algoritma yöntemini kullanarak oluşturulan anahtarın bütün kullanıcılara benzer anahtarın dağıtılması

güvenlik açısından büyük bir problem olarak görülmektedir. Kullanıcıların her birine değişik bir anahtar tahsis edilmesi durumunda sistem içerisinde çok fazla değişik anahtar olacağından dolayı sorun oluşturabilmektedir. Böyle sorunlara çözüm üretmek için yeni bir yöntem olarak asimetrik şifreleme algoritmaları geliştirilmiştir. Bu şifreleme algoritmalarında anahtarla şifre çözmek için kullanılan anahtar birbirinden farklıdır. Şifrelemede kullanılan anahtar açık anahtar, şifreyi çözmek için kullanılan anahtar ise özel anahtar olarak tanımlanmaktadır. Açık anahtar herkesçe ve hangi anahtarın kime ait olduğunun bilinmesidir. Bundan dolayı sertifikalar kullanılmaktadır. Sertifikalar açık anahtarla sahibinin kimliği arasında oluşan bağlantının belgesidir. Şifreyi çözecek kullanıcıda ise sadece özel anahtar bulunur, gizlilik sadece özel anahtar içindir. Bu yüzden simetrik şifrelemeye göre asimetrik şifreleme güvenlik açısından başarılılığını kanıtlamıştır. Anahtar fazlalığı durumunu çok kullanıcılı uygulamalarda simetrik şifrelemeye göre ortaya çıkabilecek problemleri engeller. Bunun aksine hız ve donanımsal uygunluk olarak simetrik şifreleme asimetrik şifrelemenin önüne geçmiştir. Asimetrik algoritmaların güvenliliği için çok büyük değerlere sahip asal sayılar kullanılmaktadır. Zaman açısından bu durum çok büyük problemler oluşturmaktadır. Sistemsel olarak kullanılan asimetrik algoritmalar simetrik algoritmalarda kullanılan sistemlere binaen çok daha ağırdır. Dahası asimetrik şifreleme algoritmasında büyük değerlere ait sayılar kullanılarak donanım yapılarında uyumsallık sağlanmasının zorluğu görülmektedir (Yerlikaya ve ark., 2005; Kodaz ve Botsalı, 2010).

Bu yöntem ile şifrelemenin ana ilkelerinden biri olan bütün olma durumu, kimlik doğrulama ile mahremiyet gibi hizmetlerin güvenli olarak sağlanabildiği ve anahtarın kullanıcı tarafından belirlenebilir olması avantaj olarak görülebilirken anahtar uzunluğundan kaynaklı olarak algoritmanın yavaş çalışması dezavantaj olarak karşımıza çıkmaktadır. Günümüzde zamanın da değeri açıkken bir sistemin yavaş çalışması hoş karşılanmamaktadır.

1976 yılında sayılar teorisinin kullanılmayan çoğu özelliği kullanılarak Diffie-Hellman anahtar değişim algoritması ortaya çıkarılmıştır. Bu algoritma ile mesajın alıcısı ve göndericisinin ortak bir anahtarda anlaşmak için bir araya gelmesi

gerekliliğini ortadan kaldırmıştır. Böylece kriptolojide Gizli Anahtar Kriptografi ‘nin sonlarına gelinmiş ve literatüre yeni bir kavram olarak Açık Anahtarlı Kriptografi girmiştir (Canbek ve Sağıroğlu, 2006; Sağıroğlu ve Alkan, 2005; Çeşmeci, 2009; Çimen ve ark., 2008).

Diffie–Hellman iki katılımcının bilgi alışverişi yapmadan önce herhangi bir güvenliliği olmayan kanal vasıtası ile (güvenli olarak) ortak oluşturulan bir şifrede karar kılınmasına imkân sağlayan protokollerden biridir. Algoritmadaki anahtar değişiminin temel amacı, her iki tarafın oluşturmuş olduğu anahtarın güvenli olarak birbirlerine iletip ve daha sonra ise belirtilen anahtar yardımıyla oluşturulan şifrelenmiş mesajların birbirlerine gönderebilmelerine imkân sağlamasıdır. Diffie–Hellman algoritmasında, problemlerden biri olarak gözüken gizli anahtarın korunması ve dağıtılması aşılmıştır.

RSA (Rivest-Shamir-Adleman) Açık Anahtar Kriptolojisi ile şifrelemede yeni bir çağ başlamıştır. Artık mesajın alıcısı ve göndericisi birbirini tanımak ve anlaşmak zorunda kalmadan kendi arasında gizli haberleşme yapabilir hale gelmiştir. Bu düşünceden etkilenerek Ronald Rivest, Adi Shamir ve Leonard Adleman, 1977'de RSA(Rivest-Shamir-Adleman) adını verdikleri yeni bir açık anahtar şifreleme sistemini bulmuştur. Bu yöntem temel olarak çarpanlara ayırma problemine dayanmaktadır (Canbek ve Sağıroğlu, 2006; Sağıroğlu ve Alkan, 2005; Çeşmeci, 2009; Çimen ve ark., 2008; Akleylek ve ark., 2011).

RSA’da güvenilirlik, büyük tamsayılar ile işlemler yapılması esnasında karşılaşılan zorluklara dayanan şifreleme tekniklerinden biridir. Anahtar oluşturmada kullanılan asıl işlem, asal sayılar kullanılarak güvenli bir yapı için zemin hazırlanması olmuştur. RSA ticari olan uygulamalar içerisinde kullanılarak tam sayılarda iyileştirme teknolojisi kullanarak üretilen anahtarlardan biridir. RSA algoritmasında sistemin güvenilirliği ile birlikte hız değerinin de yüksek olmasında anahtardaki sayısal büyüklük önem arz etmektedir. RSA’yla 1024 bit boyutunda ki anahtar basit uygulamalarda yeterli şifreleme tekniklerinden birini kullanabilmektedir. Ayrıca RSA algoritmasının diğer algoritmalara göre daha basit bir algoritma olduğu görülmektedir.

RSA algoritması kullanılarak asimetrik şifreleme tekniğinin yaygın kullanımının arttığı gözlemlenmektedir.

2.3. Kuantum Şifreleme

İncetaş ve Sağıroğlu (2015), cihazlardaki ya da ortam içersinden kaynaklanabilecek gürültülerin gözlemlenmediği ortamların birinde BB84 Kuantum Anahtar Dağıtım Protokolünü kullanarak, göndericiyle alıcı arasındaki ortak anahtar oluşturmasını sağlayan bir simülasyon tasarlanıp bu simülasyon yardımı ile ortamda bir dinleyicinin olup olmaması durumunda oluşturulan anahtar uzunluklarıyla araya giren dinleyicinin, oluşturulmuş anahtarlar üzerindeki etkisi araştırılmıştır. Belirtilen amaç ile (100, 150, 200, 250,…,850, 900, 950, 1000) sayılarında rastgele foton dizileri oluşturulmuş bununla birlikte dinleyicinin olup olmaması durumlarında her biri için ayrı olarak 1000'er defa gönderilmiştir. Yapılan işlem sonrasında oluşan anahtar üzerindeki iletilen foton sayılarını hesaba katıp dinleyici tarafından kaynaklanmakta olan hatalar için yaklaşık oran değerleri tespit edilmiştir. Böylelikle gerçek bir ortam içerisinde çalışırken oluşa bilecek hatalarda, kuantum kanalında bir dinleyici olduğuna dayandırılarak oluşacak durumlar için yorum yapılabilmesini hedeflemişler.

Hosseini-Khayat ve Marvian (2005), BB84 protokolünün, iki dezavantajı vardır: (1) Güvenlik, Gönderici'nin qubit kaynağının, aynı qubit'in birden fazla kopyasını yanlışlıkla göndermemesi anlamında mükemmel olduğu varsayımına dayanır. Bu varsayım ihlal edilirse, çoklu-qubit emisyon saldırısı başlatılabilir. (2) BB84 önceden belirlenmiş anahtarları aktaramaz olması; dağıtabildiği anahtarlar süreçte oluşturulur. Hosseini-Khayat ve Marvian tarafından oluşturulan protokol bu dezavantajlara sahip değil. Bu protokol, BB84'ten farklı olarak, çoklu-qubit emisyon saldırısına karşı savunmasız değildir. Protokolün bir dezavantajı, gidiş geliş gereksinimidir. Bu, çoklu qubit emisyon saldırısına karşı korunmak için bir bedeldir.

Toyran (2006), Kuantum şifreleme optik iletişim tekniklerinden biridir. Dolayısıyla, sunulmakta olan bu yöntemin uygulanmasında optik bir iletişim gerçekleştiren altyapıya ihtiyaç duyulmaktadır. Ayrıca, kuantum şifreleme taraflar arasındaki iki uç arasında bir optik bağlantı sağlamakta ve fotonlar ile çalışmayı

gerektirmektedir. Böylece çok uzak mesafeler de kuantum şifreleme kullanımını zorlaştırır. İki uç arasındaki optik hat üzerindeki fotonların polarizasyonunu etkileyebilme durumlarından olan bükülme, ezilme, tekrarlayıcı, bağlantı noktaları vb. gibi durumların olmaması gerekir. Öyle ki foton gibi kuantum sistemlerde hatalarla oluşan durumlara karşı çok daha duyarlı olup, oluşan en küçük etkiden bile çok fazla rahatsız olur. Buna benzer sistemlerle çalışmanın diğer bir zorluğu ise maliyetlerinin çok yüksek olmasıdır. Toyran bu bildirisinde kuantum şifreleme kullanımına dayanarak güvenli optik iletişim yöntemi ile analizlerine değinmiştir.

Gümüş (2011), çalışmasında kuantum şifreleme'nin matematiksel şifreleme tekniği kullanılarak oluşturulan yöntemlerin avantajına değinmiş ve mevcut anahtar dağıtım protokollerini incelemiştir. Zaman içerisinde gerçekleşen bu protokollerdeki değişim sürekli olarak donanım üzerinde gerçekleşen gelişmelere ve eksikliklerden kaynaklanarak oluşan muhtemel saldırın kaynağı olduğuna değinmiştir.

Şahin ve Selçuk (2018), çalışmasında Türkiye'deki mahremiyet gerektiren çeşitli optik hatlar aracılığı ile kullanılma durumu mümkün görünen kuantum şifreleme sistemlerinde kendi imkânlarımızdan yararlanarak yeniden dizayn edilip üretilme işlemine başlanması şartını sunmuştur. Bu durum içerisinde kaçınılmaz olan, fiber altyapısındaki değişime ayak uydurabilecek kuantum şifreleme tekniklerine tasarlama imkânı sunulması, teorik ve simulatif ortam ile yapılmasına izin verilen analizlerden sonra deneysel ortam oluşturularak sistem örneklerinin kurulması ile testinin yapılması ve endüstriyel alanda pratik mühendislik bilgisi çerçevesi içerisinde oluşturulan ilk örnek imalatı ile birlikte görüntülenmesini başarıp hem bilgi hem de tecrübe kazandırma çıkarımlarında bulunulmuştur. Bu çalışma ile kuantum şifreleme uygulamaları gerçekleşirken şifreleme anahtarı olarak kullanılabilecek yine kuantum mekanik temeline dayanan bir rastgele sayı dizisinin üretilmesinde kullanılan teknik gösterilmiştir. Kullanılan bu teknikteki avantaj, fotonlardaki polarizasyonda kuantum hal belirsizlik işleminin uygulanmasıdır. Genel dalga boyu 1550nm olan optik hat kullanılmıştır. Rastgele üretilen sayı dizisinde hız sınırlama etkeni olarak fotodetektör karanlık akımı ile darbe sonrasındaki etkilerle kullanıma sunulan lazerin oluşturmuş olduğu çıktı güç değerinin değişmezliliğidir. Yapılan bu teknik ile yaklaşık saniyede

10 kbit hızda rastgele sayıda dizi üretim işlemi başarılı halde gerçekleşmiştir. Rastgele sayı dizisi üretimindeki hızın arttırılma işlemi fotodetektörler içersindeki krayojenik yöntemler kullanılarak soğutma işlemine tabi tutulması mümkün olacağına değinmiştir.

Toyran (2003), Bu tezde kuantum kriptografinin detaylı bir incelemesini vermeyi amaçlanmıştır. Ancak, metinde kuantum mekaniği yasalarının kullanıldığı diğer kuantum uygulamalar hakkında da bilgiler bulmak mümkündür.

Zhao ve ark. (2007), Bu makalede, Winnow protokolü olarak adlandırılan hata mutabakat prosedürünün düzeltme yeteneği analiz edilmekte ve tahmin edilmekte, ayrıca, bu konuda bazı ifadeler vermektedir. CASCADE ve BINARY her zaman tek bir hatayı kaldırır ve hiçbir zaman birden fazla hata bloğuna ek hatalar çıkarır, çünkü bir blokta üç veya beş hata olduğunda Winnow protokolü ek hata verir, çünkü Hamming algoritması her blokta sadece tek bir hata ortaya çıkarır. CASCADE ve BINARY, daha fazla iki yönlü iletişim gerektirir ve gönderilen her bi paket, kimlik doğrulaması için log2 n gerektirebilir. Ve iletişim zamanları ham anahtarın uzunluğuyla orantılıdır. Winnow protokolü, yukarıdaki yöntemlerden daha uzun olan ham anahtar bitlerinin tüm hatalarını ortadan kaldırmak için yalnızca daha az iletişim gerektirirken, daha önemlisi, iletişimin ham anahtarın uzunluğu ile hiçbir ilgisi olmadığı zaman, sadece hata oranına bağlıdır.

Toyran ve ark. (2012), Bu çalışmasında ikisinde de parite kontrol tabanlı olan CASCADE hata tespit ve düzeltme protokolüyle LDPC hata tespit ve düzeltme kodları tanıtılmakta olup ve bunların performans karşılaştırılma işlemleri için gerçekleştirilen bilgisayar simülasyonlarının oluşturmuş olduğu (fazlalık bilgi, başarım) sonuçlara yer vermektedir. LDPC için mesaja ek olarak gönderilen fazlalık bilgisinin miktarındaki hata olasılığından bağımsız, belirli ve sabittir. CASCADE durumunda ise fazlalık bilgisinin miktarı p'ye bağımlı, değişken ve belirsizdir. Hata olasılığındaki artış doğru orantılı olarak etkilemektedir. Bu durumda, LDPC kodu hataların tümünü düzeltememekte CASCADE ise hataların tümünü düzeltmektedir.

Sasaki ve ark. (2011), Bir metropol alanında kuantum anahtar dağılımı ile yeni bir güvenli iletişim ağı rapor etmiştir. Farklı QKD şemaları, güvenli bir televizyon konferansını 45km mesafede, uzun süreli istikrarlı çalışmayı ve cep telefonlarını güvenli bir şekilde kullanabilmeniz için entegre etilmiş, Tokyo QKD Ağı'nı kullanarak bir QKD saha denemesinin sonuçlarını sunmuştur. Bu çalışmada, yeni GHz-saatli QKD sistemleri, bir QKD akıllı telefon, güvenilir bir ticari QKD ürünü ve bir dolaşıklık QKD sistemi kullanmış, ortak bir API kullanarak birkaç temel yönetim aracıları ile birbirine bağlamış ve tek bir anahtar yönetim sunucusu tarafından yönetmiştir.

Mateo ve ark. (2013), Bu çalışmasında, yüksek hızlı bir QKD cihazının tasarımında ortaya çıkan soruları açıklığa kavuşturmak amacıyla, olağan verimlilik odaklı çalışmalarla farklılıkları karşılaştırarak, modern postprocessing protokollerinin gerçek iş süreçlerinin ölçülmesi için bir çalışma sunmaktadır. Mevcut teorik çalışmalar ile farklı uygulamalar için optimize edilmiş pratik uygulama uygulamaları arasındaki farklılıkları vurgulamak amacıyla, anahtar mutabakat süreci için bir dizi yüksek performans, kısa blok uzunluğu, düşük yoğunluklu parite kontrolü (LDPC) kodları kullanılmaktadır. Bu kod ailesi, performansı ve düşük kaynak gereksinimleri nedeniyle kablosuz ağlarda yaygın olarak kullanılmaktadır. QKD'ye uygulanması, yüksek performanslı QKD sistemlerinin klasik postprocessing parçasının tasarımında dikkate alınması gereken tradeofflar ve parametreler olan oldukça iyi bir şekilde göstermektedir. Çalışma sırasında bilinen Cascade protokolü, geleneksel mutabakat yöntemlerinin temsilcisi olarak karşılaştırma amacıyla kullanılmıştır.

Gigov (2013), Tez çalışmasında, Mevcut karasal kuantum bağlantıları yaklaşık 250 km ile sınırlıdır. Ancak, QKD yakında, güvenilir bir düğüm olarak kullanılan bir yörüngedeki uyduya serbest alan bağlantıları üzerinden global ölçekte konuşlandırılabileceğini savunmuştur. Düşük bir Dünya yörüngesindeki uyduya yerleştirilmiş bir kuantum alıcısına fotojenik bir bağlantı kurulması, Kanada Kuantum Şifreleme ve Bilim Uydusu (QEYSSat), Kanada üniversiteleri, Kanada Uzay Ajansı (CSA) ve endüstri ortaklarını içeren ortak bir projedir. Bu tez, QEYSSat misyonunun fizibilite çalışmalarına yönelik yürütülen bazı araştırmaları sunmaktadır. Bu

araştırmanın temel amaçlarından biri veri edinimi için teknolojiler geliştirmek ve uydu tabanlı bir QKD sistemi için gerekli işlem olan; çalışan bir test yatağı sistemi, genel karmaşıklığın, gerekli bilgi işlem kaynaklarının ve klasik iletişim kanalının bant genişliği gereksinimlerinin kesin olarak temelli tahminlerini oluşturmaya yardımcı olmaktır. Ayrıca QEYSSat'ın gelecekteki bir yük bilgisayarının tasarımı ve geliştirilmesi için iyi bir temel olarak hizmet edilebilir olduğunu savunmuştur. Bu tez, her bir uçta simetrik bilgi işlem kaynaklarını kullanan çoğu geleneksel uygulamadan farklı olarak, bağlantının bir tarafında hesaplama gereksinimlerini en aza indirmeyi amaçlayan bir QKD işlem sonrası sisteminin tasarımını ve uygulanmasını tarif etmektedir. İşlem sonrası yazılım, hassas tesadüfi analiz, düşük yoğunluklu parite kontrol kodlarına dayalı hata düzeltme ve otomatik polarizasyon hizalaması için bir prosedür sunar.

Calver (2011), Bu araştırma, farklı hata oranları, örnekleme oranları, hata dağılımları ve daha büyük elenmiş anahtar boyutları altında etkinliğini ölçmek için Cascade gizli anahtar uzlaşma protokolünün ampirik bir analizini sunmaktadır. Araştırmanın temel bulguları:

- %25'lik bir hata örnekleme oranı, değişken blok boyutlarını kullanırken optimum Cascade performansı sağlar.
- Elenmiş anahtar uzunluğu seçimi Cascade hata tahmininin doğruluğunu doğrudan etkiler
- Cascade algoritması, ilk permütasyonla birlikte patlama hatası ortamlarında iyi performans gösterir
- Tamponun boyutu ile sızan bilgi miktarı arasında bir uyuşmazlık vardır.

Johnson (2012), Bu araştırmasında, bu LDPC kodlarının QKD ortamında etkinliğini değerlendirirken, çalışma zamanı, çıktı ve iletişim karmaşıklığı gibi gerçek dünya parametrelerini iyi bilinen Cascade ve Winnow algoritmaları ile deneysel olarak karşılaştırmayı amaçlamıştır. Ayrıca, her üç protokolde hatalı hata tahmininin, tekdüze olmayan hata dağılımının ve değişen anahtar uzunluğunun etkileri, aynı giriş anahtar dizileri için değerlendirmiştir. Her üç protokolün performansını karakterize etmek ve

her birinin güçlü ve zayıf yanlarını belirlemek için sonuçlar üzerinde analizler yapmıştır.

Günümüzde kuantum anahtar dağıtımı alanında farklı çalışmalar yapıldığı gözlemlenmiştir.

- Cambridge Üniversitesi ile Toshiba tarafından BB84 protokolü kullanılarak gerçekleştirilmiş olan bir deneyde 20 km uzunluğundan fazla bir fiber optik kablo ile gerçekleştirilen yüksek bit hızıyla saniyede 1 megabit kullanılarak güvenli anahtar değişim işlemi gerçekleştirilmiştir. Yapılan bu deneye ilaveten 100 km'lik bir mesafede yine fiber optik kablo ile gerçekleştirilen bir diğer deneyde ise yüksek bit hızıyla saniyede 10 kilobit hıza ulaşmıştır.

- 2006 yılın içerisinde E91 protokolünü kullanarak iki Kanarya adası arasında 144 km'lik bir mesafede kablosuz olarak kuantum anahtar dağıtım işlemi gerçekleştirme deneyi yapılmıştır.

- Mart 2007 yılında BB84 protokolünü kullanarak NITS firması tarafından 148,7 km'lik bir menzilde fiber optik hat üzerinde anahtar dağıtım işlemi gerçekleştirme deneyi yapılmıştır.

- Ağustos 2015 yılında 307 km'lik bir mesafede fiber optik hat üzerinde kuantum anahtar dağıtımı deneyi gerçekleştirme işlemi yapılmıştır. Bil hayli yüksek uzunlukta olan bu mesafede gerçekleştirilen deneyde hız olarak saniyede 12.7 kilobit değerine ulaşmayı başarmışlardır.

Kuantum anahtar dağıtımının ticari alanda da kullanımı görülmektedir.

- 2004 yılı içerisinde Avusturya'nın başkenti Viyana şehrinde kuantum anahtar dağıtımı kullanarak dünyada ilk defa banka havale işlemi gerçekleştirilmiştir.

- Ekim 2007 yılında İsviçre'de yapılan seçimin sonuçları kuantum şifreleme teknolojisinden yararlanılıp iletim işlemi başarılı bir şekilde gerçekleşmiştir.

3. MATERYAL ve YÖNTEM

3.1. Kuantum Kriptolojisi

Temeli fizik kanunu olan Heisenberg belirsizlik ilkesinden gelen ve güvenli iletişim için kuantum mekaniği kullanan bir kriptoloji yöntemidir.

Heisenberg belirsizlik ilkesine göre, kuantum fiziğinde bir nesne olan fotonun iki özelliği olan konum ve momentum bilgilerinin aynı anda ölçülmesi imkânsızdır. Bu özelliklerin birinde sırası ile yapılacak olan ilk ölçüm sonrasında yapılacak ikinci ölçüm değerinin çıktısını kararsız hale getirmektedir. Heisenberg belirsizlik ilkesi, optik hat üzerindeki iletimi gerçekleşen ve ışık parçacığının en küçüğü olarak kabul edilen fotonun, kubit olarak taşımakta olduğu veri değerinin polarizasyonuna bağlılığı ile ardı sıra yapılacak okuma gibi ölçümlerle bozulacağını öne sürmektedir (Gümüş, 2011).

3.2. Kuantum Kriptolojisinin Amacı

Gizli dinleyicilerin şifrelenmiş iletilerin okunması ve içeriğinin çözülmesini önlemek için geleneksel şifreleme tekniklerinde kullanılan değişik [matematiksel|matematik] yöntemlerin tersi yönünde, kuantum şifreleme, oluşturulan bilgi ya da veri fiziğini kendine esas almaktadır. Gizli dinleme olarak kabul edilen, fiziki olarak bir nesneyi ölçme olarak da tabir edilebilir. Bu durum içerisinde verinin taşıyıcılarından biri kuantum süper pozisyonu ya da kuantum dolaşıklılığına benzer kuantum fenomenlerinden birini kullanıp her daim gizli dinleyicilerin tümünü sezme yeteneğine sahip bir iletişim sistemi gerçekleştirebilir. Bundan ötürü bilgi ya da veri, kuantum taşıyıcısının üzerinde yapılan ölçümlerde değişiklik meydana getirir dolayısıyla bu tarz girişimler her daim iz bırakır (Anonim, 2015c).

3.3. Kuantum Anahtar Dağıtım Yöntemi

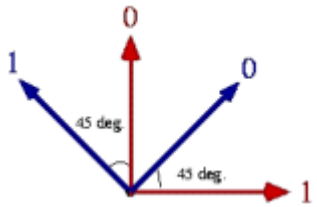
Kuantum şifrelemede bilinen en iyi ve pratik uygulamaların ilki olan *kuantum anahtar dağıtımı (KAD)* dır.

Anahtar, taraflar arasında KAD yöntemi kullanılarak dağıtılır. Dolayısıyla, kuantum kriptolojisinde anahtar dağıtım problemi KAD yöntemi ile çözülmektedir. Güvenliği kanıtlanmış olan KAD, anahtar dağıtım yöntemleri arasında tamamen güvenli tek yöntemdir.

Şifreleme işlemi Vernam şifreleme tekniği kullanılarak yapılmaktadır. Vernam şifresi kırılmazlığı kanıtlanmış tek şifredir. Böylelikle, kuantum kriptolojisinde gerçek anlamda güvenli bir iletişim ortam garantililiği sağlanmış olur (Toyran, 2011).

3.3.1. BB84 protokolü

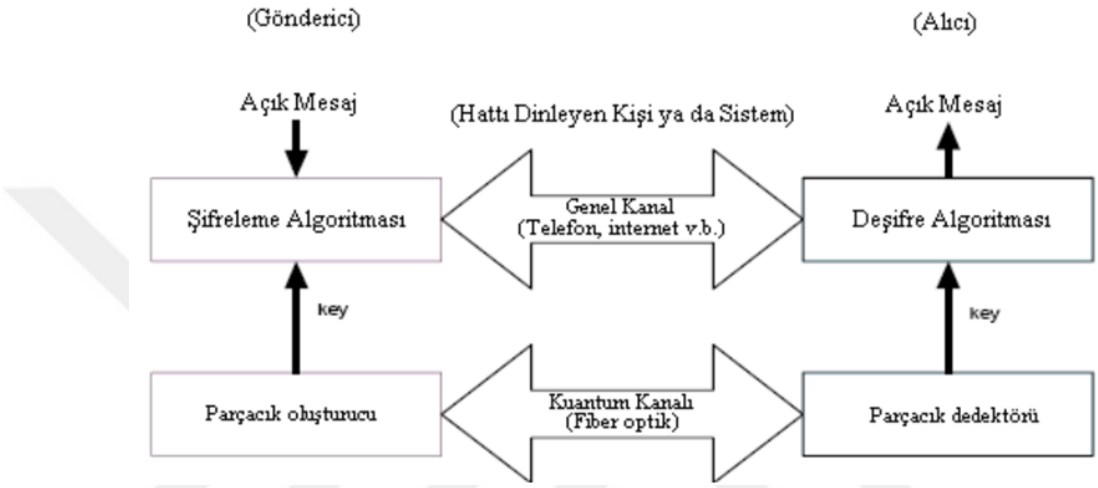
İlk kuantum anahtar dağıtım protokollerinden biri olan BB84, 1984 yılında Charles Bennett ile Gilles Brassard tarafından geliştirilen bir yöntemdir. Belirtilen protokol ile anahtar iletiminde kullanılan dört değişik türde polarizasyon açısına ait foton tipleri görülmektedir. Şekil 3.1.'de de görüldüğü üzere bu dört farklı polarizasyon 0 ve 1 olmak üzere aynı olmayan iki kubit değerini simgelemektedir (Gümüş, 2011).



Şekil 3.1. BB84 Protokolünde Polarizasyon Kubit Değeri Eşleşmesi

45º ve 90º polarizasyon değerlerine ait fotonlar için kubit bilgisindeki 0 anlamlı değeri ile işlem yaptığı, 0º ve 135º polarizasyon değerlerine ait fotonların ise kubit bilgisindeki 1 anlamlı değer ile işlem yaptığı Şekil 3.1.'de gösterilmektedir. Bu durumdaki seçimler isteğe bağlı olarak düzenlenebilme imkânları bulunmaktadır. Gönderim ve okuma işlemlerinde hem gönderici tarafın hem de alıcı tarafın benzer şekilde polarizasyon türlerinin belirlenmesi gerekmektedir.

Sistem tarafından kullanılan fotonlar –, /, |, \ türünde birbirinden farklı 4 polarizasyon kullanılarak sırası ile 0º, 45º, 90º ve 135º polarizasyon değerlerine ait olup ve okuma işlemi için bu foton polarizasyonu için belirtilen + (düz) veya × (köşegen) türünde ki filtrelerden geçirilip okuma işlemi gerçekleşmektedir. Oluşturulan düz ve köşegen filtreler de 0 ile 1 değerlerine sahip kubit değerlerini okuyabilecek yapı bulunmaktadır.

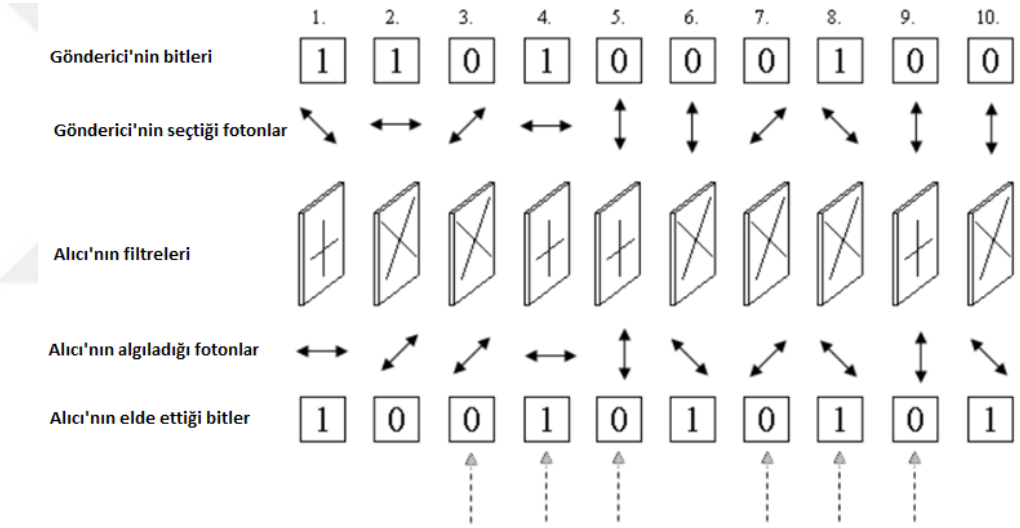


Şekil 3.2. Kuantum Anahtar Dağıtımı Modeli

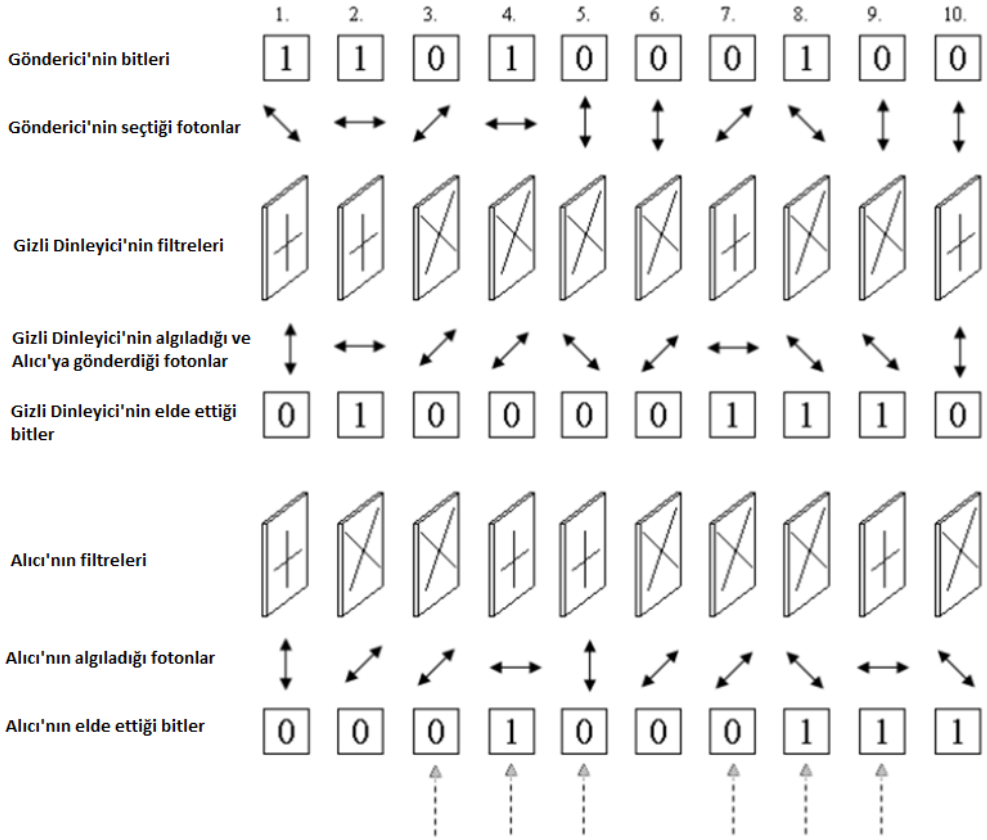
Şekil 3.2.'de görüleceği üzere kuantum anahtar dağıtımında iki ayrı kanal kullanılmaktadır. Bu kanalların ilki anahtarın belirlenmesinde gönderilecek parçacıkların kullanıldığı optik kanal olarak tabir edilen kuantum kanalı, ikinci kanal ise telefon ya da internet olarak tabir edilen genel kanalı temsil eder şifrelenmiş mesajların ve oluşturulan diğer bilgilerin doğruluğunun testi bu kanal üzerinden gerçekleşmektedir. (İncetaş ve Sağıroğlu, 2015).

Gönderici, karşı taraftaki Alıcı ile bir mesajlaşma gerçekleştireceği zaman, hattı dinleyen kişi olarak Gizli Dinleyici bu iletişimdeki mesajı edinmek için çok çaba göstermektedir. Bu tarz durumlarda Gönderici ile Alıcı, ilk olarak haberleşme için bir anahtar kümesi kullanıp kuantum kriptografi den yararlanarak anlaşmaktadırlar. Bundan ötürü öncelik olarak 0 ile 1 olan değerlere eş fotonların belirlenmesi ile işe başlanmalıdırlar. Örnek olarak 0 değerinde | ile /, 1 değerinde – ile \ gibi polarizasyon değerine ait fotonlar kullanırlar. Şekil 3.2.'de görülen bu iletişim süreci dinlemeye açık

genel kanal üzerinden yani güvenliğin sağlanmasının gerekmediği hatlar üzerinden gerçekleştirilir. Sonrasında ise Gönderici göndereceği anahtarı ikili bit olarak seçip bu bitler için uygun olarak görülen rastgele olarak belirlenen polarizasyon fotonlarını Alıcı'ya iletir. Gönderici bu durumdaki tüm polarizasyon değerini kaydedip ayrıca bu değeri saklar. Alıcı tarafında ki durum, fotonların alınmasında rastgele bir şekilde seçilen filtreler kullanılmaktadır. Bu süreçte Alıcı, fotonlar içi filtre işlemi uygulayarak oluşturmuş olduğu bit değerini saklar. Gönderici fotonların tamamı için gönderme işlemi yapıp sonrasında, Alıcı ile belirtilen genel hat üzerinde yeniden iletişim oluşturur. Alıcı ise almış olduğu fotonlar için kullanmış olduğu filtreleri Gönderici'ye gönderir. Gönderici bu durumda Alıcı'ya filtrelerden doğru olanın hangileri olduğunu seçip gönderir. Bu noktada anahtarın üretimi gerçekleşmiş olur.



Şekil 3.3. Anahtar Bitlere Karar Verilmesi



Şekil 3.4. Hattın Dinlenmesi ve Sonuçları

Şekil 3.3.'te gösterilen örnekte Gönderici 10'ar adet rastgele üretilen bit ile foton polarizasyonunu kuantum kanalı üzerinden göndermiş olsun. Burada 1 değerine ait olan birinci bit \ polarizasyona ait fotonla gönderilme yapılırken, 1 değerine ait olan ikinci bit – polarizasyona ait fotonla gönderme işlemi yapılmaktadır. İlk foton için Alıcı tarafından düz (+), ikinci foton da ise köşegen(X) filtreleri üretilmektedir. Gönderici'nin göndermiş olduğu bütün bitler 1101000100 şeklinde ve sırası ile \, –, /, –, ı ,ı ,\ ,/ ,ı ,ı şeklinde oluşturulan polarizasyonlara ait fotonlar kullanılmıştır. Alıcı tarafından kullanılan filtre dizisi +, X, X, +, +, X, X, X, +, X olarak belirlenmiş ve edinmiş olduğu bit dizisi 1001010101 olarak oluşturulmuştur. Gönderici ile genel hat üzerinden yapılan görüşme neticesinde belirtilen 3., 4., 5., 7., 8. ve 9. bitler için filtre eşleşmesi olup bu işlem ile anahtar 010010 olarak oluşturulmuştur.

Eğer gizli bir dinleyici belirtilen süreç içerisine dâhil olmaması durumunda, Gönderici ile Alıcı ortak gizli bir anahtar oluşturmuş olurlar. Burada asıl problem Gizli Dinleyici'nin hattı dinlemesi ve Alıcı'ya benzer fotonların belirlenmesinde rastgele

üretilen filtrelerle oluşacak durumun akıbetidir. Böyle bir koşulda Gizli Dinleyici'nin fotonları okuma ya da ölçme işlemleri gerçekleştirdikten sonra bunları Alıcı tarafına tekrar göndermesi gerekmektedir. Fotonları göndermediği durumda Alıcı hiçbir veri alamayacağından iletişim işlemi gerçekleşmez. Şekil 3.4.'de Gizli Dinleyici'nin Gönderici ile Alıcı'yı dinlerken oluşturulmuş olan çalışma durumu görülmektedir.

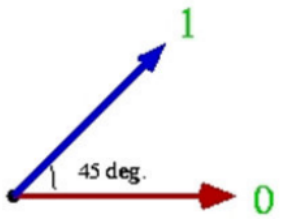
Elbette Gizli Dinleyici'nin seçmiş olduğu filtrelerin doğruluğu konusunda tahmini olarak bir fikre sahip olmayıp ve bunları doğrulama konusunda da Gönderici ile iletişime geçmesi imkansızdır. Fakat yine Eve, Gönderici ile Alıcı arasında gerçekleşen iletişimde hattı dinleyebilmektedir. Evvelki örnekte Eve, Gönderici ile Alıcı arasında gerçekleşen iletişimde aynı değerler için 3., 4., 5., 7., 8. ve 9. filtrelerinin doğruluğunu kabullenip bu yüzden doğru filtre diziliminin X + + X X + olduğunu öğrenecektir. Eve kendi oluşturmuş olduğu filtre diziliminde 2., 3., 8. ve 10. bitlerinin doğruluğunu görecektir. Bu aşamada Eve, Gönderici ile Alıcı arasında ki oluşturulan anahtarlar içerisinde yalnızca 3. ve 8. bit değeri bilgisine sahip olmaktadır.

Böyle bir durum risk olarak görünüyor olsa bile aslında hem Gönderici hem de Alıcı için rahatsız edici bir hal olarak görülmemektedir. Bu yüzden belirtilen yöntem ile Eve yalnızca anahtarı ortaya çıkarmakla kalmayıp, Gönderici ile Alıcı'ya kendini fark ettirmesine sebep olmuştur. Şekil 3.4.'de belirtildiği üzere Alıcı, doğru filtre işlemleri kullanarak 010011 anahtarını edinmiştir. Fakat Gönderici'nin 010010 şeklinde anahtar ürettiği görülmektedir.

Basit test işlemleri uygulanarak Gönderici ile Alıcı'nın oluşturmuş oldukları anahtarların farklı oldukları kolay bir şekilde belirlenip ve bu iletişim esnasında arada bir dinleyicinin olduğu ortaya çıkartılması sağlanmış olur.

3.3.2. B92(Bennet 1992) protokolü

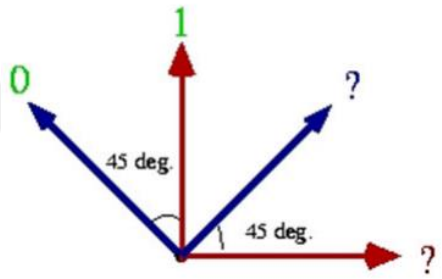
BB84 protokolünün geliştiricilerinden biri olan Charles Bennett tarafından önerilmiş olup tüm kubit değeri için Şekil 3.5.'de görülen 0º veya 45º polarizasyonunu ifade eder.



Şekil 3.5. B92 Protokolünde Polarizasyon-Kubit Değeri

Polarizasyon değeri olarak 0º olan fotonlar 0 kubit, Polarizasyon değeri 45º olan fotonlar ise 1 kubit değeri taşımaktadırlar.

Burada alıcı görevini üstlenen taraf gönderilen foton değerlerinde okuma işlemi gerçekleştirmek için BB84 protokolü ile tanımlanan düz ve köşegen filtre türleri kullanırlar. Fakat polarizasyon değerleri 0º ya da 45º olarak okunan fotonlar eleme işlemine tabi tutularak anahtara dâhil edilmez. Diğer polarizasyon değerleri 90º ya da 135º'ye sahip olan okumalar geçerli kabul edilir. Şekil 3.6.'da bu görülmektedir.



Şekil 3.6. B92 Protokolünde Okuma Basamağındaki Polarizasyon-Kubit Değeri

Böyle bir durumda polarizasyon ve filtre eşleşmelerinde ilgili sonuçlar Tablo 1'de gösterilen şekilde oluşacaktır.

Belirtildiği gibi, BB84 protokolü alıcı ile göndericinin benzer tür filtre kullanmaması sebebi ile foton için mevcut kabul etme olasılık %50 değere sahip olmasına rağmen B92 protokolü içerisinde bu olasılık %33 olarak görülmektedir. Belirtilen durum mevzu olan iki protokolün kıyaslanması ile eşit uzunluk değerindeki anahtarların üretilmesinde, B92 protokolü ile yapılmakta olan iletim işleminin BB84 protokolü ile yapılan iletim işleminden daha uzun sürmesi anlamı taşımaktadır. B92 protokol işlemi belirtilen açıdan bir dezavantaj olarak görülürken "gizli dinleyici" tarzı

saldırılarda çok yüksek dinleme tespit oranı sahip olarak güvenlik açısından avantajlı bir yönünün göstermektedir. Tablo 2'de belirtilen durum görülmektedir. Böylelikle BB84 protokolünde elde edilen geçerli kabul edilen bit değerlerinde %40 oranının dinlendiği sonucuna varılırken B92 protokol işleminde elde edilen bu oran değeri %50 olarak görülmektedir (Gümüş, 2011).

Çizelge 3.1. B92 Protokolü iletimi ile Yapılan Altı Kubitte Olası Okuma Sonuçları

Yollanan Kubit	Foton Polarizasyonu	Okuma Filtresi	Okunan Polarizasyon	Okunan Değer	Sonuç
1	/	×	/	?	Geçersiz
0	–	+	–	?	Geçersiz
1	/	+	|	1	Geçerli
1	/	+	–	?	Geçersiz
0	–	×	/	?	Geçersiz
0	–	×	\	0	Geçerli

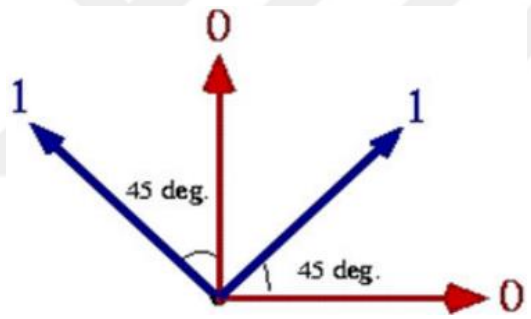
Çizelge 3.2. B92 Protokolü iletimi ile Yapılan Altı Kubitte Olası Okuma Sonuçları

Gönderen	Dinleyen		Alıcı		BB84		B92	
Çıkış	Filtre	Çıkış	Filtre	Çıkış	Durum	Dinleme	Durum	Dinleme
–	+	–	+	–	OK	Yok	NOK	
–	+	–	×	/	NOK		NOK	
–	+	–	×	\	NOK		OK	Yok
–	×	/	+	–	OK	Yok	NOK	
–	×	/	+	|	OK	Var	OK	Var
–	×	/	×	/	NOK		NOK	
–	×	\	+	–	OK	Yok	NOK	
–	×	\	+	|	OK	Var	OK	Var
–	×	\	×	\	NOK		OK	Yok

3.3.3. SARG04(Scarani&Acin&Ribordy&Gisin) protokolü

2004 yılı içerisinde önerilen bu yeni protokol kuantum şifreleme tekniğinin ticari uygulamalarda kullanılmasına başlandığını gösterir. Hali hazırda icat edilmemiş olan bu yöntem gelecekteki teknolojik gelişmelerin kullanılması öngörüldüğünde BB84 tarzı protokollerde ne kadar önemli derecede bir risk olduğunu gösterir (ANONİM, 2015b).

Günümüzde kullanılan kuantum anahtar dağıtımı uygulamaları içerisinde fiber optik hat ya da ışın dalgası kullanılarak iletim sağlayan hatlar kullanılarak işlemler gerçekleştirilir. Fakat bu yöntemin uygulaması ile karşılaşılan bazı problemlerden biri, belirtilen foton üreteçleri olarak bilinen cihazların, bir kubit içi iletim gerçekleştirilmesi esnasında yalnızca bir tane foton üretmemesi bunun yerine benzer polarizasyonlarda birden fazla foton üretimi gerçekleştirmesidir. BB84 protokolünde risk bu durumda meydana gelmektedir. Önceden de belirtildiği üzere BB84 protokolü gönderim işlemini tamamlayınca alıcı, okuma işlemi sırasında kullanmış olduğu filtre türlerini genel kanal üzerinden göndericiye bildirir. Eğer ki gizli bir şekilde hattı dinlemekte olan kişi, her bir kubit değerinde üretilerek gönderilen N adet foton içerisinde bir âdetini yakamla imkânı sağlarsa bu değeri genel kanal üzerinden yapılan filtre yayınlama işlemine kadar kuantum bellek üzerinde saklama imkânı bulabilirse anahtarı öğrenebilme ortamı oluşmaktadır.



Şekil 3.7. SARG Protokolü İçin Polarizasyon-Kubit Değeri Eşleşmesi

PNS tarzı saldırılara karşı BB84 protokolünün savunma konusunda yetersiz olduğunu gözlemleyen Scarani ve ark. anahtar doğrulama işlemini açık kanaldan yapılabilirliği üzerine düzenlemeler yapmıştırlar. Yeni oluşturulan metot ile alıcı taraf, okumanın gerçekleşmesi esnasında kullanmış olduğu filtrelerin açıklanmaması, yalnızca gönderici tarafının göndermiş olduğu polarizasyon ve bu polarizasyon ile 45º açı yapabilen farklı bir polarizasyonun açıklamasıdır. Farz edelim ki alıcı taraf, açıklanmış olan polarizasyon değerlerinden herhangi birine $90^{0'}$lik bir açı gerçekleştirerek okuma yapmış ise yapmış olduğu okumanın geçerli sayıldığını karşı tarafa bildirir ayrıca okumuş olduğu kubit değerinin tümleyenini anahtara dâhil eder. Şekil 3.7.'de gösterilen polarizasyon-kubit değer eşleşmesi ile bu protokol içerisinde

gerçekleşmekte olan gönderme işleminde oluşan ilişki 0º açıda polarizasyon değerine sahip bir fotonda muhtemel ihtimalleri gösteren altı değişik iletim durumu Tablo 3'de görülmektedir.

Çizelge 3.3. 0 Derece Açı ile Polarizasyona Sahip Bir Fotonun Olası İhtimallerinde SARG Protokolü ile Altı Farklı İletimi

Gönderim Polarizasyonu	Açıklanan Pol. Çifti	Okuma Filtresi	Okunan Polarizasyon	Kabul Durumu	Kubit Değeri
–	/ –	+	–	Geçersiz	
–	/ –	×	/	Geçersiz	
–	/ –	×	\	Geçerli	0
–	\ –	+	–	Geçersiz	
–	\ –	×	/	Geçerli	0
–	\ –	×	\	Geçersiz	

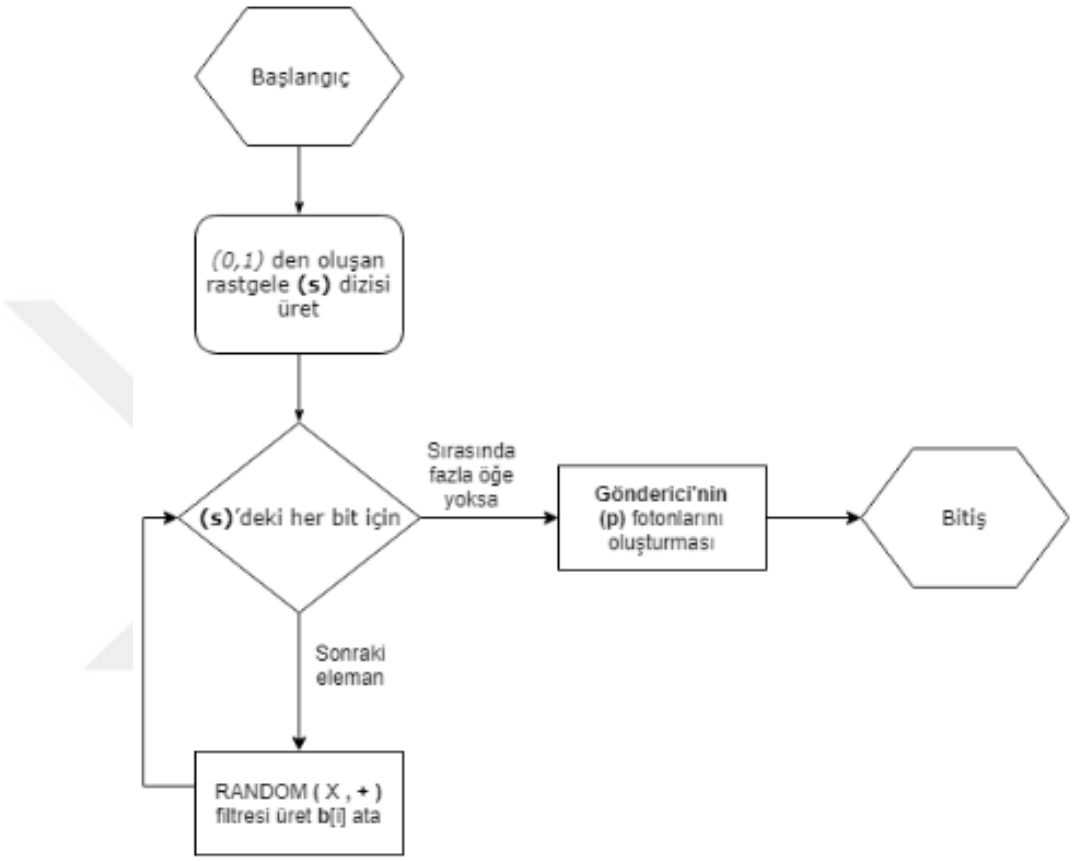
3.3.4. E91 protokolü

1991 yılında Artur Ekert tarafından E91 adı ile kuantum anahtar dağıtımı için yeni bir yaklaşım geliştirmiştir. Heisenberg belirsizlik ilkesi BB84 protokolünde olduğunun aksine E91 protokolünde kullanılmaz. Bu protokolün kendine temel aldığı ilke iki fotondaki kuantum hallerinin birlik olmasıdır. Hem alıcı tarafına hem de gönderici tarafına birer adet foton gelir. Gerçekleşen bu işlem sırasında fotonların durumları kendi aralarında karşıt değer içerdikleri için alıcı taraf gönderici tarafın kuantum durumunu öngörebilmektedir. Bu durumda hem gönderici hem de alıcı tarafın ortak kullanabileceği bir anahtarın oluşturması sağlanır (Bodur, 2016)

3.4. Yapılan Çalışmalar

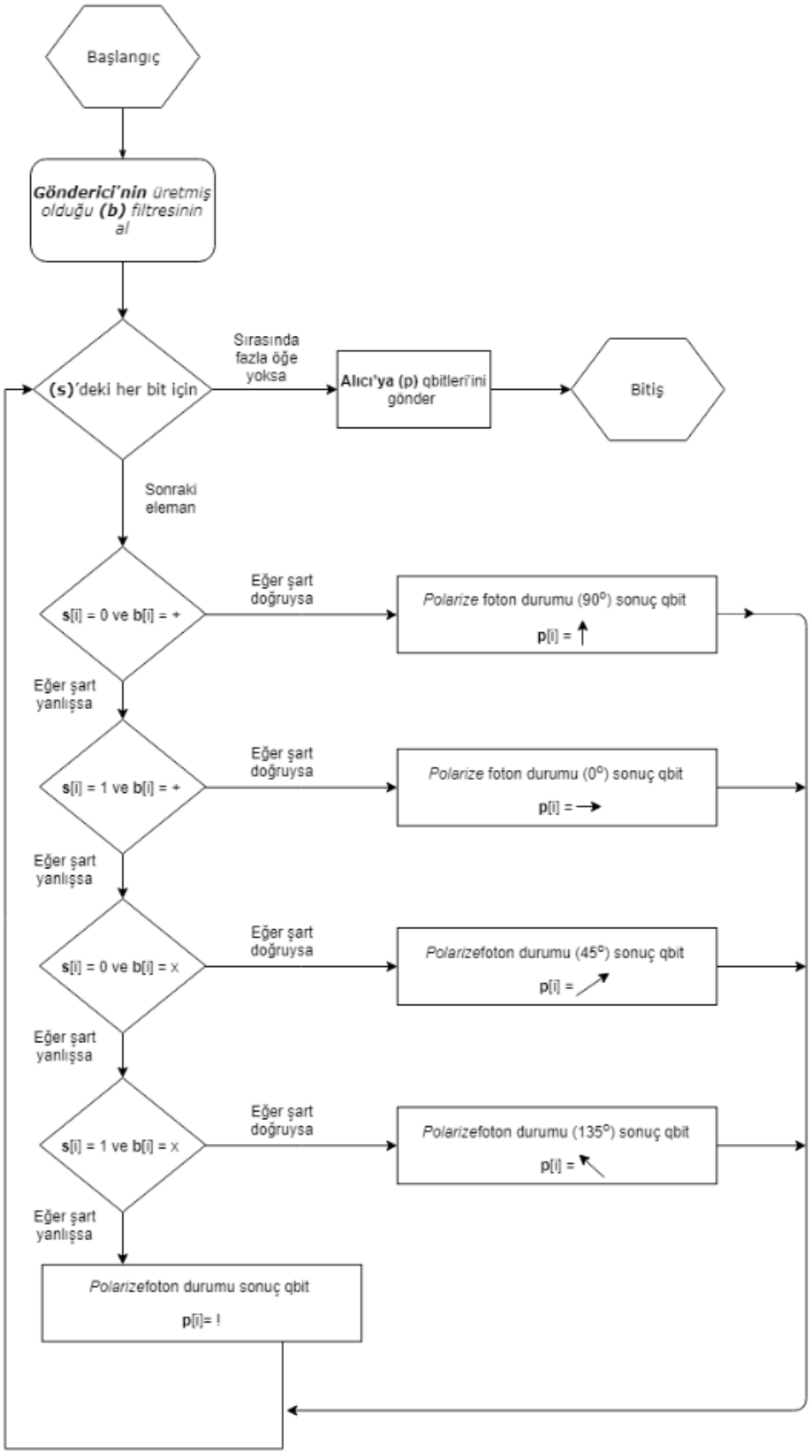
3.4.1. BB84 protokolü algoritması

Kuantum kanalı üzerindeki iletişim;



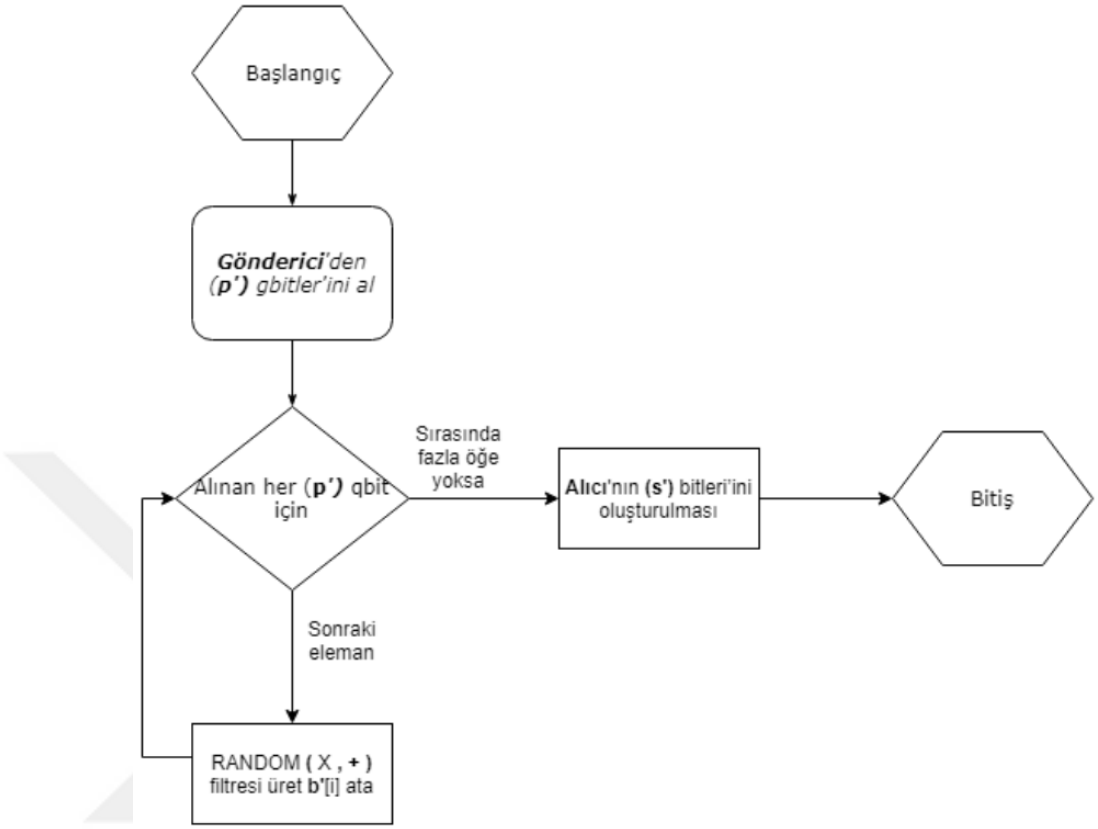
Şekil 3.8. Gönderici - Kuantum Kanal Üzerindeki İletişim Diyagramı

- Şekil 3.8.'deki diyagramda gösterildiği gibi Gönderici, rastgele üretmiş olduğu filtre dizisi ve bu diziler için rastgele oluşturmuş olduğu bit dizisini karşılaştırarak, Şekil 3.9.'ddki diyagramda gösterilen foton (0, 45, 90,135 derecelik) polarizasyonu elde etmiş olur.



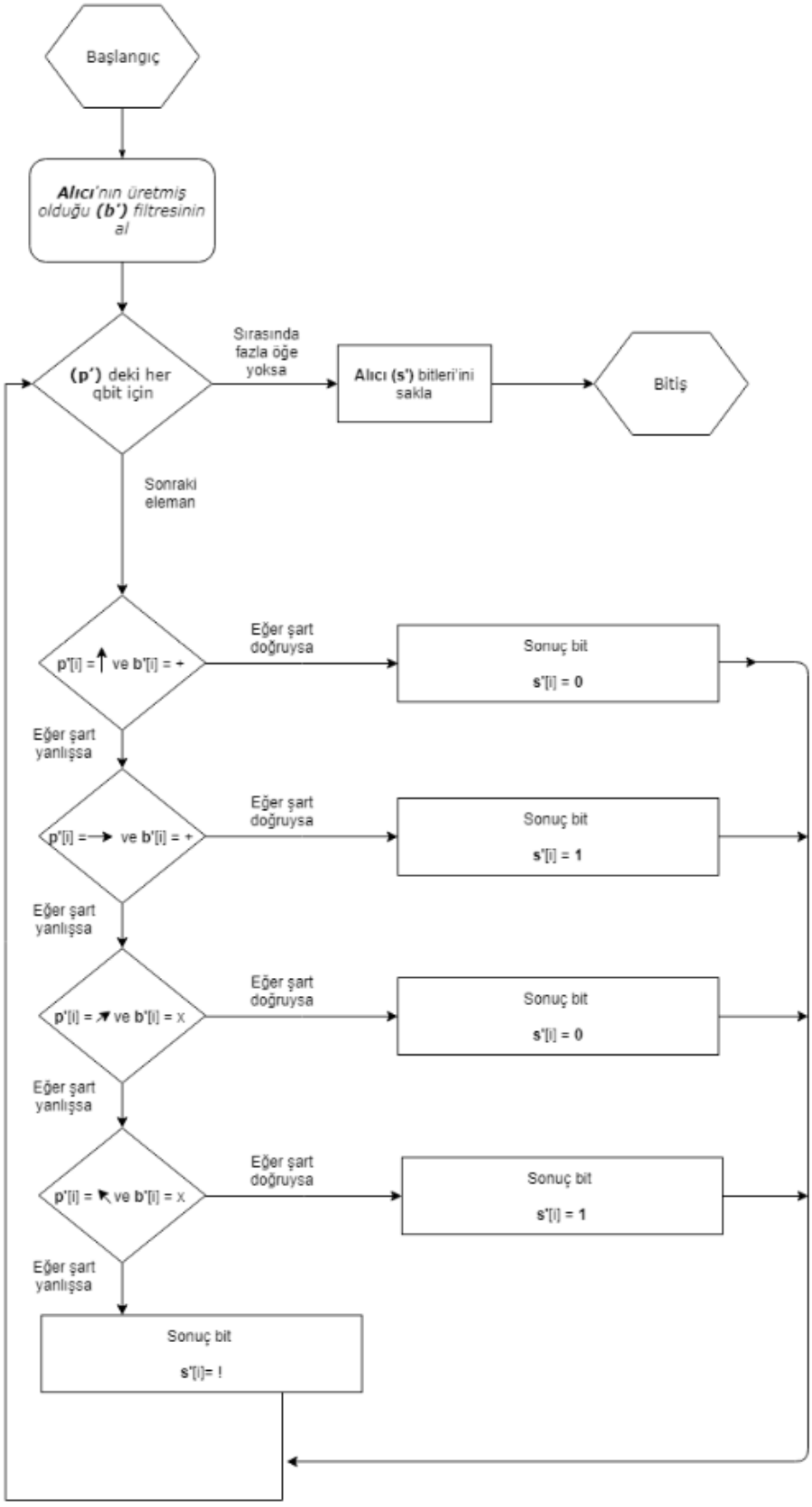
Şekil 3.9. Gönderici Foton Oluşturma Diyagramı

- Gönderici, her bir foton polarizasyonunu kaydeder ve bunu Alıcı'ya gönderir.



Şekil 3.10. Alıcı - Kuantum Kanal Üzerindeki İletişim Diyagramı

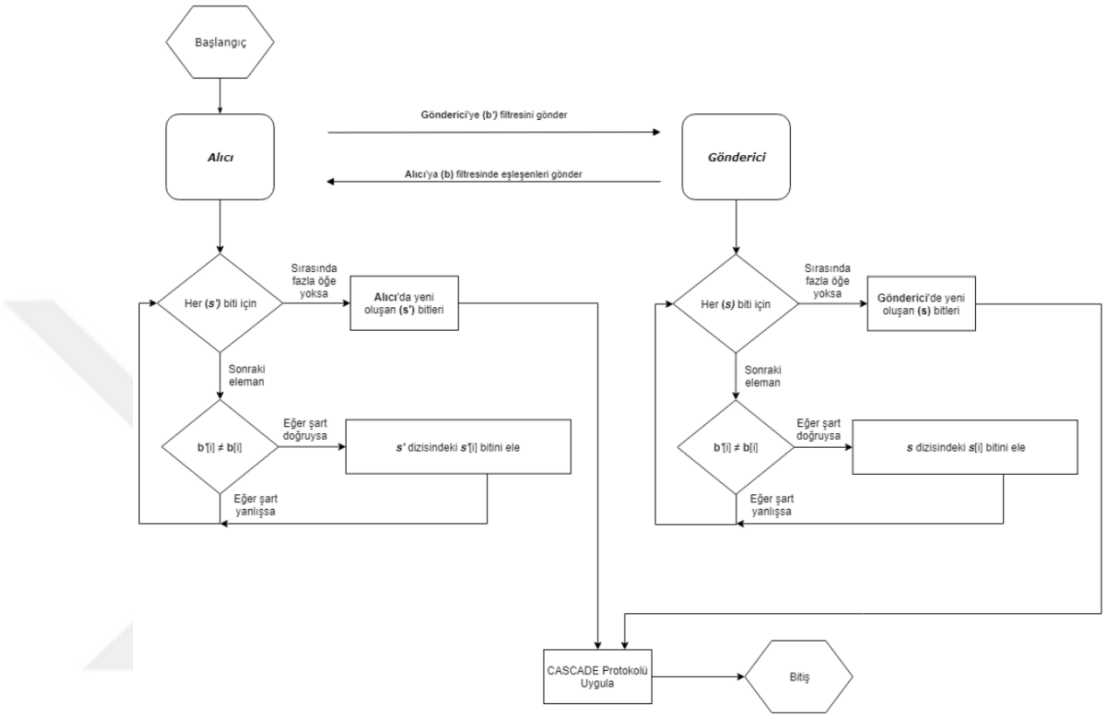
- Şekil 3.10.'da görülen diyagramda Alıcı, Gönderici tarafından gönderilen fotonları alır ve her bir foton için kendi içerisinde rastgele üretmiş olduğu doğrusal ya da diyagonal filtre sistemini kullanır. Alıcı, ölçüm türünü ve ortaya çıkan polarizasyonu kaydeder. Alıcı, ölçümlerden hangisinin deterministik olduğunu bilmez, Gönderici ile aynı ölçüm türünü kullanır. Alıcı, üretilen rastgele filtreden geçmeyen fotonlar için filtreye uygun rastgele foton üretir. Bütün ölçümlerden sonra Şekil 3.11.'de gösterilen diyagram adımları ile Alıcı ikili bir diziye sahip olacaktır.



Şekil 3.11. Alıcı Foton Oluşturma Diyagramı

Gönderici ve Alıcı, bu aşamadan sonra genel bir kanal üzerinden iletişim kurarak işlemine devam eder.

Klasik bir kanal üzerinden iletişim;



Şekil 3.12. Gönderici - Alıcı Klasik Kanal Üzerinden İletişim

- Şekil 3.12.'deki diyagramda görüldüğü gibi Ortak kanal üzerinden Alıcı, her bir ölçüm için kullanmış olduğu filtre sistemini Gönderici'ye iletir. Gönderici dizi içerisinde eşleşen filtreleri Alıcı'ya iletir. Eşleşmeyen filtreler diziden çıkartılır. Eğer üçüncü bir kişi dinleme yapmadıysa (gürültü hariç) sonuçta üretilen anahtar aynı olacaktır. Eğer üçüncü bir kişi dinleme işlemi yapmış (gürültü hariç) ise üretilen anahtar farklı olacaktır. Bu durumda CASCDE Protokolü uygulanarak Hata Sezme ve Düzeltme işlemi yapılır (Singh ve ark., 2014).

3.4.2. CASCADE (Hata Tespit ve Düzeltme) protokolü algoritması

CASCADE protokolünde ana mantık elinde bulundurmuş olduğu mesajları bloklar haline getirerek bu blokları temsil eden pariti(eşlik) değerlerini eşleştirerek hataların tespit edilmesini sağlayarak gerektiğinde düzeltme işlemi yapmasıdır. Bu protokol ile verimliliğin artırılmasında bütün blokların bir kaydının tutulması gerekmektedir. CASCADE protokolünde kullanılması planlanan BINARY işlemi için gerekli adımlar;

BINARY işlem için Gönderici'nin elinde bulundurduğu A ile Alıcı'nın elinde bulundurduğu B dizilerinde tek (1,3,5…) olarak belirtilen sayıda hatanın tespit edilmesi durumunda,

1. Gönderici kendinde bulunan A dizisini iki parça haline getirip ilk parça tarafından hesaplanan eşlik değeri Alıcı'ya iletir.
2. Alıcı kendinde bulunan B dizisini aynı yöntem ile iki parça haline getirip tek sayıdaki hatayı barındıran parçayı bulmak için Gönderici tarafından gelen eşlik değeri ile karşılaştırma işlemi gerçekleştirir.
3. Bir hata bulununcaya değin belirtilen bu iki işlem tekrarlanır.

CASCADE işlemi içi protokol birden fazla çevrim ile gerçekleşir. Çevrim sayısı Gönderici ile Alıcı tarafından CASCADE protokolü çalıştırılmadan belirlenir. Belirlenen seçim ile kuantum kanalı hata olasılık değeri ∈ parametresiyle ilgilidir.

Gönderici ile Alıcı tarafından oluşturulan bit dizileri sırası ile,

A = A1,A2,.....,AN;
B = B1,B2,…….,BN; *(Ai,Bi ∈ {0; 1}) olsun:*

Gönderici ile Alıcı, ilk çevrim olan blok uzunluk değeri için k_1 değerini belirleyip mevcut olan dizileri belirtilen k_1 bitlik bloklar haline getirir. Pozisyonları $K_v^1 = \{l|(v-1)k_1 < l \leq vk_1\}$ olan bütün bitler 1. çevrimde v. bloğunu oluştururlar. Bu durumda Gönderici, tüm bu blokların pariteleri değerlerini Alıcı'ya

gönderir. Alt kısımda belirtilen BINARY işlemi kullanılarak Alıcı kendindeki eşlik değeri ile Gönderici'deki eşlik değerine karşılık gelen her farklı blok için hata düzeltilir. Çevrim sonunda Alıcı'da bulunan blokların tamamı çift (0,2,4,…) sayıda olacaktır.

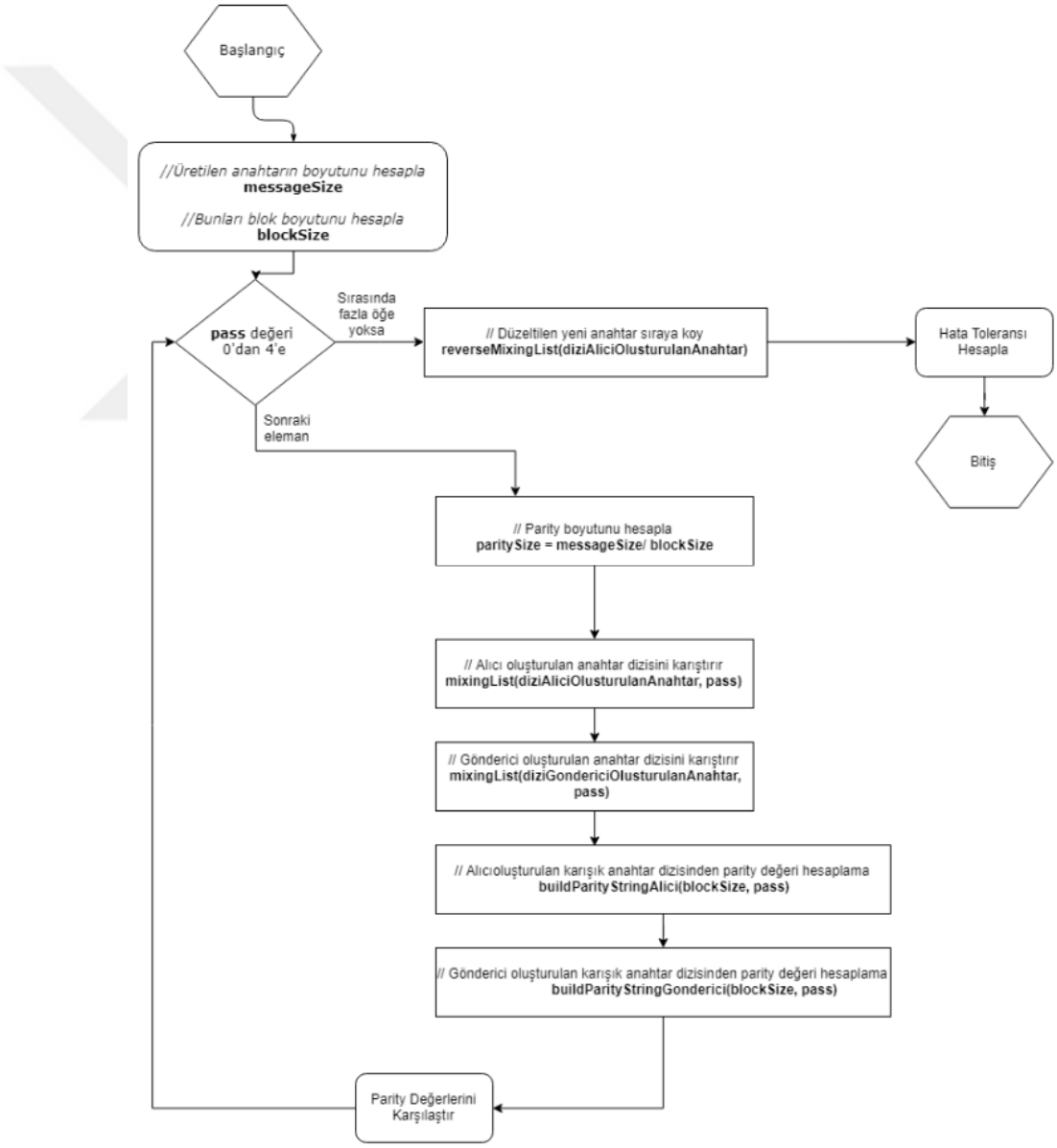
Tüm $i > 1$ çevrimlerinde, Gönderici ile Alıcı k_i değerini rastgele bir fonksiyonla üretir $fi : [1..n] \rightarrow [1..\left\lceil\frac{n}{k_i}\right\rceil]$. Pozisyonları $K_j^i = \{l|fi(l) = j\}$ olan bütün bitler i. çevrimin j. bloğunu oluşturur ve Gönderici tarafından her bir $j(1 \leq j \leq \left\lceil\frac{n}{k_i}\right\rceil)$ mesaj blok eşik değeri hesaplanır ve tamama Alıcı'ya gönderilir.

$$aj = \bigoplus_{l \in K_j^i} = A_l$$

Alıcı ise kendi bj eşik değerlerini aynı yöntem ile hesaplayıp onları Gönderici tarafından gelen aj'ler ile karşılaştırır. Yapılan her bir hesaplamada $bj != aj$ durumu için K_j^i olarak tanımlanan blok da BINARY metodu çalıştırılır. Alıcı, bu işlemden sonra $Bl != Al$ olan bir $l \in K_j^i$ bulup onu düzeltme işlemi uygulayacaktır. Son olarak, Gönderici ile Alıcı geriye doğru izleme prosedürün gerçekleştirirler.

Geriye doğru izleme: $l \in K_j^i$ durumu içerisinde $1 \leq u < i$ olarak tanımlana bütün eski u çevrimlerin de $l \in K_v^u$ olarak geçen tüm geçmiş K_v^u blokları bundan sonra tek sayıda hata tipine sahip olacaktır. Böyle olan bloklar kümesine K diyelim. Şu an Gönderici ile Alıcı, K'nın içermiş olduğu en küçük bloklar belirlenebilir ayrıca farklı bir hatayı tespit edebilmek için de BINARY metodu kullanılmaya devam edilir. A ile B dizilerinde ki tespit edilen bu yeni hatanın pozisyonu için l' değişkenini kullanalım. Buradaki $B_{l'}$ bitinde düzeltme işlemi yapıldıktan sonra, Alıcı her bir hesaplanan u çevrimi için $B_{l'}$ bitini içeren blokları oluşturup B kümesini de bu bloklar ile belirleme durumuna sahiptir. Ayriyeten, $K' = (B \cup K) \setminus (B \cap K)$ değeri hesaplanarak tek sayıda ki hataları içeren blokların kümesi olarak tanımlanan K' kümesi elde edilir. Eğer ki $K' \neq \emptyset$ (bloklar içerisinde tek sayıda hata var, $\emptyset$: boş küme) durumu oluşur ise

Alıcı benzer yöntemle farklı bir hata çifti bulup düzeltme işlemi uygular. Bu süreç içersinde $K' = \emptyset$ (bloklar içerisinde tek sayıda hata yok) sonucuna ulaşıncaya denk tekrarlama işlemi uygulanır. Geriye doğru izleme prosedürü sonlandığı zaman Gönderici ile Alıcı, i. çevrim içerisindeki eşlik değerlerinin karşılaştırılması işlemine devam eder. Tek bir eşlik değerinin farklı olması durumunda yeni bir geriye doğru izleme süreci başlatılır. Bütün eşlik değerleri kontrol edilip sonrasında i. çevrim sonlandırılır. Bu noktada sonra, 1. çevrim ile i. çevrim arasındaki blokların tümü çift sayıda (muhtemelen 0) hata içerir (Toyran ve ark., 2012).

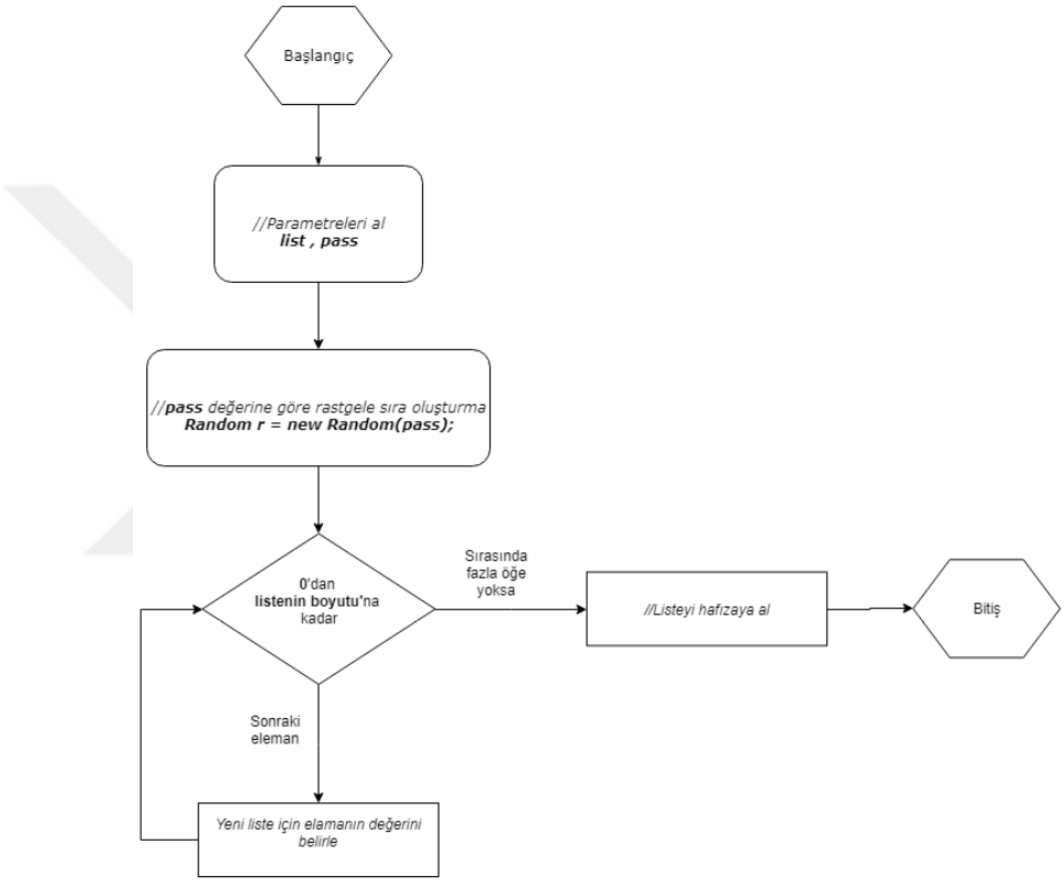


Şekil 3.13. CASCADE Hata Bulma Diyagramı

Cascad protokolünde ana mantık Şekil 3.13.'de de görüldüğü üzere;

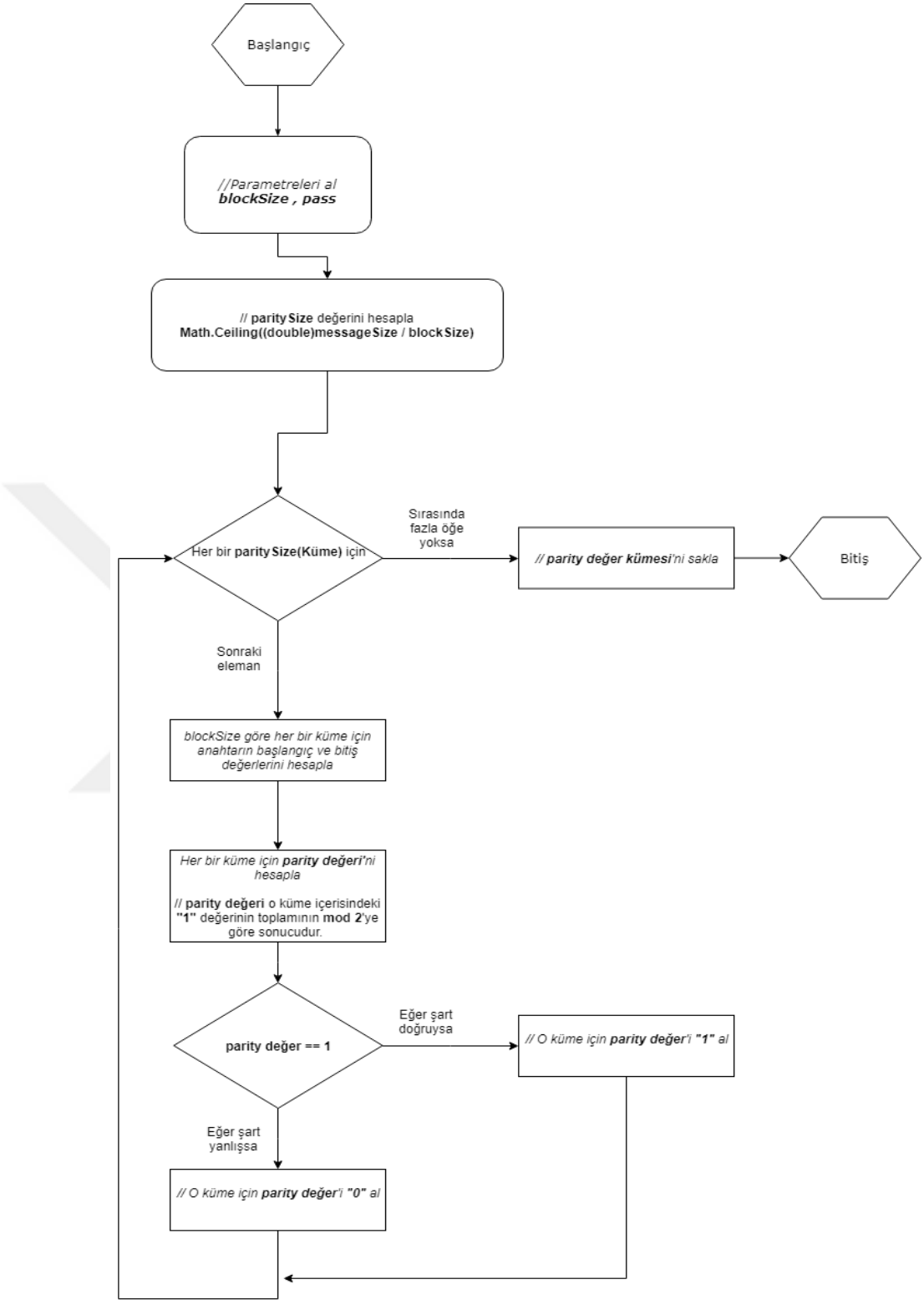
Gönderici ve Alıcı tarafından

- Elindeki bit dizisini Şekil 3.14.'de gösterilen diyagrama uygun bir şekilde karıştır



Şekil 3.14. Diziyi Karıştırmak için Kullanılan Algoritmanın Diyagramı

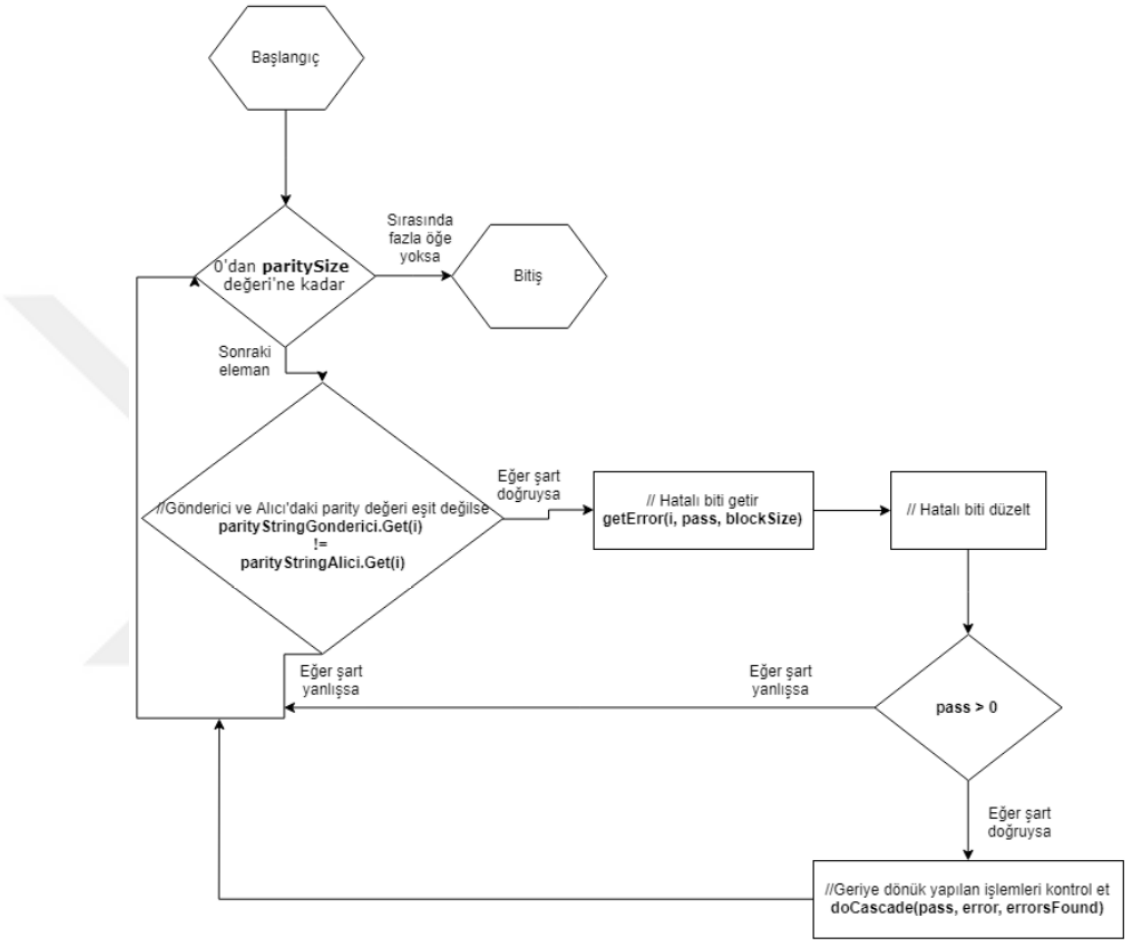
- Elindeki bit dizisini bloklara ayır
- Her bir blok için Şekil 3.15.'de gösterilen diyagrama uygun **Parity Değerini** hesapla



Şekil 3.15. Bloklara Ayrılmış Dizinin Parity Değerini Hesaplama Algoritması Diyagramı

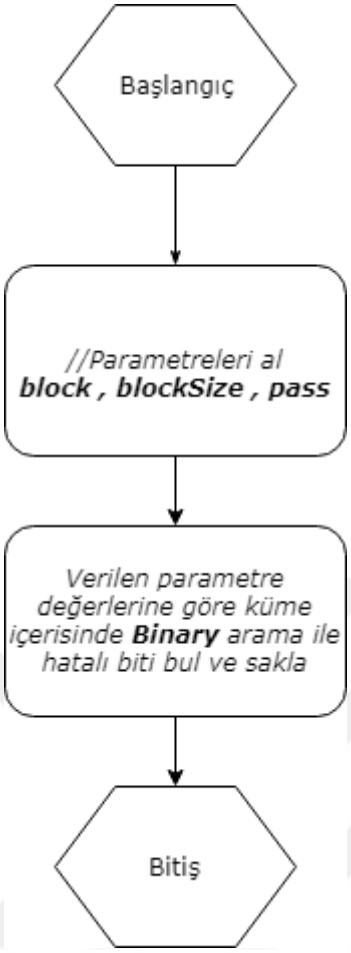
Alıcı tarafında

- Şekil 3.16.'daki diyagramda görüldüğü gibi Göndericideki her bir bloğun **Parity Değeri** ile kendi **Parity Değerini** karşılaştır



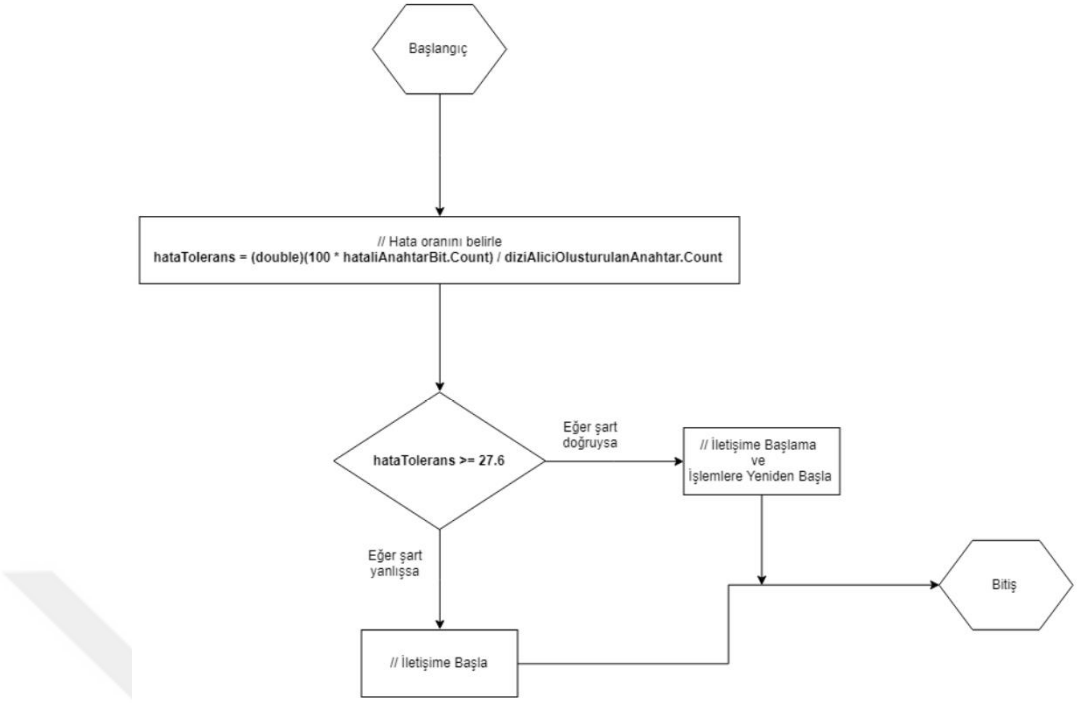
Şekil 3.16. Gönderici - Alıcı Parity Değerlerin Karşılaştırma Algoritma Diyagramı

- Eğer eşleşmeyen blok varsa o blok için **Binary** işlem ile hatalı biti bulup düzeltme işlemi uygula (Şekil 3.17.).



Şekil 3.17. Hatalı Bit Bulmak için Kullanılan Algoritma Diyagramı

- Düzeltme işlemi sonucunda yapılan hata oranı kontrolünde hata oranı >= 27.6 ise CASCADE Protokolüne göre iletişim başlatma ve tüm işlem tekrardan yap(Şekil 3.18.).



Şekil 3.18. Hata Toleransı Hesaplamak için Kullanılan Algoritma Diyagramı

3.4.3. Vernam şifreleme algoritması

Vernam şifrelemesinde bir mesajın şifreli olduğunu "***E***" (Encrypted), şifreli mesajın çözüldüğünü belirtmek için "***D***" (Decrypted) terimleri kullanılmaktadır. Anahtar belirtmek için "***k***", mesaj belirtmek için "***m***", şifrelenmiş mesajın "***c***" ile gösterilmesi durumunda "***j***" miktardaki bit karakterinde;

$E (k_j, m_j) = k_j$

$U\ m_j = c_j$

$D (k_j, c_j) = k_j$

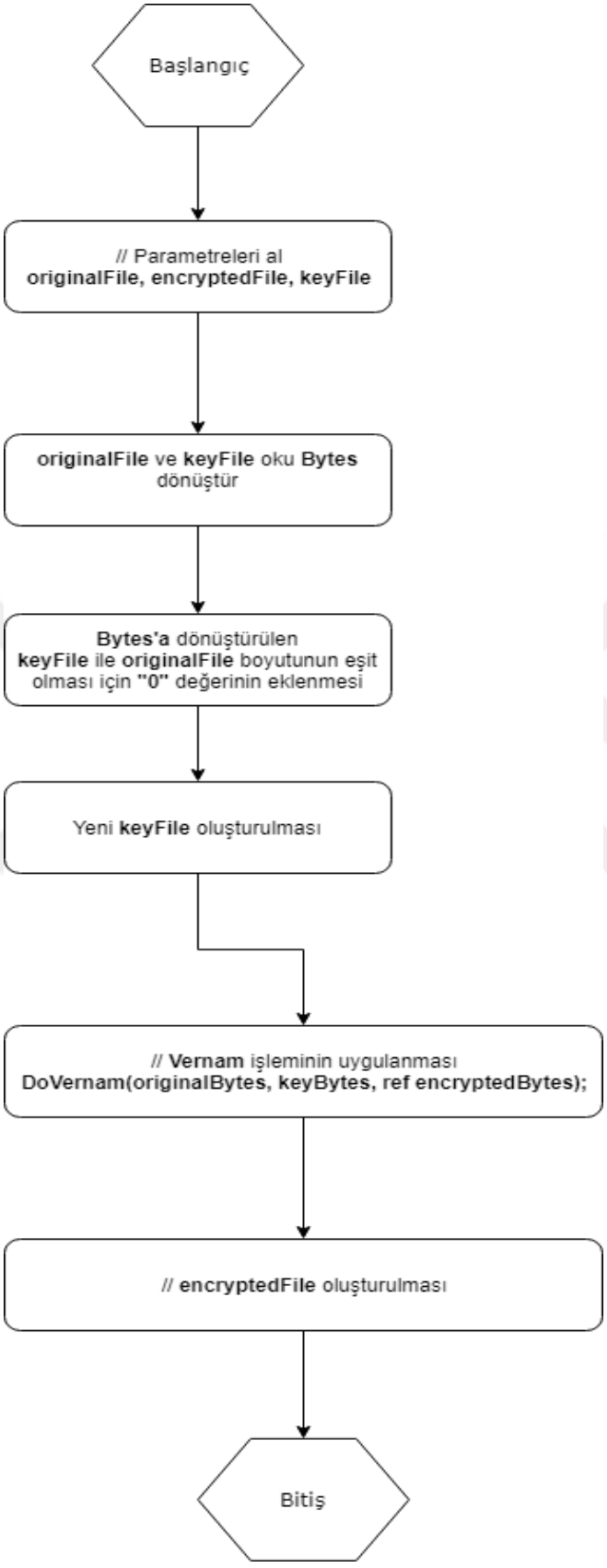
$U\ c_j = m_j$ dir.

Mesaj olarak $m_0,m_1,m_2,\ldots\ldots,m_j$, anahtar olarak $k_0,k_1,k_2,\ldots\ldots,k_j$, ve şifrelenmiş mesaj olarak $c_0,c_1,c_2,\ldots\ldots,c_j$ gösterilmekte ve j karakteri için bit indeksi olarak (j+1) kullanılmaktadır.

Algoritmanın test edilmesi durumunda;

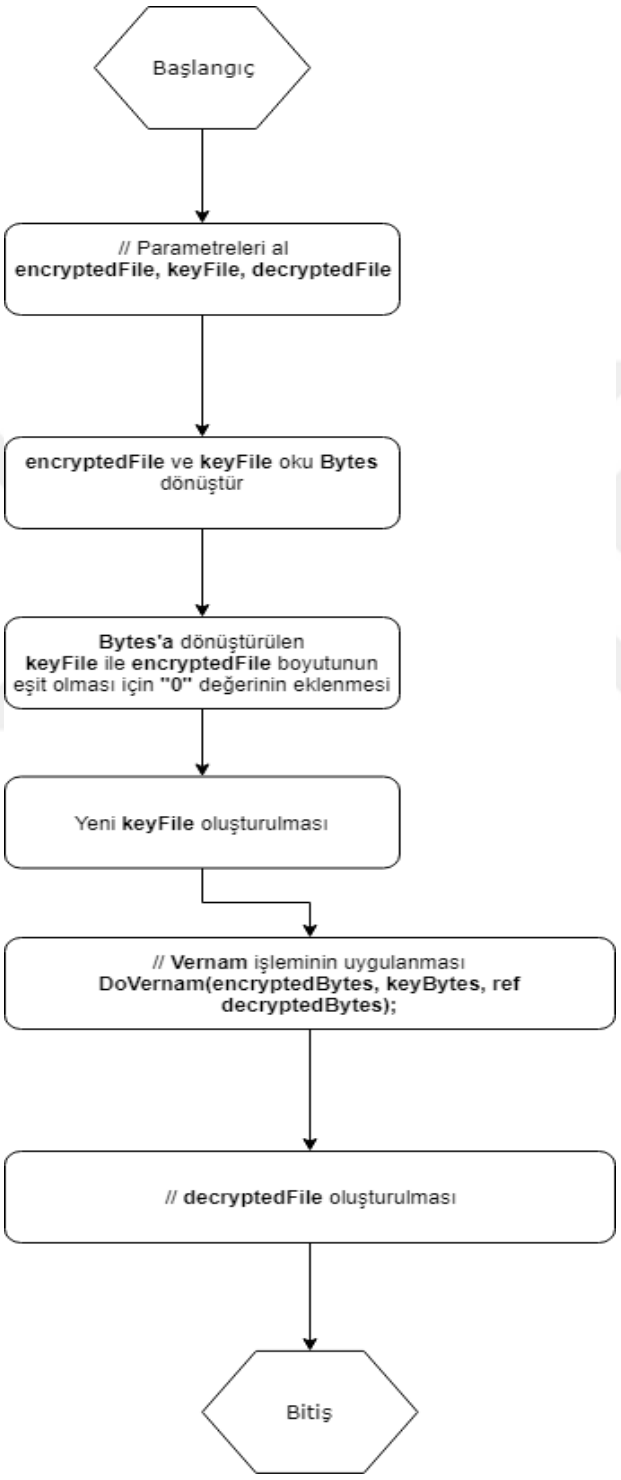
$m_j = D (k_j , E (k_j , m_j))$ olarak hesaplanmaktadır.

Şekil 3.19.'daki akış diyagramında görüldüğü gibi vernam şifreleme tekniğinde orijinal dosya ile anahtar dosyası boyutunun eşitlenmesinden sonra yeni bir anahtar dosyası oluşturulup vernam işlemi uygulanarak şifrelenmiş dosya üretilir.



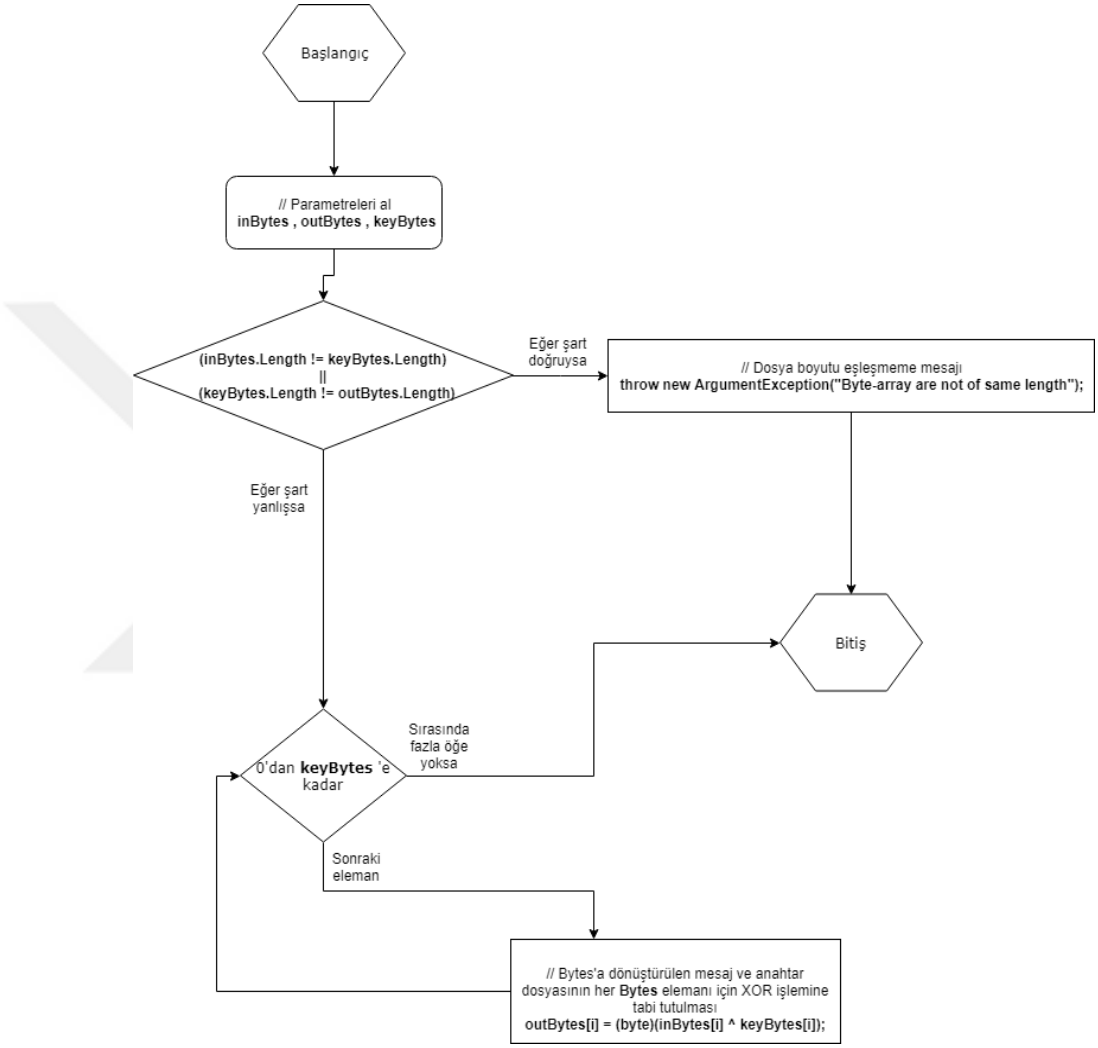
Şekil 3.19. Vernam Encrypt Algoritması Akış Diyagramı

Şekil 3.20.'deki akış diyagramında ise vernam şifre çözme tekniği ile şifrelenmiş dosya ile anahtar dosyası vernam işlemi uygulanarak orijinal dosya oluşturulur.



Şekil 3.20. Vernam Decrypt Algoritması Akış Diyagramı

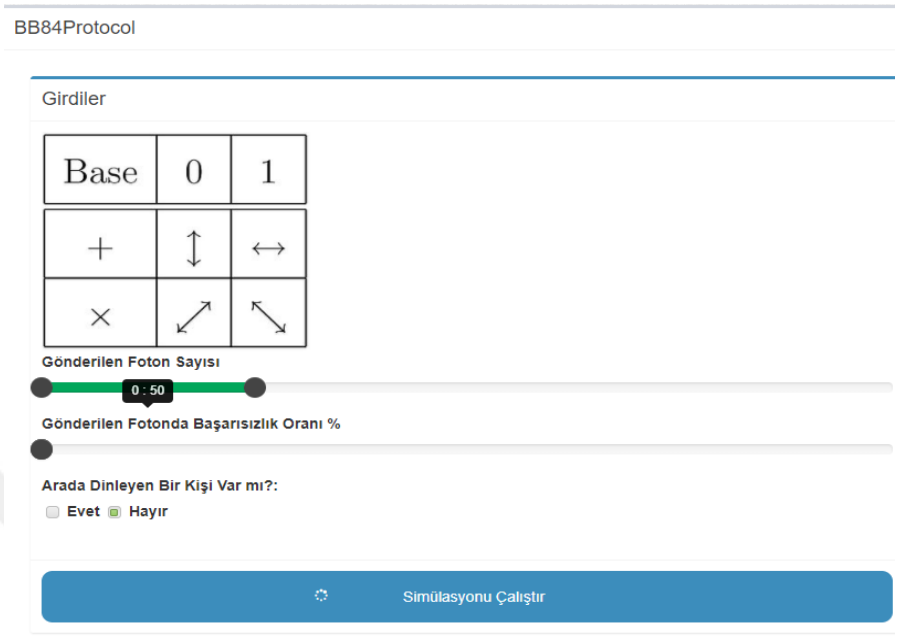
Şekil 3.21.'deki akış diyagramında ise vernam işleminin uygulanması görülmektedir. Şifrelenecek ya da şifresi çözülecek dosya ile anahtar dosyası Bytes boyutunda XOR işlemine tabi tutularak şifrelenecek dosyalar şifrelenir, şifresi çözülecek dosyalar orijinal haline dönüştürülür.



Şekil 3.21. Vernam Algoritması Akış Diyagramı

3.5. Uygulama

3.5.1. BB84 protokol uygulaması

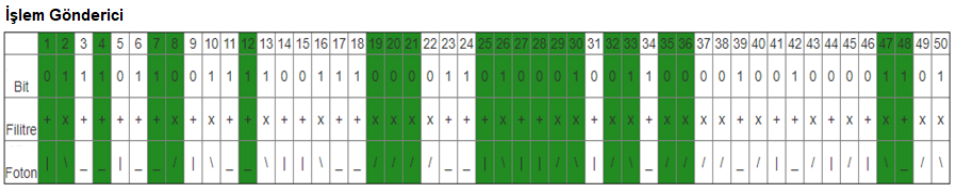


Şekil 3.22. BB84 Simülasyonun Foton Sayısı 50, Kayıp ve Dinleme Olmadan Çalıştırması

Şekil 3.22.'de göründüğü gibi simülasyon için 3 girdi parametresi ile işlem gerçekleşmiştir. Bunlar;

- Gönderilen foton sayısının belirlenmesi
- Foton kayıp oranının belirlenmesi
- Arada dinleyicinin olup olmaması

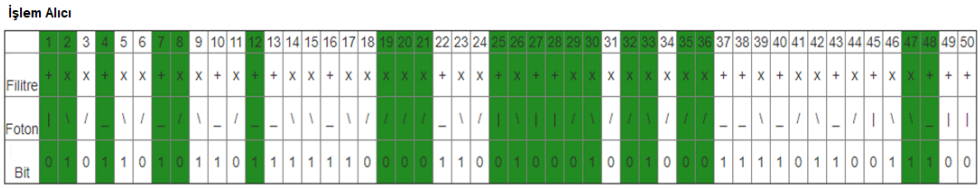
a. Simülasyon girdi değerleri için ilk olarak **foton sayısı 50** belirleyip **kayıp (başarısız)** ve **dinlemenin olmadığı** bir ortam varsayarak simülasyonu çalıştırdık.



Şekil 3.23. Foton Sayısı 50, Kayıp ve Dinleme Olmadan Gönderici Tarafından Oluşan Simülasyon Sonucu

Şekil 3.23.'deki tabloda görüldüğü üzere Gönderici tarafından 50 Bitlik rastgele bir dizi oluşturulup bu 50 Bite karşılık rastgele Doğrusal ya da Diyagonal filtre sistemi üretilip bunlara karşılık gelen fotonlar oluşturulmuştur.

Oluşturulan bu fotonlar Şekil 3.2.'de gösterildiği gibi Kuantum Kanal (Fiber optik) üzerinden Alıcı'ya gönderilir.

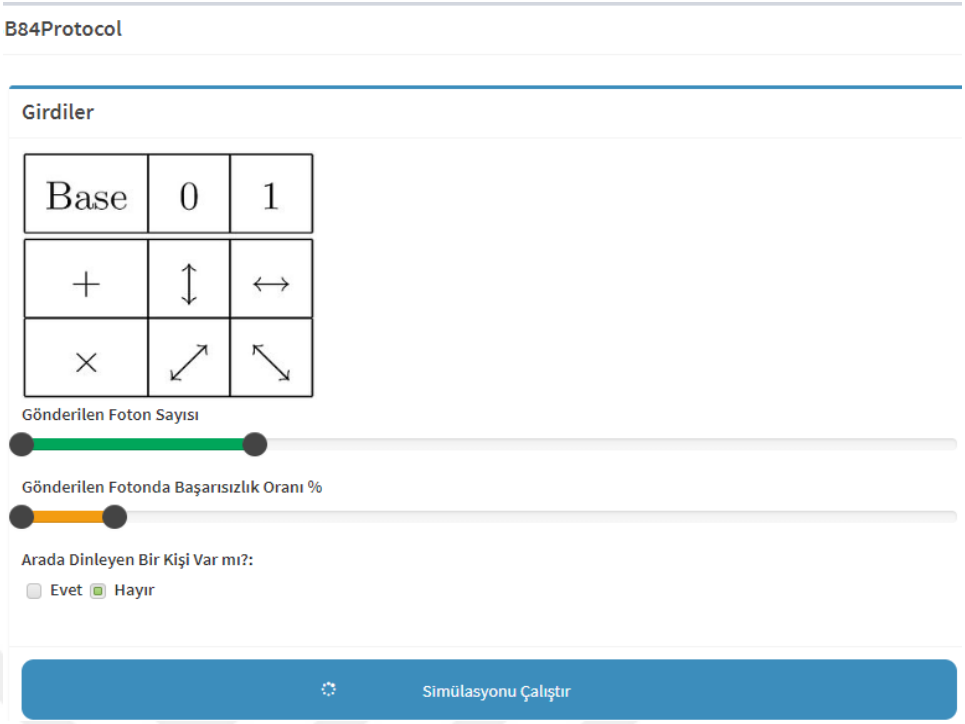


Şekil 3.24. Foton Sayısı 50, Kayıp ve Dinleme Olmadan Alıcı Tarafından Oluşan Simülasyon Sonucu

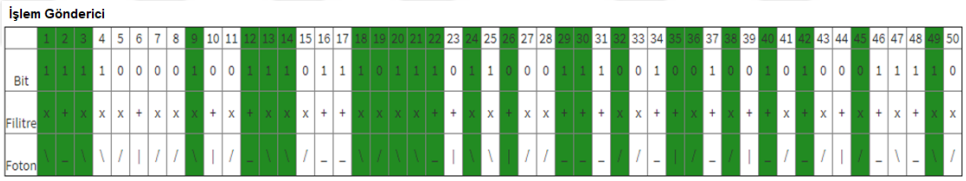
Şekil 3.24.'deki tabloda Alıcı, Gönderici tarafından gönderilen fotonları alarak her bir foton değeri için rastgele bir filtre (Doğrusal ya da Diyagonal) oluşturularak bunlara karşılık gelen bit (0 ya da 1) değeri üretilir.

Alıcı işlem sonucunda oluşturmuş olduğu filtre dizisini Göndericiye gönderir. Şekil 3.23. ve Şekil 3.24.'de görüldüğü üzere eşleşen filtre bitleri (1, 2, 4, 7, 8, 12, 19, 20, 21, 25, 26, 27, 28, 29, 30, 32, 33, 35, 36, 47, 48) yeşil renk olarak belirtilmiştir. Arada bir dinleyici ve kayıp olmadığı için fotonlarda polarizasyon oluşmamıştır. Gönderici eşleşen bu filtre bitlerini Şekil 3.2.'de gösterilen Genel Kanal üzerinden Alıcı'ya gönderir. Gönderici ve Alıcı tarafından da bu filtre bitlerine karşılık gelen Bitler saklanır diğer Bitler diziden çıkartılarak 50 dizilik bir foton gönderme işleminden sonra 21 dizilik(bitlik) bir anahtar oluşturulur.

b. Şekil 3.25.'de gösterildiği gibi simülasyon girdi değerleri için ikinci olarak **foton sayısı 50** belirleyip **kaybın olduğu, dinlemenin olmadığı** bir ortam varsayarak simülasyonu çalıştırdık.



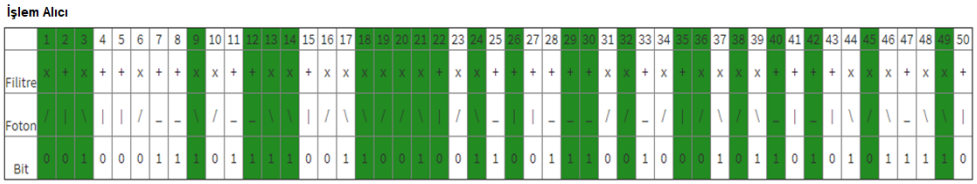
Şekil 3.25. Simülasyonun Foton Sayısı 50, Kaybın Olup ve Dinlemenin Olmadığı Şekilde Çalıştırması



Şekil 3.26. Foton Sayısı 50, Kaybın Olup ve Dinlemenin Olmadığı Ortamda Gönderici Tarafından Oluşan Simülasyon Sonucu

Şekil 3.26.'daki tabloda görüldüğü üzere Gönderici tarafından 50 Bitlik rastgele bir dizi oluşturulup bu 50 Bite karşılık rastgele Doğrusal ya da Diyagonal filtre sistemi üretilip bunlara karşılık gelen fotonlar oluşturulmuştur.

Oluşturulan bu fotonlar Şekil 3.2.'de gösterildiği gibi Kuantum Kanal (Fiber optik) üzerinden Alıcı'ya gönderilir.

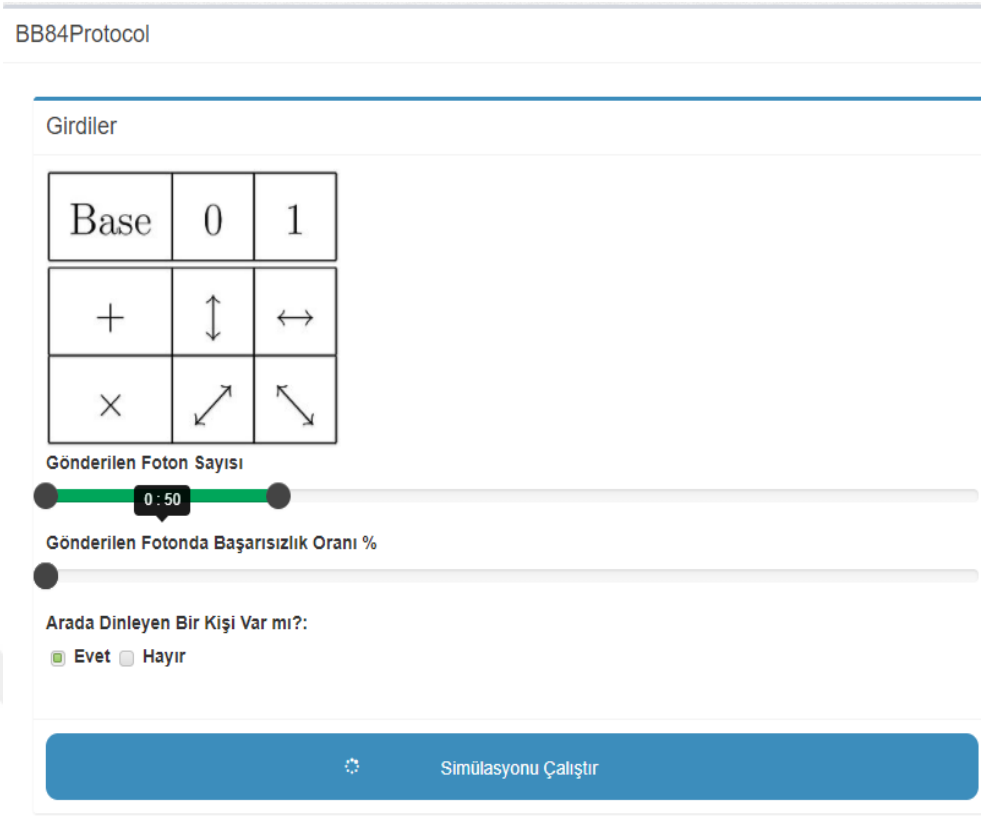


Şekil 3.27. Foton Sayısı 50, Kaybın Olup ve Dinlemenin Olmadığı Ortamda Alıcı Tarafından Oluşan Simülasyon Sonucu

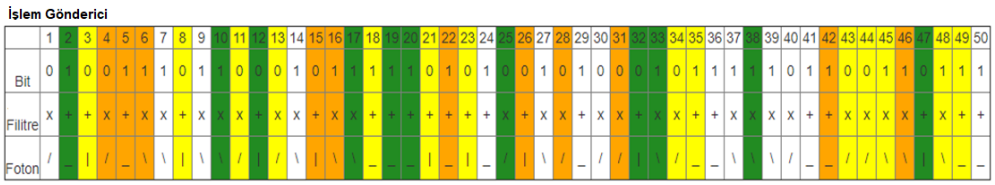
Şekil 3.27.'deki tabloda Alıcı, Gönderici tarafından gönderilen fotonları alarak her bir foton değeri için rastgele bir filtre (Doğrusal ya da Diyagonal) oluşturularak bunlara karşılık gelen bit (0 ya da 1) değeri üretilir.

Alıcı işlem sonucunda oluşturmuş olduğu filtre dizisini Göndericiye gönderir. Şekil 3.26. ve Şekil 3.27'de görüldüğü üzere eşleşen filtre bitleri (1, 2, 3, 9, 12, 13, 14, 18, 19, 20, 21, 22, 24, 26, 29, 30, 32, 35, 36, 38, 40, 42, 45, 49) yeşil renk olarak belirtilmiştir. Arada bir dinleyici yok fakat kayıp olduğu için fotonlarda polarizasyon oluşmuştur. Dikkatli bir şekilde incelendiğinde Gönderici ile Alıcı arasında (1, 2, 20, 22) filtre bitlerine denk gelen Filtreler aynı olmasına rağmen Foton ve Bit değerleri farklı olduğu gözlemlenmiştir. Buradan da anlaşıldığı üzere (1, 2, 20, 22) filtre bitlerinde polarizasyon meydana gelmiştir. Gönderici eşleşen bu filtre bitlerini Şekil 3.2.'de gösterilen Genel Kanal üzerinden Alıcı'ya gönderir. Gönderici ve Alıcı tarafından da bu filtre bitlerine karşılık gelen Bitler saklanır diğer Bitler diziden çıkartılarak 50 dizilik bir foton gönderme işleminden sonra 24 dizilik(bitlik) eşleşmeyen bir anahtar oluşturulur.

c. Şekil 3.28.'de gösterildiği gibi simülasyon girdi değerleri için üçüncü olarak **foton sayısı 50** belirleyip **kaybın olmadığı, dinlemenin olduğu** bir ortam varsayarak simülasyonu çalıştırdık.



Şekil 3.28. Simülasyonun Foton Sayısı 50, Kaybın Olmadığı ve Dinlemenin Olduğu Şekilde Çalıştırması



Şekil 3.29. Foton Sayısı 50, Kaybın Olmadığı ve Dinlemenin Olduğu Ortamda Gönderici Tarafından Oluşan Simülasyon Sonucu

Şekil 3.29.'daki tabloda görüldüğü üzere Gönderici tarafından 50 Bitlik rastgele bir dizi oluşturulup bu 50 Bite karşılık rastgele Doğrusal ya da Diyagonal filtre sistemi üretilip bunlara karşılık gelen fotonlar oluşturulmuştur.

Oluşturulan bu fotonlar Şekil 3.2.'de gösterildiği gibi Kuantum Kanal (Fiber optik) üzerinden Alıcı'ya gönderilir. Fakat Gizli Dinleyici bütün fotonları kendi alarak işlem gerçekleştirir.

İşlem Gizli Dinleyici

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50
Bit	1	0	0	0	1	1	0	0	0	1	0	0	0	0	0	1	0	1	0	1	0	1	0	1	0	0	0	0	1	0	0	0	1	0	1	1	1	1	0	1	0	1	0	0	1	1	1	1	1	1
Filitre	+	x	+	x	+	x	+	+	+	+	x	x	x	+	+	x	+	+	x	x	+	+	+	x	+	+	+	x	x	+	x	x	+	x	+	x	+	+	+	+	x	+	x	x	x	x	x	+	x	
Foton	–	/	|	/	_	\	|	|	|	_	/	/	/	|	|	\	_	/	\	|	_	\	|	|	|	/	\	|	/	/	_	/	_	|	_	/	_	/	/	\	\	\	\	_	\

Şekil 3.30. Foton Sayısı 50 Gizli Dinleyici Tarafından Oluşan Simülasyon Sonucu

Şekil 3.30.'daki tabloda Gizli Dinleyici, Gönderici tarafından gönderilen fotonları alarak her bir foton değeri için rastgele bir filtre (Doğrusal ya da Diyagonal) oluşturularak bunlara karşılık gelen bit (0 ya da 1) değeri üretilir.

Gizli Dinleyici işlem sonucunda oluşturmuş olduğu filtre dizisini Alıcı'ya gönderir. Şekil 3.29. ve Şekil 3.30.'da görüldüğü üzere eşleşen filtre bitleri (3, 4, 5, 6, 8, 11, 13, 15, 16, 18, 21, 22, 23, 26, 28, 31, 34, 35, 42, 43, 44, 45, 46, 48, 49) sarı renk olarak belirtilmiştir. Kaybın olmayıp fakat arada bir dinleyici olması sebebi ile fotonlarda polarizasyon meydana gelecektir.

İşlem Alıcı

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50
Filitre	+	+	x	x	+	x	+	x	+	x	+	+	+	+	+	x	x	x	+	+	x	+	x	x	x	+	+	x	x	+	x	+	x	+	x	x	+	+	+	+	x	+	+	+	+	x	+	x	x
Foton	–	|	/	/	_	\	|	\	|	|	_	|	_	|	\	\	/	_	|	/	_	/	\	\	|	|	/	\	|	/	|	/	\	\	_	|	_	/	_	_	|	_	\	\	|	\	\
Bit	1	0	0	0	1	1	0	1	0	1	1	0	1	0	0	1	0	1	1	0	0	1	0	1	1	0	0	0	1	0	0	0	0	0	1	1	1	1	0	1	0	1	1	0	1	1	0	0	1	1

Şekil 3.31. Foton Sayısı 50, Kaybın Olmadığı ve Dinlemenin Olduğu Ortamda Alıcı Tarafından Oluşan Simülasyon Sonucu

Şekil 3.31.'deki tabloda Alıcı, Gizli Dinleyici tarafından gönderilen fotonları Gönderici tarafından gönderilmiş gibi alarak her bir foton değeri için rastgele bir filtre (Doğrusal ya da Diyagonal) oluşturularak bunlara karşılık gelen bit (0 ya da 1) değeri üretilir.

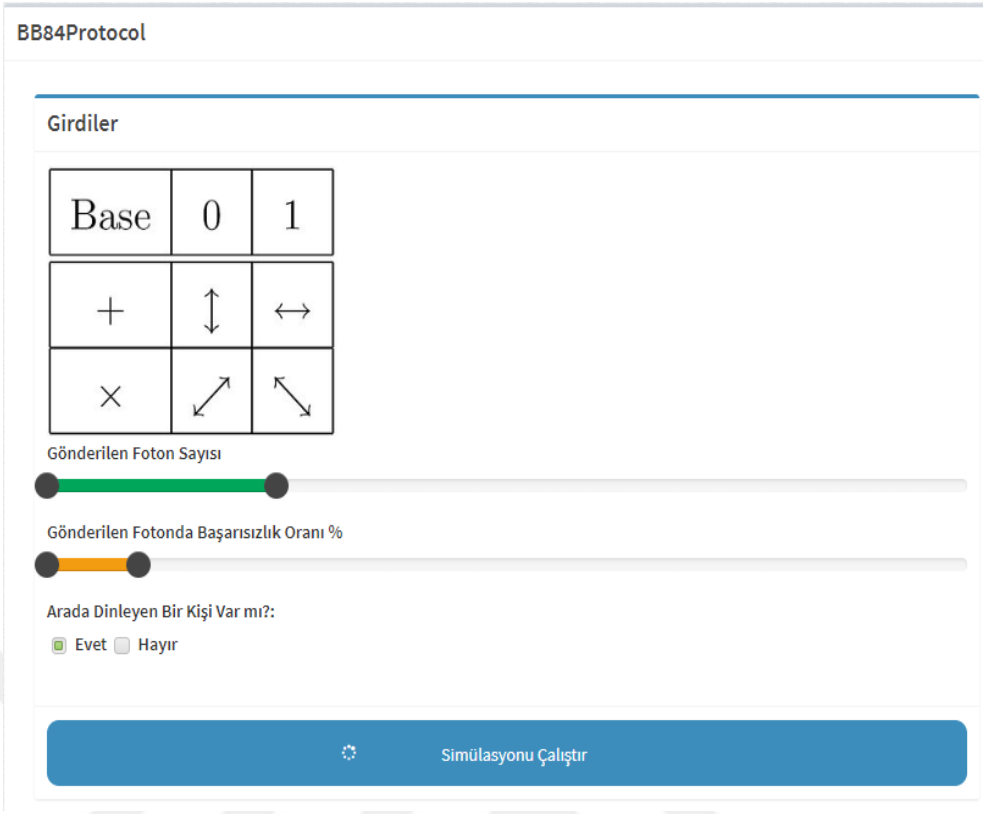
Alıcı işlem sonucunda oluşturmuş olduğu filtre dizisini Göndericiye gönderir. Şekil 3.29. ve Şekil 3.31.'de görüldüğü üzere eşleşen filtre bitleri (2, 4, 5, 6, 10, 12, 15, 16, 17, 19, 20, 22, 25, 26, 28, 31, 32, 33, 38, 42, 46, 47) yeşil renk olması gerekirken Gönderici tarafından (2, 10, 12, 17, 19, 20, 25, 32, 33, 38, 47) filtre bitleri yeşil, (4, 5, 6, 15, 16, 22, 26, 28, 31, 42, 46) filtre bitleri turuncu, (3, 8, 11, 13, 18, 21,

23, 34, 35, 43, 44, 45, 48, 49) filtre bitleri sarı olarak belirtilmiştir. Burada Yeşil renk sadece Gönderici ile Alıcı tarafından eşleşen filtre bitleri belirtir, Sarı renk sadece Gönderici ile Gizli Dinleyici tarafından eşleşen filtre bitleri belirtir, son olarak ise Turuncu renk Gönderici, Gizli Dinleyici ve Alıcı tarafından eşleşen filtre bitlerini belirtir.

Arada bir dinleyici olması sebebi ile fotonlarda polarizasyon meydana gelecektir. Oluşacak polarizasyonlar Yeşil renk olarak belirtilen alanlarda meydana gelecektir. Sebebi ise Sarı renkli alanlar Gönderici ile Alıcı arasında Filtreler eşleşmediği için anahtara dâhil edilmeyecektir, Turuncu renkli alan ise Gönderici, Gizli Dinleyici ve Alıcı tarafından aynı Filtre seçiminden dolayı polarizasyon oluşturmayacaktır.

Dikkatli bir şekilde incelendiğinde Gönderici ile Alıcı arasında (2, 17, 20, 25, 33) filtre bitlerine denk gelen Filtreler aynı olmasına rağmen Foton ve Bit değerleri farklı olduğu gözlemlenmiştir. Buradan da anlaşıldığı üzere (2, 17, 20, 25, 33) filtre bitlerinde polarizasyon meydana gelmiştir. Gönderici eşleşen bu filtre bitlerini Şekil 3.2.'de gösterilen Genel Kanal üzerinden Alıcı'ya gönderir. Gönderici ve Alıcı tarafından da bu filtre bitlerine karşılık gelen Bitler saklanır diğer Bitler diziden çıkartılarak 50 dizilik bir foton gönderme işleminden sonra 22 dizilik(bitlik) eşleşmeyen bir anahtar oluşturulur.

d. Şekil 3.32.'de gösterildiği gibi simülasyon girdi değerleri için dördüncü olarak **foton sayısı 50** belirleyip **kaybın ve dinlemenin olduğu** bir ortam varsayarak simülasyonu çalıştırdık.



Şekil 3.32. Simülasyonun Foton Sayısı 50, Kayıp ve Dinlemenin Olduğu Şekilde Çalıştırması

İşlem Gönderici

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50
Bit	0	1	0	0	1	0	0	0	0	1	1	1	0	1	1	0	1	1	1	1	1	1	1	0	1	0	1	1	1	0	1	1	1	1	1	1	0	0	1	0	0	0	0	0	1	0	1	1	1	1
Filitre	x	+	x	x	+	x	x	x	+	x	+	+	+	+	x	+	+	+	x	+	x	x	+	+	x	x	x	x	x	x	+	+	+	x	x	+	x	+	x	+	x	x	x	x	+	x	x	x	+	+
Foton	/	_	/	/	_	/	/	/	|	\	_	_	|	_	\	|	_	_	\	_	\	\	_	|	\	/	\	\	\	/	_	_	_	_	\	\	|	\	|	|	/	/	/	/	/	_	/	\	\	_

Şekil 3.33. Foton Sayısı 50, Kayıp ve Dinlemenin Olduğu Ortamda Gönderici Tarafından Oluşan Simülasyon Sonucu

Şekil 3.33.'deki tabloda görüldüğü üzere Gönderici tarafından 50 Bitlik rastgele bir dizi oluşturulup bu 50 Bite karşılık rastgele Doğrusal ya da Diyagonal filtre sistemi üretilip bunlara karşılık gelen fotonlar oluşturulmuştur.

Oluşturulan bu fotonlar Şekil 3.2.'de gösterildiği gibi Kuantum Kanal (Fiber optik) üzerinden Alıcı'ya gönderilir. Fakat Gizli Dinleyici bütün fotonları kendi alarak işlem gerçekleştirir.

İşlem Gizli Dinleyici

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50
Bit	0	1	0	0	1	1	0	0	0	0	1	1	0	1	0	1	1	0	1	1	1	1	1	1	1	0	1	0	1	0	1	1	1	1	1	1	1	0	1	0	0	0	0	1	0	1	1	1	1	0
Filitre	x	x	+	+	+	+	+	+	x	+	+	+	+	+	+	x	+	+	x	+	+	x	+	x	x	x	x	+	+	x	x	+	x	x	x	+	x	+	+	+	x	+	+	+	+	x	+	x	x	+	x
Foton	/	\	|	|	_	_	|	|	/	|	_	_	|	_	|	_	|	\	_	|	\	_	\	\	/	\	|	_	/	\	_	\	\	\	_	\	|	_	|	/	|	|	_	/	_	\	\	_	/

Şekil 3.34. Sayısı 50 Gizli Dinleyici Tarafından Oluşan Simülasyon Sonucu

Şekil 3.34.'deki tabloda Gizli Dinleyici, Gönderici tarafından gönderilen fotonları alarak her bir foton değeri için rastgele bir filtre (Doğrusal ya da Diyagonal) oluşturularak bunlara karşılık gelen bit (0 ya da 1) değeri üretilir.

Gizli Dinleyici işlem sonucunda oluşturmuş olduğu filtre dizisini Alıcı'ya gönderir. Şekil 3.33. ve Şekil 3.34.'de görüldüğü üzere eşleşen filtre bitleri (1, 5, 11, 12, 13, 14, 17, 18, 19, 20, 22, 23, 25,26, 27, 30, 32, 35, 38, 40, 41, 47, 48, 49) sarı renk olarak belirtilmiştir. Kayıp ve arada bir dinleyici olması sebebi ile fotonlarda polarizasyon meydana gelecektir.

İşlem Alıcı

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50
Filitre	+	x	x	x	x	x	+	+	x	x	+	+	x	+	x	+	+	+	x	x	x	+	x	+	x	+	+	+	x	+	x	+	x	+	x	x	x	+	x	+	+	x	+	x	x	+	+	x	+	x	+
Foton	-	\	\	\	\	\	|	|	/	\	-	_	\	-	\	_	-	|	\	/	\	|	\	|	\	/	_	|	_	/	_	/	|	\	\	\	\	_	|	/	|	\	\	|	_	\	|	\	_
Bit	1	1	1	1	1	1	0	0	0	1	1	1	1	1	1	1	1	1	0	1	0	1	0	0	1	0	1	0	1	0	1	0	0	1	1	1	1	1	1	0	0	0	1	1	0	1	1	0	1	1

Şekil 3.35. Foton Sayısı 50, Kayıp ve Dinlemenin Olduğu Ortamda Alıcı Tarafından Oluşan Simülasyon Sonucu

Şekil 3.35.'deki tabloda Alıcı, Gizli Dinleyici tarafından gönderilen fotonları Gönderici tarafından gönderilmiş gibi alarak her bir foton değeri için rastgele bir filtre (Doğrusal ya da Diyagonal) oluşturularak bunlara karşılık gelen bit (0 ya da 1) değeri üretilir.

Alıcı işlem sonucunda oluşturmuş olduğu filtre dizisini Gönderici'ye gönderir. Şekil 3.33. ve Şekil 3.35.'de görüldüğü üzere eşleşen filtre bitleri (3, 4, 6, 10, 11, 12, 14, 15, 16, 17, 18, 19, 21, 24, 25, 26, 30, 31, 33, 35, 36, 40, 41, 43, 44, 45, 47, 50) yeşil renk olması gerekirken Gönderici tarafından (3, 4, 6, 10, 15, 16, 21, 24, 31, 33, 36, 43, 44, 45, 50) filtre bitleri yeşil, (11, 12, 14, 17, 18, 19, 25, 26, 30, 35, 40, 41, 47) filtre

bitleri turuncu, (1, 5, 13, 20, 22, 23, 27, 32, 38, 48, 49) filtre bitleri sarı olarak belirtilmiştir. Burada Yeşil renk sadece Gönderici ile Alıcı tarafından eşleşen filtre bitleri belirtir, Sarı renk sadece Gönderici ile Gizli Dinleyici tarafından eşleşen filtre bitleri belirtir, son olarak ise Turuncu renk Gönderici, Gizli Dinleyici ve Alıcı tarafından eşleşen filtre bitlerini belirtir.

Arada bir dinleyici olması ve kayıp sebebi ile fotonlarda polarizasyon meydana gelecektir. Oluşacak polarizasyonlar Yeşil renk olarak belirtilen alanlarda meydana gelecektir. Sebebi ise Sarı renkli alanlar Gönderici ile Alıcı arasında Filtreler eşleşmediği için anahtara dâhil edilmeyecektir, Turuncu renkli alan ise Gönderici, Gizli Dinleyici ve Alıcı tarafından aynı Filtre seçiminden dolayı polarizasyon oluşturmayacaktır.

Dikkatli bir şekilde incelendiğinde Gönderici ile Alıcı arasında (3, 4, 6, 16, 18, 33, 43, 44, 45) filtre bitlerine denk gelen Filtreler aynı olmasına rağmen Foton ve Bit değerleri farklı olduğu gözlemlenmiştir. Buradan da anlaşıldığı üzere (3, 4, 6, 16, 18, 33, 43, 44, 45) filtre bitlerinde polarizasyon meydana gelmiştir. Gönderici eşleşen bu filtre bitlerini Şekil 3.2.'de gösterilen Genel Kanal üzerinden Alıcı'ya gönderir. Gönderici ve Alıcı tarafından da bu filtre bitlerine karşılık gelen Bitler saklanır diğer Bitler diziden çıkartılarak 50 dizilik bir foton gönderme işleminden sonra 28 dizilik(bitlik) eşleşmeyen bir anahtar oluşturulur.

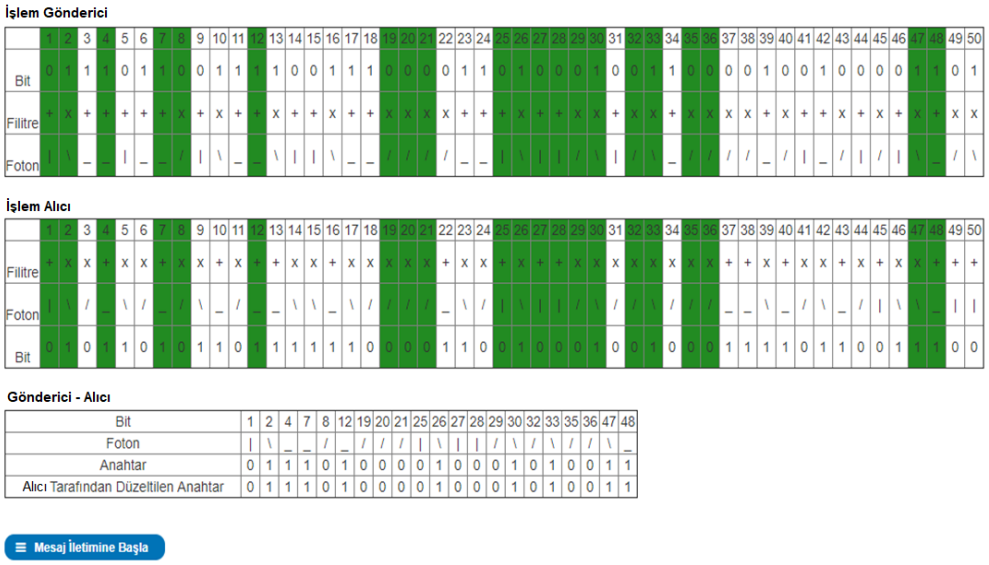
3.5.2. CASCADE protokol uygulaması

CASCADE protokolü, Gönderici ile Alıcı arasında oluşturulan ortak anahtarın dinlenme ya da kayıp sebebi ile oluşan eşleşmeme ihtimaline karşılık uygulanan Hata Sezme ve Düzeltme protokolüdür.

Girdi parametrelerine göre yapılan CASCADE işlemleri;

a. Simülasyon girdi değerleri için ilk olarak **foton sayısı 50** belirleyip **kayıp (başarısız)** ve **dinlemenin olmadığı** bir ortam varsayarak çalıştırılan

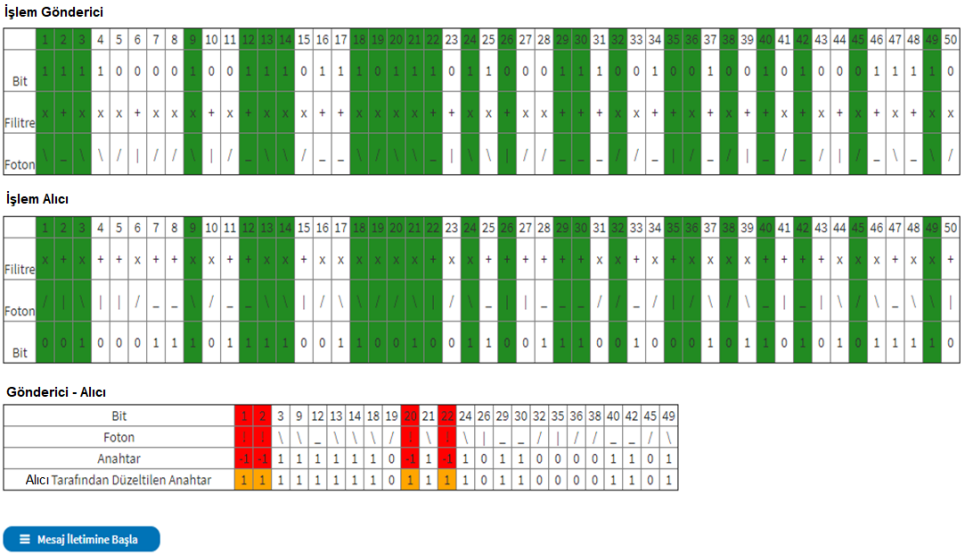
simülasyonda Gönderici tarafından Şekil 3.23. ve Alıcı tarafından Şekil 3.24.'de gösterilen tabloda üretilen ortak anahtar Şekil 3.36.'da gösterilmiştir.



Şekil 3.36. Foton Sayısı 50, Kayıp ve Dinleme Olmadan Oluşan Simülasyonda CASCADE İşlemini Uygulanması

Şekil 3.36.'da görüldüğü gibi Şekil 3.23. ve Şekil 3.24'deki tablolarda aynı filtre bitine karşılık gelen sonuçlarda bir farklılık gözlemlenmemiştir. Bundan dolayı CASCADE Hata Sezme ve Düzeltme işlemi uygulanmış ortak anahtardaki bütün Bitler aynı olmasından dolayı yani polarizasyon olmadığı için bir değişiklik uygulanmamıştır.

b. Simülasyon girdi değerleri için ikinci olarak **foton sayısı 50** belirleyip **kaybın olduğu, dinlemenin olmadığı** bir ortam varsayarak çalıştırılan simülasyonda Gönderici tarafından Şekil 3.26. ve Alıcı tarafından Şekil 3.27.'de gösterilen tabloda üretilen ortak anahtar Şekil 3.37.'de gösterilmiştir.



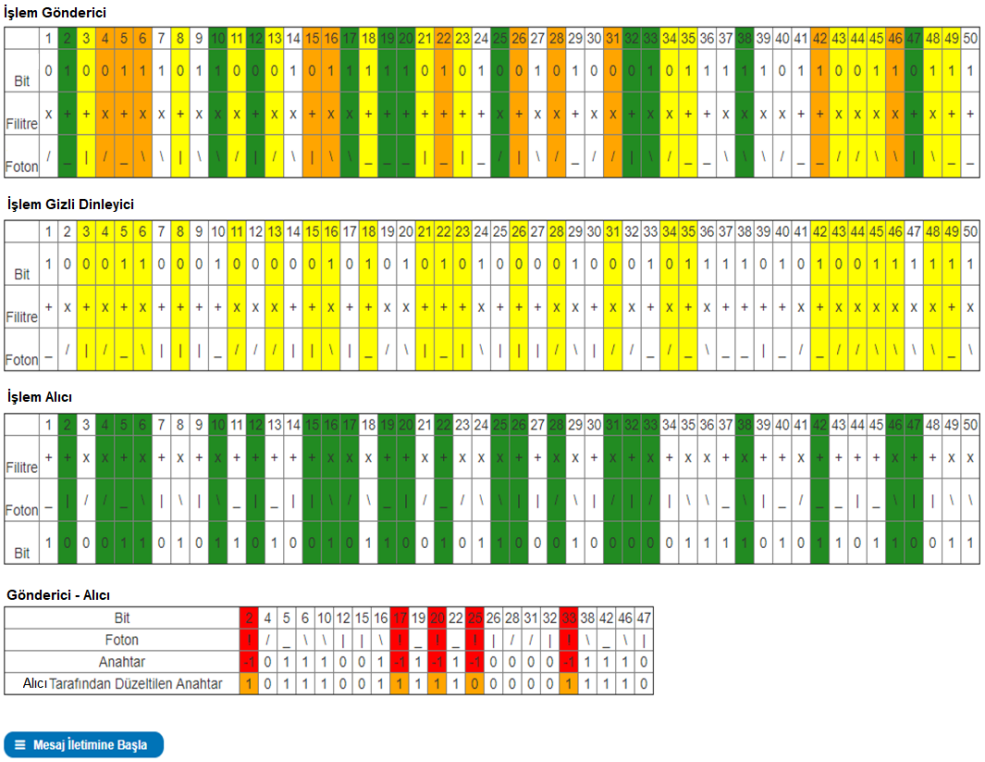
Şekil 3.37. Foton Sayısı 50, Kaybın Olup ve Dinleme Olmadan Oluşan Simülasyonda CASCADE İşlemini Uygulanması

Şekil 3.37.'de görüldüğü gibi Şekil 3.26. ve Şekil 3.27.'deki tablolarda aynı filtre bitine karşılık gelen sonuçlarda (1, 2, 20, 22) filtre bitlerinde bir farklılık gözlemlenmiştir. Bu filtre bitleri Şekil 3.37.'de da görüldüğü üzere kırmızı olarak renklendirilmiştir. Bu filtre bitlerinde eşleşme olmadığı için "**Foton**" alanı "**!**", "**Anahtar**" alanı "**-1**" olarak belirtilmiştir. Alıcı kendi oluşturmuş olduğu anahtardaki (1, 2, 20, 22) filtre bitlerin deki (0, 0, 0, 0) değerlerini CASCADE Hata Sezme ve Düzeltme işlemi uygulayarak (1, 1, 1, 1) yapıp oluşturmuş olduğu anahtarı Gönderici'deki anahtara benzeterek iletişim için aynı anahtarı elde etmiş olur. Şekil 3.18.'de de gösterildiği gibi CASCADE Hata Sezme ve Düzeltme Protokolünde belirtilen hatalı bit sayısı %27.6 dan büyük ve eşit olması durumunda iletişimin başlamaması gerekmektedir. Böyle bir durumda bütün işlemler baştan başlatılması gerekmektedir. Bizim bu simülasyonda oluşturulan ortak anahtar boyutu 24 ve oluşan polarizasyon sayısı 4 olduğu için;

(100*4) / 24 = 16.66

16.66 < 27.6 olduğundan dolayı iletişim başlatılır.

c. Simülasyon girdi değerleri için üçüncü olarak **foton sayısı 50** belirleyip **kaybın olmadığı, dinlemenin olduğu** bir ortam varsayarak çalıştırılan simülasyonda Gönderici tarafından Şekil 3.29. ve Alıcı tarafından Şekil 3.31.'de gösterilen tabloda üretilen ortak anahtar Şekil 3.38.'de gösterilmiştir.



Şekil 3.38. Foton Sayısı 50, Kaybın Olmayıp ve Dinlemenin Olup Oluşan Simülasyonda CASCADE İşlemini Uygulanması

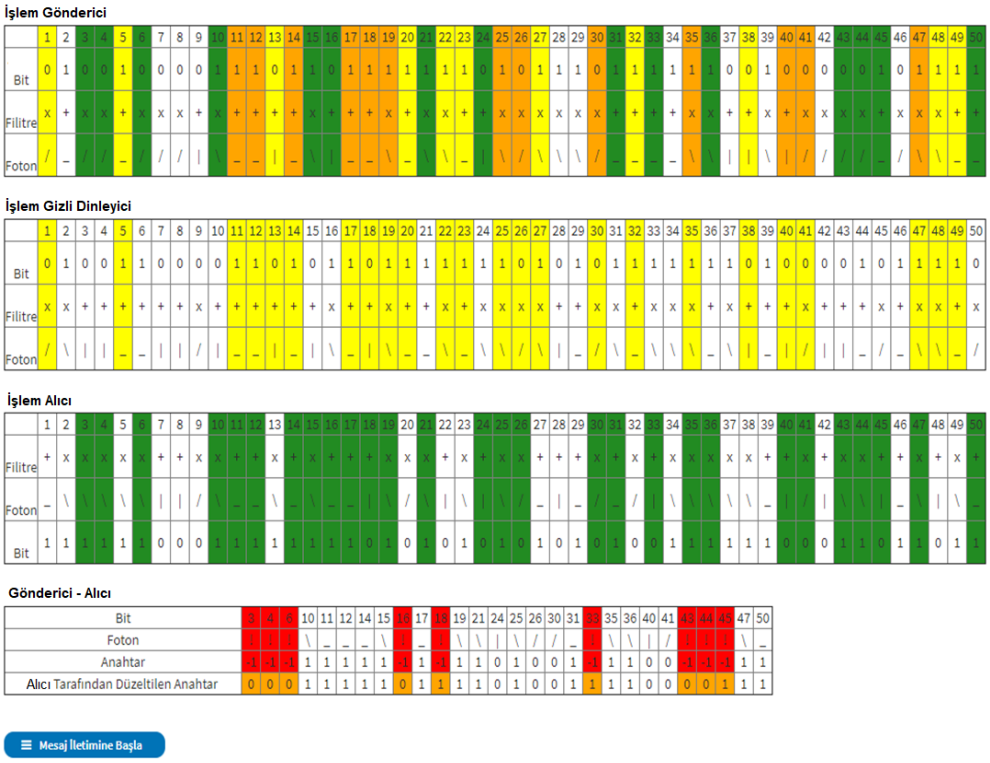
Şekil 3.38.'de görüldüğü gibi Şekil 3.29. ve Şekil 3.31.'deki tablolarda aynı filtre bitine karşılık gelen sonuçlarda (2, 17, 20, 25, 33) filtre bitlerinde bir farklılık gözlemlenmiştir. Bu filtre bitleri Şekil 3.38.'de de görüldüğü üzere kırmızı olarak renklendirilmiştir. Bu filtre bitlerinde eşleşme olmadığı için "**Foton**" alanı "**!**", "**Anahtar**" alanı "**-1**" olarak belirtilmiştir. Alıcı kendi oluşturmuş olduğu anahtardaki (2, 17, 20, 25, 33) filtre bitlerin deki (0, 0, 0, 1, 0) değerlerini CASCADE Hata Sezme ve Düzeltme işlemi uygulayarak (1, 1, 1, 0, 1) yapıp oluşturmuş olduğu anahtarı Gönderici'deki anahtara benzeterek iletişim için aynı anahtarı elde etmiş olur. Şekil 3.18.'de de gösterildiği gibi CASCADE Hata Sezme ve Düzeltme Protokolünde belirtilen hatalı bit sayısı %27.6 dan büyük ve eşit olması durumunda iletişimin

başlamaması gerekmektedir. Böyle bir durumda bütün işlemler baştan başlatılması gerekmektedir. Bizim bu simülasyonda oluşturulan ortak anahtar boyutu 22 ve oluşan polarizasyon sayısı 5 olduğu için;

(100*5) / 22 = 22.72

22.72 < 27.6 olduğundan dolayı iletişim başlatılır.

d. Simülasyon girdi değerleri için üçüncü olarak **foton sayısı 50** belirleyip **kaybın ve dinlemenin olduğu** bir ortam varsayarak çalıştırılan simülasyonda Gönderici tarafından Şekil 3.31. ve Alıcı tarafından Şekil 3.35.'de gösterilen tabloda üretilen ortak anahtar Şekil 3.39.'da gösterilmiştir.



Şekil 3.39. Foton Sayısı 50, Kayıp ve Dinleme Olup Oluşan Simülasyonda CASCADE İşlemini Uygulanması

Şekil 3.39.'da görüldüğü gibi Şekil 3.33. ve Şekil 3.35.'deki tablolarda aynı filtre bitine karşılık gelen sonuçlarda (3, 4, 6, 16, 18, 33, 43, 44, 45) filtre bitlerinde

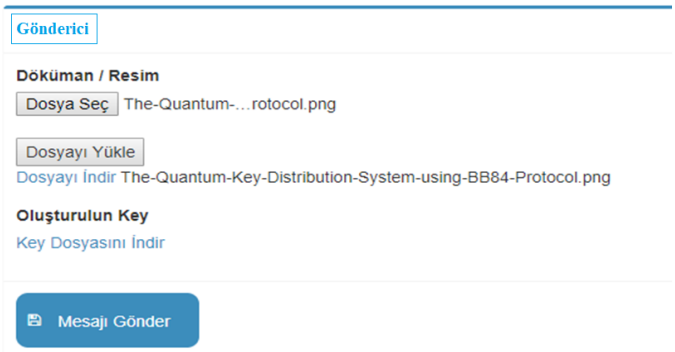
bir farklılık gözlemlenmiştir. Bu filtre bitleri Şekil 3.39.'da de görüldüğü üzere kırmızı olarak renklendirilmiştir. Bu filtre bitlerinde eşleşme olmadığı için "**Foton**" alanı "**!**", "**Anahtar**" alanı "**-1**" olarak belirtilmiştir. Alıcı kendi oluşturmuş olduğu anahtardaki (3, 4, 6, 16, 18, 33, 43, 44, 45) filtre bitlerin deki (1, 1, 1, 1, 0, 0, 1, 1, 0) değerlerini CASCADE Hata Sezme ve Düzeltme işlemi uygulayarak (0, 0, 0, 0, 1, 1, 0, 0, 1) yapıp oluşturmuş olduğu anahtarı Gönderici'deki anahtara benzeterek iletişim için aynı anahtarı elde etmiş olur. Şekil 3.18.'de de gösterildiği gibi CASCADE Hata Sezme ve Düzeltme Protokolünde belirtilen hatalı bit sayısı %27.6 dan büyük ve eşit olması durumunda iletişimin başlamaması gerekmektedir. Böyle bir durumda bütün işlemler baştan başlatılması gerekmektedir. Bizim bu simülasyonda oluşturulan ortak anahtar boyutu 28 ve oluşan polarizasyon sayısı 9 olduğu için;

(100*9) / 28 = 32.14

32.14 > 27.6 olduğundan dolayı iletişim başlatılmaz.

3.5.3. Vernam şifreleme uygulaması

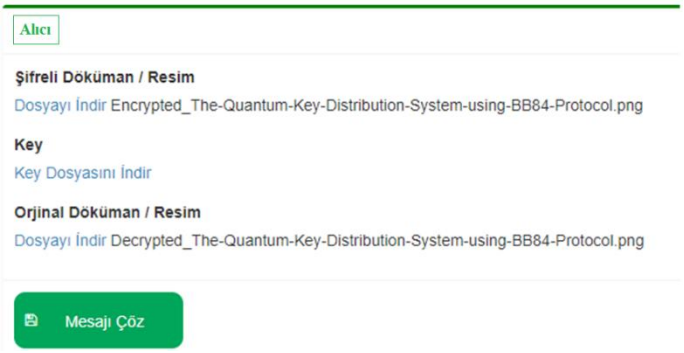
BB84 protokolü kullanılarak oluşturulan anahtarı Vernam şifreleme tekniği kullanarak güvenilir bir şekilde mesaj iletişimi gerçekleştirile bilinir.



Şekil 3.40. Gönderici Vernam Şifreleme Uygulaması

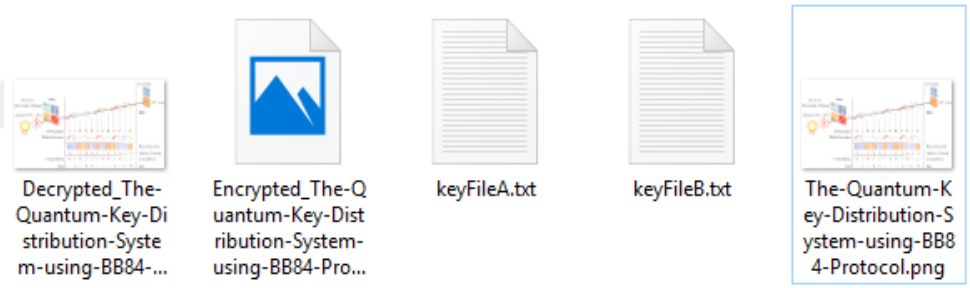
Şekil 3.40.'da gösterildiği gibi şifreleme işlemi Gönderici tarafından oluşturulan ortak anahtara ile yapılmaktadır. Gönderici iletmek istediği mesajı oluşturmuş olduğu anahtar ile XOR işlemine tabi tutarak şifrelenmiş dosya elde eder.

Elde etmiş olduğu bu dosyayı Şekil 3.2.'de gösterilen Genel Kanal üzerinden Alıcı'ya gönderir.



Şekil 3.41. Alıcı Vernam Şifre Çözme Uygulaması

Şekil 3.41.'de görüldüğü gibi Gönderici tarafından şifrelenip gönderilen mesaj Alıcı tarafından barındırılan anahtar ile çözülerek orijinal dosya elde edilmiş olur.



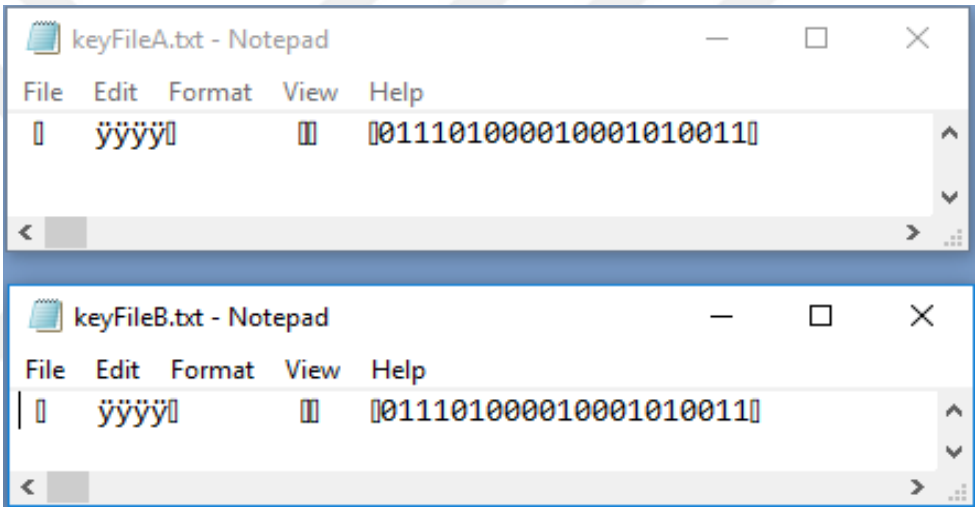
Şekil 3.42. Vernam Uygulaması ile Oluşturulan Dosyalar

Şekil 3.42.'de belirtildiği üzere;

- Orijinal mesaj "**The-Quantum-Key-Distribution-System-using-BB84-Protocol.png**"
- Şifrelenmiş mesaj "**Encrypted_The-Quantum-Key-Distribution-System-using-BB84-Protocol.png**"
- Deşifre edilmiş mesaj "**Decrypted_The-Quantum-Key-Distribution-System-using-BB84-Protocol.png**"
- Gönderici'nin oluşturmuş olduğu anahtar "**keyFileA.txt**"
- Alıcı'nın oluşturmuş olduğu anahtar "**keyFileB.txt**"

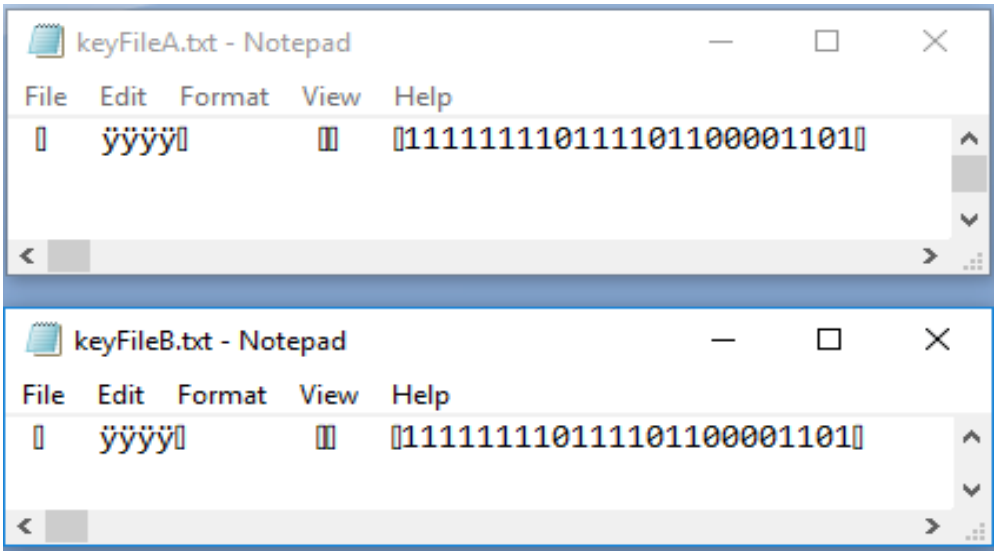
Dikkatli bir şekilde incelendiğinde Şekil 3.42.'de Orijinal mesaj ile Şifresi Çözülmüş mesaj açık bir şekilde görülmektedir. Şifrelenmiş mesaj ise ne olduğu anlaşılmayacak şekilde görülmektedir.

- Simülasyon girdi değerleri için ilk olarak **foton sayısı 50** belirleyip **kayıp (başarısız)** ve **dinlemenin olmadığı** bir ortam varsayarak çalıştırılan simülasyonda üretilen ortak anahtar Gönderici tarafından "**keyFileA.txt**" dosyasında, Alıcı tarafından "**keyFileB.txt**" dosyasında saklanmaktadır. Şekil 3.43.'de gösterilen bu iki dosyanın içeriğinin Şekil 3.36.'da gösterilen değerlerle aynı olduğu görülmektedir.



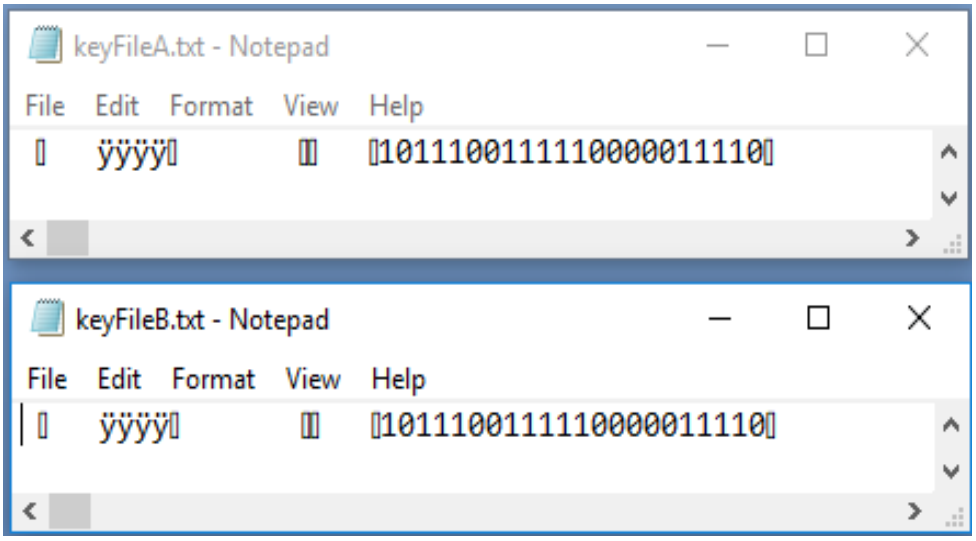
Şekil 3.43. Foton Sayısı 50, Kayıp ve Dinleme Olmadan Simülasyonda Gönderici ve Alıcı Tarafından Üretilen Anahtar Dosyaları

- Simülasyon girdi değerleri için ikinci olarak **foton sayısı 50** belirleyip **kaybın olduğu, dinlemenin olmadığı** bir ortam varsayarak çalıştırılan simülasyonda üretilen ortak anahtar Gönderici tarafından "**keyFileA.txt**" dosyasında, Alıcı tarafından "**keyFileB.txt**" dosyasında saklanmaktadır. Şekil 3.44.'de gösterilen bu iki dosyanın içeriğinin Şekil 3.37.'de gösterilen değerlerle aynı olduğu görülmektedir.



Şekil 3.44. Foton Sayısı 50, Kaybın Olup ve Dinleme Olmadan Simülasyonda Gönderici ve Alıcı Tarafından Üretilen Anahtar Dosyaları

- Simülasyon girdi değerleri için üçüncü olarak **foton sayısı 50** belirleyip **kaybın olmadığı, dinlemenin olduğu** bir ortam varsayarak çalıştırılan simülasyonda üretilen ortak anahtar Gönderici tarafından "**keyFileA.txt**" dosyasında, Alıcı tarafından "**keyFileB.txt**" dosyasında saklanmaktadır. Şekil 3.45.'de gösterilen bu iki dosyanın içeriğinin Şekil 3.38.'de gösterilen değerlerle aynı olduğu görülmektedir.



Şekil 3.45. Foton Sayısı 50, Kaybın Olmayıp ve Dinlemenin Olduğu Simülasyonda Gönderici ve Alıcı Tarafından Üretilen Anahtar Dosyaları

- Simülasyon girdi değerleri için üçüncü olarak **foton sayısı 50** belirleyip **kaybın ve dinlemenin olduğu** bir ortam varsayarak çalıştırılan simülasyonda Şekil 3.39.'da görüldüğü üzere CASCADE Hata Sezme ve Düzeltme Protokolünde belirtilen hatalı bit sayısı %27.6 dan büyük olmasından dolayı iletişim ortamı sağlanmamış bundan dolayı Gönderici tarafından "**keyFileA.txt**" dosyası ve Alıcı tarafından "**keyFileB.txt**" dosyası oluşturulmamıştır.

4. SONUÇLAR ve ÖNERİLER

4.1. Sonuçlar

Oluşturulan benzetim sistemi ile iletişim kanallarında anahtar üretimi ve paylaşımı sırasında Gizli Dinleyici olarak araya girme işleminin belirlenmesi sağlanmıştır.

Bu önerilen yöntem ile kampüs içerisinde farklı network sistemine sahip olan Harran Üniversitesi Araştırma ve Uygulama Hastanesi ile Harran Üniversitesi Ana Kampüsü arasında güvenli iletişim sağlayacak bir yöntem oluşturulmuştur. Bu yöntemin gerekli fiziksel cihazların teminleri yapılarak uygulanabilirliği görülmüştür.

Benzer olarak aralarında fiber optik bağlantı bulunan lokasyon ya da kurumlar için BB84 Protokolü kullanılarak kuantum şifreleme yöntemi ile güvenli iletişim yapıla bileceği görülmüştür.

Kuantum alanındaki çalışmalar olarak nitelendirilen kuantum bilgisayarlar, kuantum algoritmalar, kuantum anahtar dağıtımı ve kuantum şifreleme vb. çalışmalar devam etmektedir. Kuantum şifreleme ve anahtar dağıtımın amacı iletişim hattının güvenliliğini sağlamak iken, kuantum algoritmalarının amacı temelini matematiksel zorluklara dayandırarak günümüzün güvenilir kabul edilen sistemleri kırmasına olanak tanımasıdır.

Kuantum kriptografinin yüksek güvenlik seviyesi sağlayan verimli ve kullanıcı dostu sistemler sunmaya hazır olduğu açıktır. Klasik yöntemler hala kısa süreli güvenlik ihtiyacı olan şifrelemeler için güvenli olmakla birlikte, daha uzun süreli beklentiler ile bakıldığında kuantum kriptografinin daha değerli olduğu söylenebilir. Kuantum bilgisayarların geliştirilmesindeki ilerleme bilgi teknolojileri pazarında kuantum anahtar dağıtımı gereksinimini hızlandıracak belirgin bir rol oynayabilir. Kuantum anahtar dağıtımı ayrıca mevcut altyapı ile de gayet iyi birleştirilebilir. Çok düşük bit oranlı (saniyede yüzlerce bit) kuantum anahtar dağıtımı bile çağdaş kripto

sistemleri belirgin bir şekilde geliştirebilir. Örneğin AES gibi simetrik şifreler için gizli anahtarların saniyede birkaç kez değiştirilmesini sağlar (Şenay, 2012).

Yapılan bu çalışmayla fiziksel kurulumu ciddi maliyet içeren kuantum ortamı çevrimiçi bir sistemde gerçeklenip test ve eğitim ortamı tasarlanmasına imkân sağlayan bir simülasyon ortamı sunulmuştur. Bu yol ile gerçek bir sistemin çalışma mantığı görselleştirilip sunulmuştur. Buna ek olarak yeni tasarlanan algoritmalar ile değişik dinleme senaryolarında sistemin vermiş olduğu etkiler izleme imkânı sağlanmıştır. Bu çalışmanın sonraki aşamalarında yapılacak olan hata tespit ve düzeltme algoritmalarının performansa etkisi için hibrid modellerin tasarlanması incelenecektir.

Kuantum hesaplama simülasyonu son zamanlarda sıcak bir araştırma konusu olmuştur. Öte yandan, bazı ayrık problemlerde fiziksel bir sistemi uygulamak zor, pahalı ve zaman alıcıdır. Bu nedenle, bu durumlarda simülasyon, bu boşluğu doldurmak için iyi bir yaklaşım haline gelir. Sistemi simülasyon yoluyla matematiksel ve fiziksel olarak tanımlayabiliriz. Gelişmekte olan trendden başka bir şey değil, simülasyon kuantum hesaplamayı incelemek ve yeni kuantum algoritmasını yenilemek için güçlü bir araç olacaktır.

4.2. Öneriler

Hali hazırda kullanılan algoritmalardan Shor ya da Grover gibi günümüzde birçok şifreleme algoritmasını güvenli olarak sayılmasına olanak tanıyan matematik zorlukları yok edebilme imkânı sağlayan kuantum algoritmaları mevcuttur. Bu algoritmaların uygulanabilirliği için büyük ölçekte yeterli sayıda kubit değerine sahip kuantum bilgisayarların içerdiği fiziksel varlık gerekmektedir.

Kriptograflar, güvenli bir şekilde anahtar dağıtım işlemini gerçekleştirme imkânı sağlayarak kuantum alanında öne geçmiş olsalar bile, teknolojinin gelişmesi ile paralel şekilde ilerleyen kuantum bilgisayarların mevcudiyeti ile birlikte, kuantum algoritmalarının uygulanma şansı bulma imkânı olan kriptanalistler zamanla oluşan

aradaki bu farkı kapatacak, binlerce yıl aynı yöntem ile süregelen bu mücadele kuantumun içermiş olduğu alanlar içinde devam edeceği kaçınılmazdır.

KAYNAKLAR

AKLEYLEK, S., YILDIRIM, M.H., & TOK, Z.Y., 2011. Kriptoloji ve Uygulama Alanları:Açık Anahtar Altyapısı ve Kayıtlı Elektronik Posta, Akademik Bilişim Konferansı , Malatya.

ANONİM, 2015a. Wikipedia, https://tr.wikipedia.org/wiki/Mısır_hiyeroglifleri.

ANONİM, 2015b. Kriptoloji Nedir, http://www.bilgiustam.com/kriptoloji-nedir/

ANONİM, 2015c. Kuantum Kriptografi, https://tr.0wikipedia.org/wiki/Kuantum_kriptografi.

ANONİM, 2018. I. Kriptografiye Giriş, https://akademikguvenlik.files.wordpress.com/2008/07/11_kriptografi_uygulamalari.pdf.

BAHADIR, E., & ÖZDEMİR, A.Ş., 2012. Yer değiştirme şifrelemesi etkinliğinin uygulanabilirliğinin incelenmesi ve öğrencilerin etkinlikle ilgili görüşleri. KALEM Uluslararası Eğitim ve İnsan Bilimleri Dergisi, 2(2): 51-90.

BODUR, H., 2016. Java Diliyle Kriptoloji Uygulamaları.

CALVER, T.I., 2011. An empirical analysis of the cascade secret key reconciliation protocol for quantum key distribution (No. AFIT/GIR/ENV/11-S01). Aır Force Inst Of Tech Wrıght-Patterson Afb Oh School Of Engıneerıng And Management.

CANBEK, G., & SAĞIROĞLU, Ş., 2006. Bilgi ve Bilgisayar Güvenliği Casus Yazılımlar ve Korunma Yöntemleri. Grafiker Yayınları, Ankara, 16-22,33,198-204.

ÇEŞMECİ, M.Ü., 2009. Kriptoloji Tarihi. UEKAE Dergisi, 1(1): 20-31.

ÇİMEN, C., AKLEYLEK, S., & AKYILDIZ, E., 2007. Şifrelerin Matematiği : Kriptografi. ODTÜ.

ÇİMEN, C., AKLEYLEK, S., & AKYILDIZ, E., 2008. Şifrelerin Matematiği Kriptografi 6.Basım. ODTÜ. Yayıncılık, Ankara, 1: 5-66.

GİGOV, N., 2013. Quantum Key Distribution Data Post-Processing with Limited Resources: Towards Satellite-Based Quantum Communication (Master's thesis, University of Waterloo).

GÜMÜŞ, E., 2011. Kuantum Kriptografi ve Anahtar Dağıtım Protokolleri. Akademik Bilişim.

HOSSEİNİ-KHAYAT, S., & MARVİAN, I., 2005. Secure Communication Using Qubits. arXiv preprint quant-ph/0503157.

İNCETAŞ, O., & SAĞIROĞLU, Ş., 2015. Kuantum Kriptografide Gönderilen Foton Sayısının, Gürültüsüz Ortamda Elde Edilen Anahtar Uzunluklarına Etkisi. SDÜ Mühendislik Bilimleri ve Tasarım Dergisi, 3.1: 29-42.

JOHNSON, J.S., 2012. An analysis of error reconciliation protocols for use in quantum key distribution (No. AFIT/GCE/ENG/12-06). Aır Force Inst Of Tech Wrıght- Patterson Afb Oh Graduate School Of Engıneerıng And Management.

KARA, O., 2009. 2. Dünya Savaşı'ndan Günümüze Kriptoloji: Enigma'danAES'e Şifreleme. Bilim ve Teknik Dergisi, (500): 28-33.

KAŞKALOĞLU, K., 2016. Geçmişten Günümüze Kriptoloji: Şifrelerin Bilimi.

KODAZ, H., & BOTSALI, F., 2010. Simetrik ve asimetrik şifrleme algoritmalarının karşılaştırılması. Selçuk Üniversitesi Teknik Online Dergisi, Cilt: 9 sayı: 1, Konya.

MARTİNEZ-MATEO, J., ELKOUSS, D., & MARTİN, V., 2013. Key reconciliation for high performance quantum key distribution. Scientific reports, 3: 1576.

ÖZDAĞ, Ü., 2009. İstihbarat Teorisi, 126s.

ÖZDEMİR, S., 2008. Kablosuz Algılayıcı Ağlarında Homomorfik Şifreleme İle Güvenli Veri Kümeleme. Gazi Üniversitesi Mühendislik-Mimarlık Fakültesi Dergisi, 23.2.

SAĞIROĞLU, Ş., & ALKAN, M., 2005. Bilgi Güvenliği Bilimi(Kriptoloji). Her Yönüyle Elektronik İmza, Grafiker Yayınları, Ankara, 21-50.

SASAKİ, M., FUJİWARA, M., ISHİZUKA, H., KLAUS, W., WAKUİ, K., TAKEOKA, M., & YOSHİNO, K., 2011. Field test of quantum key distribution in the Tokyo QKD Network. Optics express, 19(11): 10387-10409.

SİNGH, H., GUPTA, D., & SİNGH, A., 2014. Quantum key distribution protocols: a review. IOSR Journal of Computer Engineering (IOSR-JCE), 16.

ŞAHİN, A. B., & SELÇUK, G., 2006. İletişim Ağ Güvenliğinde Son Aşama: Kuantum Kriptografi ve Fiber Optik Ortamda Kuantum Temelli Rastsal Sayı Üretimi. Ulusal Elektronik-İmza Sempozyumu, Ankara, 57.

ŞENAY, V., 2012. Quantum Cryptography. MASTER OF SCIECE THESIS Department of Physics.

TOYRAN, M., 2003. Kuantum Kriptografi. İstanbul Üniversitesi, Fen Bilimleri Enstitüsü, Yüksek Lisans Tezi, İstanbul, 176.

TOYRAN, M., 2006. Optik Ağlarda Kuantum Kriptografi Kullanarak Güvenli İletişim.

TOYRAN, M., PEDERSEN, T. B., HASEKİOĞLU, A. A., CAN, M. A., & BERBER, S., 2011. Bilgi Güvenliğinde Kuantum Teknikler. Bildiriler Kitabı, 98.

TOYRAN, M., PEDERSEN, T. B., HASEKİOĞLU, A. A., CAN, M. A., & BERBER, S., 2012. Comparison of CASCADE error correction protocol and LDPC error correction codes. In Signal Processing and Communications Applications Conference (SIU), 2012 20th (pp. 1-4). IEEE.

YERLİKAYA, T., BULUŞ E., & ARDA D., 2005. Asimetrik Kripto Sistemler ve Uygulamaları. 2. Mühendislik Bilimleri Genç Araştırmacılar Kongresi MBGAK2005, İstanbul.

ZHANG, X., WEN, Q., & ZHU, F., 2007. Object-oriented quantum cryptography simulation model. In Natural Computation, 2007. ICNC 2007. Third International Conference on (Vol. 4, pp. 599-602). IEEE.

ZHAO, F., FU, M., WANG, F., LU, Y., LİAO, C., & LİU, S., 2007. Error reconciliation for practical quantum cryptography. Optik-International Journal for Light and Electron Optics, 118(10): 502-506.

ÖZGEÇMİŞ

KİŞİSEL BİLGİLER

Adı Soyadı : İdris TÜRKER
Uyruğu : T.C.
Doğum Yeri : Şanlıurfa – Haliliye
E-mail : iturker@harran.edu.tr

EĞİTİM

Derece	**Adı – İlçe İl**	**Bitirme Yılı**
Lise	Davut Zeki Akpınar – Şanlıurfa	2010
Üniversite	Harran Üniversitesi – Şanlıurfa	2014
Yüksek Lisans	Harran Üniversitesi – Şanlıurfa	2018

İŞ TECRÜBESİ

Dönem	**Ünvan**	**Adı**
2014 – 2015	Yazılım Geliştiricisi	Sentim BilişimHarran
2016 – 2018	Yazılım Geliştirme Uzmanı	Harran Üniversitesi Bilgi İşlem Daire Başkanlığı