**BB84 ve B92 KUANTUM ANAHTAR DAĞITIM PROTOKOLLERİNİN KARŞILAŞTIRILMASI**

Ercan ÇAĞLAR1, 0000-0002-6840-1519, ercaglar@comu.edu.tr
Engin ŞAHİN2, 0000-0002-8040-0519, enginsahin@comu.edu.tr

İhsan YILMAZ2, iyilmaz@comu.edu.tr

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

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. 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 IBM Kuantum Bilgisayarında Qiskit kütüphanesi kullanılarak simülasyonu ve analizleri gerçekleştirilmiş ve tartışılmıştır.

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

**COMPARISONS of BB84 and B92 QUANTUM KEY DISTRIBUTION PROTOCOLS**

Ercan ÇAĞLAR1, 0000-0002-6840-1519, ercaglar@comu.edu.tr
Engin ŞAHİN2, 0000-0002-8040-0519, enginsahin@comu.edu.tr

İhsan YILMAZ2, iyilmaz@comu.edu.tr

1Department of Computer and Instructional Technologies Education, Faculty of

Education, Çanakkale Onsekiz Mart University, Çanakkale, Turkey

 2Department of Computer Engineering, Faculty of Engineering, Çanakkale Onsekiz

Mart University, Çanakkale, Turkey

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. 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 on IBM Quantum Computer using Qiskit library were performed and discussed.

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