**KUANTUM ANAHTAR DAĞITIM PROTOKOLLERİNİN SİMÜLE EDİLEREK KARŞILAŞTIRILMASI: BB84 ve B92**

Ercan ÇAĞLAR1, 0000-0002-6840-1519, ercaglar@comu.edu.tr
İhsan YILMAZ2, 0000-0001-7684-9690, iyilmaz@comu.edu.tr

Engin ŞAHİN2, 0000-0002-8040-0519, enginsahin@comu.edu.tr

1Çanakkale Onsekiz Mart Üniversitesi, Eğitim Fakültesi, Bilgisayar ve Öğretim Teknolojileri Eğitimi Bölümü 2Çanakkale Onsekiz Mart Üniversitesi, Mühendislik Fakültesi, Bilgisayar Mühendisliği

**Özet**

Günümüzde iletişim dijital olarak gerçekleştirilmektedir. İki kullanıcının paylaştığı sayısal verinin güvenliği, şifreleme kullanılarak sağlanmaktadır. Şifreleme işlemi anahtar ile yapılmaktadır. Anahtar, iki kullanıcı arasında güvenli bir şekilde paylaşılmalıdır. Klasik yöntemlerin kullanıldığı anahtar dağıtım yöntemleri, çözülmesi güç matematiksel problemlere dayanmaktadır. Shor algoritması, büyük sayıların asal çarpanlarının kuantum bilgisayarlar ile hesaplanabileceğini göstermiştir. Kuantum mekaniği ilkelerine dayalı hesaplama fikri, 1982 yılında Feynman tarafından ortaya atıldı. Araştırmacılar, kuantum mekaniği ilkelerini kullanan bilişim teknolojileri üzerinde çalışmaya başlamışlardır. İlk olarak Bennett ve Brassard tarafından BB84 kuantum anahtar dağıtım protokolü önerilmiştir. Sonrasında Bennett tarafından BB84 protokolüne alternatif olarak B92 protokolü önerilmiştir. Bu çalışmada ilk olarak her iki protokol tanıtılmakta, sonrasında her iki protokolün teorik olarak karşılaştırılması sunulmaktadır. Son olarak ise her iki protokolün simülasyonu ve analizleri, IBM Qiskit kütüphanesi kullanılarak gerçekleştirilmiş ve tartışılmıştır.

 **Anahtar Kelimeler:** Kuantum Anahtar Dağıtımı, Kuantum Kriptografi, Bilgi Güvenliği

**Simulate Comparison of Quantum Key Distribution Protocols: BB84 and B92**

**Abstract**

Nowadays, communication is carried out digitally. The security of the digital data shared by two users is provided by using encryption. The encryption is done by using the key. The key must be shared securely between two users. Key distribution methods using classical methods are based on difficult mathematical problems. Shor's algorithm has shown that prime factors of large numbers can be calculated with quantum computers. The idea of computation based on the principles of quantum mechanics was proposed by Feynman in 1982. Researchers have started to work on information technologies that use the principles of quantum mechanics. Firstly, the BB84 quantum key distribution protocol was proposed by Bennett and Brassard. Afterwards, the B92 quantum key distribution protocol was proposed as an alternative to the BB84 protocol by Bennett. In this study, firstly, both protocols are introduced, and then the theoretical comparison of both protocols is presented. Finally, simulation and analysis of both protocols using IBM Qiskit library were performed and discussed.

 **Keywords:** Quantum Key Distribution, Quantum Cryptography, Information Security

# Giriş

Bilginin gizli bir şekilde iletilmesi üzerine yapılan çalışmalar kriptografi olarak adlandırılır. Gönderilecek mesajı şifrelemek ve alınan şifreli mesajın şifresini çözmek için anahtar kullanılmaktadır. İletişimi dinleyen üçüncü bir taraf olma ihtimaline karşı her gönderimde farklı bir anahtar kullanılması gerekmektedir. Bu durum, anahtar dağıtımı problemini ortaya çıkarmaktadır. Kriptografi; bilginin geçerliliği yitirilene kadar, bilginin ele geçirilmesini engellemeyi hedeflemektedir. Büyük sayıların asal çarpanlarına ayrılmasının zorluğuna dayanan RSA (Rivest vd.,1978) algoritması ile şifrelenen bir veri, şifrelemenin bit cinsinden türüne göre klasik bilgisayarlar ile anlamlı bir süre içerisinde çözülememektedir. RSA algoritması, tek kullanımlık anahtarların dağıtımında da kullanılabilmektedir. Shor (1994) tarafından kuantum mekaniği ilkeleri kullanılarak geliştirilen algoritma ile büyük sayıların asal çarpanlarına çok kısa zamanda ayrılabildiği gösterilmiştir. Shor algoritması, kuantum teknolojileri kullanılarak güvenlik yöntemleri geliştirmenin klasik yöntemlere göre güvenlik ve hız sağladığını ortaya koymuştur.

Feynman (1982), bilişim teknolojilerinde kuantum mekaniği ilkelerinin kullanılması fikrini ortaya atmıştır. Bennett ve Brassard (1984), ilk kuantum anahtar dağıtımı protokolü olan BB84 protokolünü geliştirmiştir. BB84 protokolüne alternatif olarak geliştirilen B92 protokolü, Bennet (1992) tarafından önerilmiştir. Çalışmamızın ilk bölümünde, BB84 ve B92 protokolleri sunulduktan sonra protokoller teorik olarak karşılaştırılmaktadır. İkinci bölümünde ise protokollerin, IBM Qiskit üzerinde yerel olarak simülasyonları gerçekleştirdikten sonra simülasyon sonuçları doğrultusunda karşılaştırılmaktadır. Çalışmamızda, iletişimi başlatan gönderici taraf “Alice”, alıcı taraf “Bob” ve araya girip iletişimin dinleyen üçüncü taraf ise “Eve” olarak ifade edilmektedir.

# BB84 ve B92 Protokolleri ve Karşılaştırılması

## BB84 Protokolü

BB84 protokolü, 1984 yılında Bennett ve Brassad tarafından önerilmiştir. Protokolde, 00, 450, 900 ve 1350 olmak üzere dört farklı polarizasyon durumu kullanılmaktadır. Fotonu polarize edebilmek için Doğrusal (Rectilinear) ve Köşegensel (Diagonal) tabanlar kullanılmaktadır. 00 ve 450 olarak polarize olmuş fotonların bit olarak değeri “0”, 900 ve 1350 olarak polarize olmuş fotonların bit olarak değeri “1” olarak kabul edilir. BB84 protokolünün adımları aşağıdaki gibidir (Bennett ve Brassard, 1984):

Adım 1: Alice, rastgele bir bit dizisi ve rastgele bir polarizasyon taban dizisi seçer.

Adım 2: Seçmiş olduğu polarizasyon taban dizisini kullanarak, bit dizisine uygun bir şekilde fotonları polarize ederek Bob’a gönderir.

Adım 3: Bob, rastgele seçmiş olduğu polarizasyon tabanlarına göre almış olduğu fotonlarda kuantum ölçüm gerçekleştirir. Bob, ölçüm sonuçlarını kendine ait bit dizisi olarak saklar.

Adım 4: Bob, seçmiş olduğu polarizasyon tabanlarını açık bir kanal vasıtasıyla paylaşır. Ölçüm sonuçlarını duyurmaz.

Adım 5: Alice, Bob’un kendisi ile aynı seçtiği tabanları yani doğru seçilen tabanları duyurur. Farklı olan tabanlardaki ölçüm sonuçları göz ardı edilerek, aynı olarak işaretlenen ölçüm sonuçları anahtar bitleri olarak ele alınır ve yola bu bit dizisi ile devam edilir.

Adım 6: Bob, anahtar bitlerinin bir kısmını duyurur. Bunun amacı Eve’nin varlığını tespit etmektir.

Adım 7: Alice, Bob’un duyurduğu bitleri kendi bitleri ile kıyaslar. Bitler aynı değere sahip ise iletişimin güvenli olduğunu onaylar. Duyurulan bitler atılarak kalan bitlerden anahtar oluşturulur. Eğer bitler farklı değere sahip ise Eve’nin varlığı tespit edilmiş olur ve anahtarın geçersiz olduğu duyurulur.

 

Şekil 1. Eve var olmadığı durumda BB84 protokolünün çalışması

Şekil 1’de iletişimi dinleyen üçüncü bir tarafın olmadığı durumda BB84 protokolünün nasıl çalıştığı görülmektedir. Örneğin 3. biti ele alalım. Alice, doğrusal tabanı seçmiştir ve “0” değerini göndermektedir. Alice, 00 şeklinde polarize ettiği fotonu Bob’a gönderir. Bob, Alice ile aynı tabanı seçip ölçüm yaptığı için %100 ihtimalle “0” sonucunu bulur. İki tarafta aynı tabanı kullandığı için 3. Bit anahtar biti olarak kabul edilecektir. 4. biti inceleyecek olursak Alice, doğrusal tabanı seçmiştir ve “0” değerini göndermektedir. Alice, 00 şeklinde polarize ettiği fotonu Bob’a gönderir. Bob, Alice ile farklı tabanı seçtiği için ölçüm sonucu %50 ihtimalle “0”, %50 ihtimalle “1” olacaktır. Örneğimizde “1” sonucunu elde etmiştir. Farklı taban seçildiği için Bob’un ölçüm sonucundan bağımsız olarak, Alice tarafından 4. bit geçersiz ilan edilecektir.



Şekil 2. Eve'nin var olduğu durumda BB84 protokolünün çalışması

Şekil 2’de iletişimi dinleyen üçüncü bir tarafın var olduğu durumda BB84 protokolünün nasıl çalıştığı görülmektedir. Örnek olarak 2. biti ele alalım. Alice, “0” değeri için 450 olarak polarize edilmiş foton gönderir. Eve, Alice ile aynı tabanı seçtiği için ölçüm sonucunda “0” değerini elde eder ve fotonun polarizasyonunu bozmaz. Bob, Eve’nin araya girip dinlediği fotonda kuantum ölçüm gerçekleştirir. Alice ile aynı tabanı seçtiği için ölçüm sonucu “0” olur. Alice ve Bob’un, tabanları ve bit değerleri aynı olduğu için Eve’nin varlığı tespit edilemez. 3. biti inceleyecek olursak Alice, “0” değeri için 00 olarak polarize edilmiş foton gönderir. Eve, Alice ile farklı tabanı seçtiği için %50 ihtimalle “0”, %50 ihtimalle “1” olarak ölçüm sonucu elde edecektir. Örneğimizde Eve’nin ölçüm sonucu “1” değeridir ve fotonun polarizasyonunu bozulmuştur. Eve’nin ölçüm sonucunda fotonun polarizasyonu 1350 haline gelir. Bob, Eve’den farklı taban kullandığı için %50 ihtimalle “0”, %50 ihtimalle “1” olarak ölçüm sonucu elde edecektir. Örneğimizde Bob’un ölçüm sonucu “1” değeridir. Alice ve Bob, aynı tabanı kullanmış olmalarına rağmen farklı bit değerlerine sahiptirler. Normalde beklenen aynı bit değerine sahip olmalarıdır. Farklı bit değerine sahip olmaları iletişimi dinleyen üçüncü bir tarafın varlığının tespit edilmesini sağlar. 5. bit, 3. bit ile benzer durumdadır. Eve, Alice’in seçtiği tabandan farklı taban seçmiştir. Eve’nin polarizasyonu bozmasına rağmen Bob, ölçüm sonucunda Alice ile aynı bit değerini elde etmiştir. Bu durumda Alice ve Bob, aynı tabanı kullanıp aynı bit değerine sahip oldukları için Eve tespit edilemez.

## B92 Protokolü

B92 protokolü, Bennett tarafından BB84 protokolüne alternatif olarak geliştirilmiştir. Protokolde, ortogonal olmayan iki durum kullanılmaktadır. Fotonu polarize edebilmek için Doğrusal (Rectilinear) ve Köşegensel (Diagonal) tabanlar kullanılmaktadır. Alice, 00 polarizasyon durumu için bit değerini “0” ve 450 polarizasyon durumu için bit değerini “1” olarak kabul eder. Bob, 900 polarizasyon durumu için bit değerini “1” ve 1350 polarizasyon durumu için bit değerini “0” olarak kabul eder. Bob, 00 ve 450 polarizasyon durumlarını kabul etmez. B92 protokolünün adımları aşağıdaki gibidir (Bennet, 1992):

Adım 1: Alice, “0” bit değeri için 00 ve “1” bit değeri için 450 polarizasyon durumlarının olduğu foton dizisini hazırlar ve Bob’a gönderir.

Adım 2: Bob, Doğrusal ve Köşegensel tabanlar içerisinden rastgele seçimler yaparak foton dizisinde ölçüm gerçekleştirir.

Adım 3: Bob, sadece 900 ve 1350 polarizasyon durumunda yapılan ölçüm sonuçlarını kabul eder. Ölçüm sonuçlarına göre Bob, 900 polarizasyon durumu için bit değerini “1” ve 1350 polarizasyon durumu için bit değerini “0” olarak kabul ederek anahtar oluşturur.

Adım 4: Bob, anahtar oluşturmak için kullandığı fotonların indislerini duyurur.

Adım 5: Eve’nin varlığını tespit etmek için Alice, kullandığı bazların bir kısmını duyurur. Kabul edilen fotonlar için Alice ve Bob’un farklı tabanları kullanması gerekir. Bob, Alice’in duyurduğu tabanlar ile kendi seçtiği tabanları karşılaştırır. Eğer aynı tabanlar seçilmiş ise Eve’nin varlığı tespit edilmiş olur ve anahtarın geçersiz olduğu duyurulur.



Şekil 3. Eve var olmadığı durumda B92 protokolünün çalışması

Şekil 3’te B92 protokol örneği görülmektedir. Alice’in ve Bob’un seçimlerine ilişkin tüm olasılıklar gözükmektedir. Alice’in, 00 polarizasyon ile foton gönderdiği durumları ele alalım. Bob, Doğrusal taban kullanarak ölçüm gerçekleştirirse %100 ihtimalle 00 polarizasyon durumunu elde edecektir. Bob, bu polarizasyon durumunu kabul etmeyecektir. Bob, Köşegensel taban kullanarak ölçüm gerçekleştirirse %50 ihtimalle 450 ve %50 ihtimalle 1350 polarizasyon durumunu elde edecektir. 450 polarizasyon durumunu kabul etmeyecektir. 1350 polarizasyon durumunu kabul eder ve bit için “0” değerini anahtara ekler. “1” değerinin gönderilmesine ilişkin ihtimaller Şekil 3’te gösterilmektedir.



Şekil 4. Eve’nin var olduğu durumda B92 protokolünün çalışması

Şekil 4’te Alice’in “0” değerini gönderdiği durum için Eve’nin ve Bob’un yapacağı seçimlerin tüm olasılıkları gözükmektedir. 00 ve 450 polarizasyon durumları Bob tarafından geçersiz kabul edilecektir. 1350 polarizasyon geçerli kabul edilecek fakat Eve’yi tespit edemeyecektir. 900 polarizasyon durumlarında Eve tespit edilebilecektir. Bob’un, 900 polarizasyon durumunda bir ölçüm yapabilmesi için Doğrusal taban kullanması gerekmektedir. Alice, “0” değerini göndermek için 00 polarizasyon durumunu kullanmaktadır. Bob, Doğrusal tabanla bu fotonu ölçtüğünde %100 ihtimalle 00 polarizasyon durumunu ölçecektir. Eğer ölçüm sonucu gelmesi imkânsız olan 900 polarizasyon durumu ise araya girip ölçüm gerçekleştirildiği ve fotonun polarizasyonunun bozulduğu anlamına gelmektedir. Böylece Eve’nin varlığı tespit edilmiş olacaktır.

##  BB84 ve B92 Protokolünün Karşılaştırılması

BB84 protokolünde, iletişimi dinleyen üçüncü bir taraf olmadığı zaman %50 ihtimalle anahtar oluşturur. B92 protokolünde, iletişimi dinleyen üçüncü bir taraf olmadığı zaman %33 ihtimalle anahtar oluşturur. BB84 protokolünde, iletişimi dinleyen üçüncü bir taraf olduğu zaman %33 oranında anahtarı kabul eder ve anahtar olarak kabul ettiği bitlerde Eve’nin varlığını tespit edemez. B92 protokolünde, iletişimi dinleyen üçüncü bir taraf olduğu zaman %22 oranında anahtarı kabul eder ve anahtar olarak kabul ettiği bitlerde Eve’nin varlığını tespit edemez. BB84 protokolü, %22 oranında Eve’nin varlığını tespit eder. B92 protokolü, %22 oranında Eve’nin varlığını tespit eder. B92 protokolü, BB84 protokolüne nazaran daha az anahtar üretim oranına sahiptir. Araya giren üçüncü tarafı ikisi de aynı oranda tespit etmektedir. B92 protokolü, araya giren üçüncü tarafın kandırmasına daha dayanıklı olduğu için daha güvenlidir.



Şekil 5. BB84 ve B92 protokollerinin karşılaştırılması

# BB84 ve B92 Protokollerinin Simülasyonu ve Karşılaştırılması

 Simülasyonlar, IBM Qiskit üzerinde yerel olarak gerçekleştirilmiştir. Simülasyon hazırlamak için Qiskit (<https://qiskit.org/textbook/ch-algorithms/quantum-key-distribution.html>) dokümanlarından faydalanılmıştır. Simülasyonlar yerel olarak yapıldığı için kanal gürültüsü gözardı edilmiştir. 00 polarizasyon durumu $|0⟩$ ,450 polarizasyon durumu $|+⟩$ ,900 polarizasyon durumu $|1⟩$ ve 1350 polarizasyon durumu $|–⟩$ ile temsil edilmektedir. Doğrusal taban Z bazı ve Köşegensel taban X bazı ile temsil edilmektedir.

## BB84 Protokolünün Simülasyonu

 Adım 1a: Alice, 0 ve 1 arasından rastgele seçim yaparak alice\_bits dizisini oluşturur.



 Adım 1b: Alice, kullanılacak bazlar için 0 ve 1 arasından rastgele seçim yaparak alice\_bases dizisini oluşturur.



 Adım 2: Alice, Bob’a göndereceği kuantum durumları hazırlar.





 Adım 3a: Bob, kullanılacak bazlar için 0 ve 1 arasından rastgele seçim yaparak bob\_bases dizisini oluşturur.



Adım 3b: Bob, seçmiş olduğu bazları kullanarak Alice’in gönderdiği kuantum durum üzerinde ölçme yapar.





 Adım 4: Bob, bob\_bases dizisini duyurur.

Adım 5: Alice, doğru seçilen bazları duyurur. Alice ve Bob’un farklı seçmiş olduğu bazlar silinir.





Adım 6: Bob, anahtar bitlerinin bir kısmını duyurur.





 Adım 7: Alice, Bob’un duyurduğu örnek bitleri kıyaslayarak Eve’nin varlığını tespit eder.



## B92 Protokolünün Simülasyonu

 Adım 1: Alice, 0 ve 1 için sırasıyla $|0⟩$ ve $|+⟩$ kuantum durumlarını hazırlar ve gönderir.





Adım 2: Bob, Alice’in gönderdiği kuantum durum üzerinde rastgele seçtiği bazlarda ölçüm yapar.



 Adım 3: Bob, ölçüm sonuçlarına göre anahtar oluşturur.







Adım 4: Bob, anahtar oluşturmak için kullandığı indislerin dizisi Bob\_list’i duyurur. Alice, duyurulan indislere göre anahtarını düzenler.





Adım 5: Alice, Eve’nin varlığını tespit etmek için kullandığı bazların bir kısmını duyurur. Bob, kendi bazları ile kıyaslayarak Eve’in varlığını tespit eder.



## BB84 ve B92 Protokollerinin Simülasyonlarının Karşılaştırılması

|  |
| --- |
| Tablo 1. BB84 ve B92 protokollerinin Eve var olmadığı durumda simülasyon sonuçları |
|  | **1** | **2** | **3** | **4** | **5** | **ORTALAMA** |  |
| Toplam Kubit | 100 | 100 | 100 | 100 | 100 | 100 |  |
| BB84  | 44 | 46 | 51 | 50 | 42 | 46.6 |  |
| B92  | 31 | 27 | 28 | 24 | 35 | 29 |  |

BB84 ve B92 protokollerinin Eve olmadan simülasyon sonuçları görülmektedir (Tablo 1). Simülasyon 5 kez çalıştırılmıştır. Her çalıştırmada 100 Kubit kullanılmıştır. BB84 protokolü, ortalama olarak %46.6 oranında anahtar oluşturmaktadır. Simülasyonumuzun sonuçları, beklenen anahtar oluşturma oranı olan %50’ye yaklaşmıştır. B92 protokolü, ortalama olarak %29 oranında anahtar oluşturmaktadır. Simülasyonumuzun sonuçları, beklenen anahtar oluşturma oranı olan %33’e yaklaşmaktadır.

|  |
| --- |
| Tablo 1. BB84 ve B92 protokollerinin Eve var olduğu durumda simülasyon sonuçları |
|  | **1** | **2** | **3** | **4** | **5** | **ORTALAMA** |  |
| Toplam Kubit | 100 | 100 | 100 | 100 | 100 | 100 |  |
| BB84 Geçerli | 35 | 37 | 38 | 33 | 24 | 33.4 |  |
| BB84 Dinleme var | 24 | 11 | 17 | 15 | 20 | 17.4 |  |
| B92 Geçerli | 26 | 15 | 17 | 23 | 17 | 19.6 |  |
| B92 Dinleme var | 16 | 19 | 24 | 20 | 23 | 20.4 |  |

BB84 ve B92 protokollerinin Eve var olduğu zaman simülasyon sonuçları görülmektedir (Tablo 2). Simülasyon 5 kez çalıştırılmıştır. Her çalıştırmada 100 Kubit kullanılmıştır. Eve varken BB84 protokolü, ortalama olarak %33.4 oranında anahtarı geçerli kabul eder. Eve varken BB92 protokolü, ortalama olarak %19.6 oranında anahtarı geçerli kabul eder. BB84 protokolü, %17.4 oranı ile dinlemenin varlığını tespit etmektedir. B92 protokolü, %20.4 oranı ile dinlemenin varlığını tespit etmektedir.

## SONUÇ

Simülasyon sonuçlarına göre B92 protokolünün, BB84 protokolünden daha düşük anahtar üretim oranına sahip olduğu görülmektedir. Her iki protokol teorik olarak aynı oranda Eve’yi tespit etmektedir. Simülasyon sonuçlarına göre B92 protokolünün, %3 daha fazla dinleme tespit ettiği gözlenmiştir. Simülasyon sonuçlarına göre, Eve’nin var olduğu durumda BB84 protokolü %33.4 oranında geçerli anahtar kabul ederken, B92 protokolü %19.6 oranında geçerli anahtar kabul etmektedir. Teorik olarak bu oran BB84 protokolü için %33 ve B92 protokolü için %22 dir. B92 protokolünün, Eve tarafından daha az kandırıldığı gözlenmiştir. Simülasyon sonuçlarını da dikkate alaraktan B92 protokolünün daha güvenli olduğu görülmektedir.

Kaynakça

Bennett C.H. (1992). Quantum Cryptography Using Any Two Nonorthogonal States, *Physical Review Letters, 68*, 3121 – 3124

Bennett C.H., & Brassard G. (1984). Quantum Cryptography: Public Key Distribution and Coin Tossing, International Conference on Computers, systems & Signal Processing Bangalore, India: 175 – 179

Feynman R.P. (1982). Simulating Physics with Computers, *International Journal of Theoretical Physics, 21*, 467 – 488

Shor P.W. (1994). Algorithms for Quantum computation: Discrete Logarithms and factoring, Proceedings of the 35th Symposium on Foundations of Computer Science, Los Alamitos, California: 124 – 134

Rivest R., Shamir A., & Adleman L. (1978). A Method for Obtaining Digital Signatures and Public Key Cryptosystems, *Commucations of the ACM, 21*(2), 120-126