EEB MÜHENDİSLİKLERİ İÇİN BİLGİSAYAR DESTEKLİ EĞİTİM: KUANTUM KRİPTOGRAFİ BENZETİM VE EĞİTİM UYGULAMASI

Mustafa TOYRAN[1]

[1]TÜBİTAK, UEKAE
P.K.: 74, 41470, Gebze, Kocaeli

[1]mtoyran@uekae.tubitak.gov.tr

ÖZET

Bu çalışmada eğitimciler, öğrenciler ve araştırmacılar için kullanılabilecek Kuantum Kriptografi Benzetim ve Eğitim Uygulaması adı verilen animasyon destekli bir eğitim yazılımı tanıtılacaktır. Kuantum Kriptografi benzetim ve eğitim ortamı BB84 kuantum anahtar dağıtım protokolünün benzetiminin yapılabildiği görsel bir uygulamadır. Program, Borland C++ Builder 6.0 programlama dili kullanılarak Windows XP ve Windows 2000 işletim ortamları üzerinde gerçekleştirilmiştir. Geliştirilmesi devam eden bu çalışmanın kuantum kriptografi ile ilgilenen eğitimcilere, araştırmacılara ve öğrencilere faydalı olması amaçlanmıştır.

1. GİRİŞ

Günümüzde bilgisayar teknolojisinden hayatın her alanında yararlanılmaktadır. Bilgisayarların yaygın olarak kullanıldığı iki uygulama alanı "eğitim" ve "benzetim"dir. Eğitimde bilgisayar teknolojisinin kullanılmasına "bilgisayar destekli eğitim" [1,2,3] denilmektedir. Bu uygulamalarda etkileşimli uygulama ve animasyonlarla öğrencilerin hem derslerde dikkati arttırılır hem de daha kolay öğrenmelerine yardımcı olunur. Ayrıca, bilgisayar benzetimleri ile oynamak sadece denklemlerle çalışmaktan çok daha iyidir. Bunun yanında, bilgisayarlar bizlere, bu çalışmada olduğu gibi, gerçeklenmesi çok zor ve karmaşık sistemlerin benzetimini yapabilme olanağı da vererek bu sistemleri inceleyebilmemize de yardımcı olurlar.

2. KUANTUM KRİPTOGRAFİ

Kuantum kriptografi, ilk olarak 1984 yılında Charles Bennett ve Gilles Brassard tarafından keşfedilen [4] kuantum mekaniksel bir kriptografik gizli anahtar dağıtım yöntemidir. Protokol, kuruluş yılından ve kurucularının soyadlarının baş harflerinden dolayı BB84 protokolü olarak da adlandırılmaktadır.

Bu teknikte iletişim, optik kanallar üzerinden fotonlar kullanılarak gerçekleştirilmekte ve iletişim esnasında optik hatta bir müdahale olup olmadığı da açığa çıkarılabilmektedir. Böylece, dinlenemez ve trafiği kopyalanamaz bir iletişim olanağı verilmektedir. Protokol özetle şu şekilde çalışmaktadır (bkz. Şekil 4):

- Gönderici, *Alice*, öncelikle rasgele bir bit dizisi seçer. Alıcının bu bit dizisinden haberi yoktur.
- Gönderici her bir biti için rasgele bir polarizasyon tabanı (+ veya X) belirler, bitini bu tabanda Şekil 3 uyarınca uygun (|, ─, / veya \ ) polarize edilmiş fotonla kodlar ve fotonu alıcıya gönderir.
- Alıcı, *Bob*, gelen her bir fotonun polarizasyonunu ölçer. Göndericinin fotonları polarize ederken hangi polarizasyon tabanlarını kullandığını bilmediğinden ölçümü sırasında fotonlar için kullanacağı polarizasyon tabanlarını rasgele seçer. Sonuçta, o da Şekil 3 uyarınca bir bit dizisi elde eder.
- Gönderici ve alıcı sadece kullandıkları polarizasyon tabanlarını kimlik kanıtlamalı bir kanal üzerinden, örneğin telefonla, birbirlerine açıklar. Aynı polarizasyon tabanlarını kullandıkları durumlar için gönderilen ve alınan bitler kesinlikle aynı olacaktır. Bu ortak, ama gizli, bitler *gizli anahtar* olarak kullanılırlar.

Kuantum kriptografide, aynı polarizasyon tabanının kullanıldığı bir durum için gönderilen ve alınan bir bitin farklı çıkması hattı dinleyen bir şüphelinin, *Eve*, varlığına işarettir. Bu özellik kullanılarak, kullanılan iletişim hattına şüpheli bir müdahale olup olmadığını açığa çıkarmak da mümkündür.

3. KUANTUM KRİPTOGRAFİ BENZETİM VE EĞİTİM UYGULAMASI

Kuantum Kriptografi benzetim ve eğitim ortamı, yukarıda kısaca özetlenen BB84 kuantum anahtar dağıtım protokolünün benzetiminin yapılabildiği görsel bir uygulamadır. Program, Borland C++ Builder 6.0 programlama dili kullanılarak, Microsoft Windows XP ve Microsoft Windows 2000 işletim ortamları üzerinde gerçekleştirilmiştir.

Uygulamanın gerçekleştirilmesinin iki temel hedefi bulunmaktadır:

- **Eğitsellik:** Kuantum Kriptografi benzetim ve eğitim ortamı temelde bir eğitim uygulamasıdır. Eğitsel mod, uygulamanın eğitim amaçlı kullanımı için hazırlanmış, görselliğin daha ön planda tutulduğu

çalışma modudur. Bu modda yapılan işlemler ayrıntılı olarak, küçük animasyonlarla kullanıcıya da gösterilir. Bu modda uygulama daha yavaş ve daha dar değer aralıklarıyla çalışır.

- **Sayıtsallık:** Kuantum Kriptografi benzetim ve eğitim ortamının sayıtsal bir yönü de mevcuttur. Uygulama bu modda çok sayıda çalıştırılarak istatistiksel birtakım bilgiler de çıkarılabilir. Sayıtsal mod, uygulamanın istatistiksel amaçlı kullanımı için hazırlanmış görselliğin daha geri planda tutulduğu çalışma modudur. Yapılan işlemlerin ya da aşamaların sadece isimleri gösterilir, animasyonlar gösterilmez. Bu modda uygulama daha hızlı ve daha geniş değer aralıklarıyla çalışır.

3.1 ARAYÜZ

Kuantum Kriptografi benzetim ve eğitim uygulaması çalıştırıldığında karşımıza Şekil 1'de görülen ekran gelecektir:

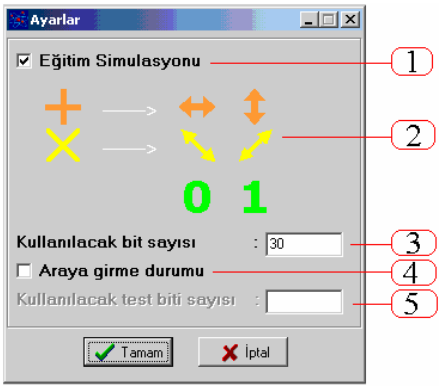
Şekil 1. Kuantum Kriptografi benzetim ve eğitim uygulaması açılış ekranı.

Uygulamanın **1** ile gösterilen menü yapısı Şekil 2'deki gibidir:

Dosya Çıkış	**Simulasyon** Yeni simulasyon Raporlar Son deneme Genel rapor Ayrıntılı rapor Özet rapor Anahtarları göster
Yardım Kuantum Kriptografi İletişim Program hakkında	

Şekil 2. Menü yapısı.

Bir benzetim başlatmak için **Simulasyon --> Yeni simulasyon** menü seçeneğinin seçilmesi ya da **2** ile gösterilen **BAŞLA** butonuna basılması gerekir. Bu durumda karşımıza Şekil 3'te görülen **Ayarlar** penceresi gelir:



Şekil 3. Ayarlar penceresi.

Ayarlar penceresinde numaralı bölgelerin anlamları şöyledir:

1: **Eğitim Simulasyonu** seçeneğinin seçili olması "Eğitsel" modun aktif olduğu anlamına gelir. Aksi halde, "Sayıtsal" mod aktiftir.

2: Bitleri fotonlarla kodlama kuralları. Örneğin, ***0 biti*** kenarsal (+) polarizasyon tabanında 0^o'lik polarizasyonda ve köşegensel (X) polarizasyon tabanında 135^o'lik polarizasyonda bir fotonla kodlanmaktadır. Bu ayarlar değiştirilemez.

3: İletişimde kullanılacak mesajların bit olarak uzunlukları **Kullanılacak bit sayısı** kutusuna girilir.

4: **Araya girme durumu** seçeneğinin seçili olması "Arada birinin bulunduğu" modun aktif olduğu anlamına gelir. Aksi halde, "Arada kimsenin bulunmadığı" mod aktiftir.

5: Kullanılacak test bitlerinin sayısı **Kullanılacak test biti sayısı** kutusuna girilir. **Kullanılacak test biti sayısı**, **Kullanılacak bit sayısı**ndan fazla olamaz.

3.2 BENZETİMLER

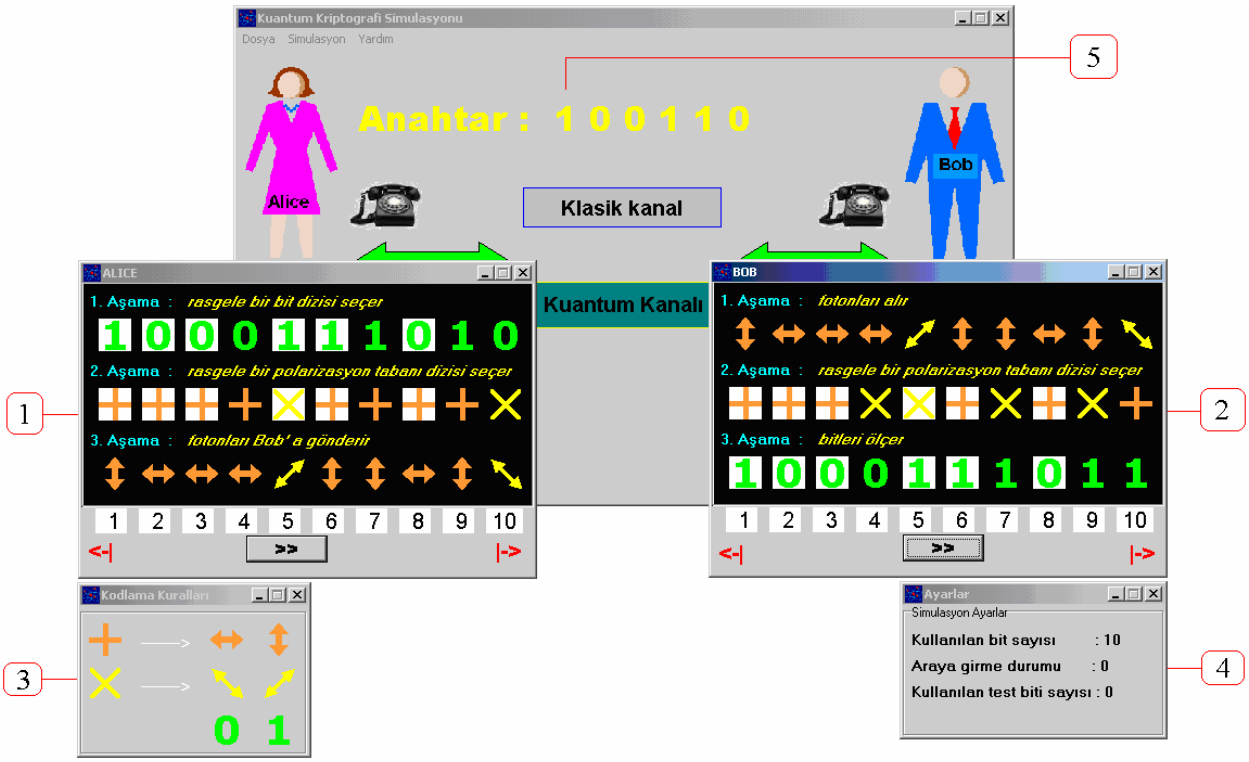
Eğitsel ve sayıtsal modda yapılabilecek iki tür kuantum kriptografi benzetimi mevcuttur:

- **Arada kimse yokken kuantum kriptografi benzetimi**: Arada iletim hattını dinleyen biri(leri)nin

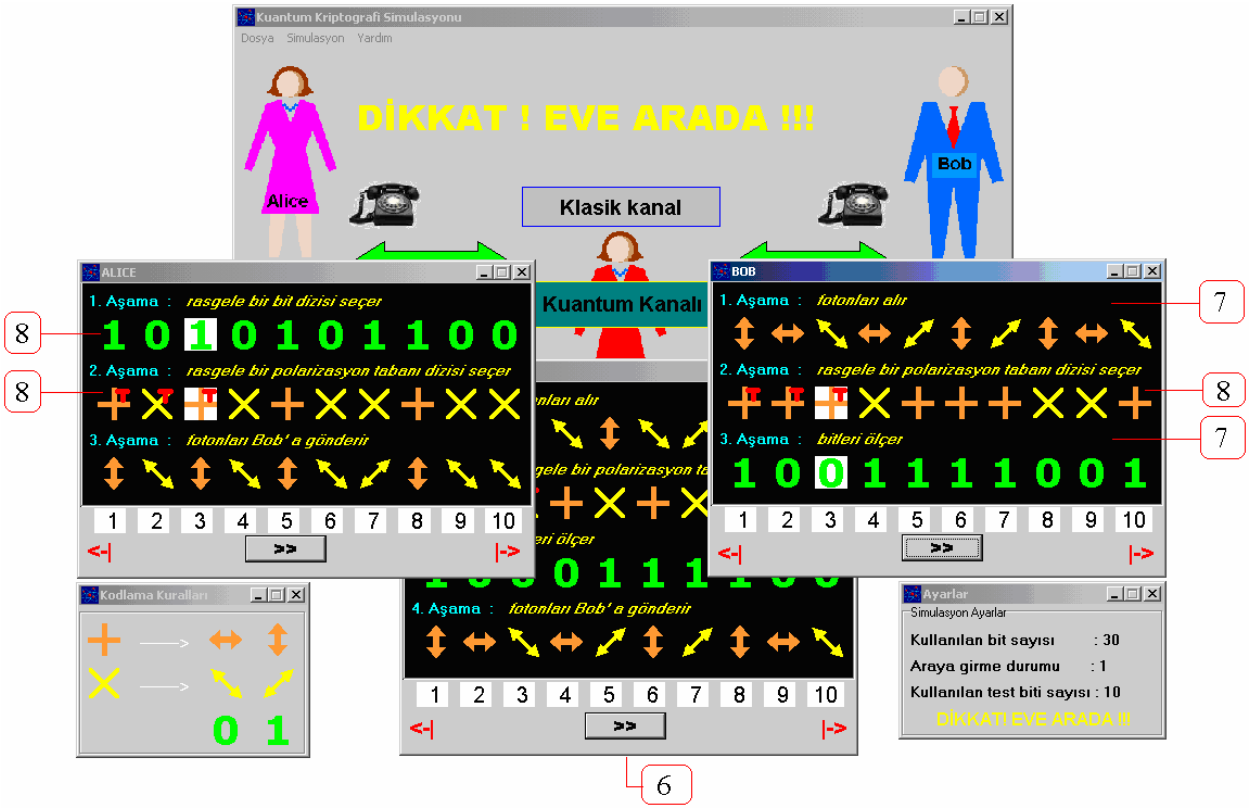
olmadığı moddur. Bu modda gönderilen mesajlar aynen karşı taraftan alınmalıdır (bkz. Şekil 4).

- **Arada biri varken kuantum kriptografi benzetimi**: Arada iletim hattını dinleyen biri(leri)nin bulunduğu moddur. Bu nedenle iletimde bir hata olmuşsa buna kesinlikle hattı dinleyenler sebep olmuştur (bkz. Şekil 5).

Uygulamada, iletişim ortamından kaynaklanan bozulmaların olmadığı kabul edilmektedir.



Şekil 4. Arada kimse yokken kuantum kriptografi benzetimi.

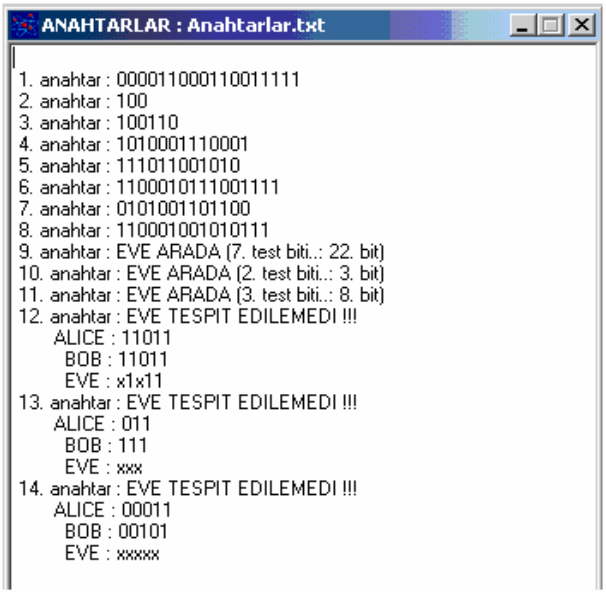


Şekil 5. Arada biri varken kuantum kriptografi benzetimi.

Benzetimlerde, sol tarafta **1** ile gösterilen Alice ve penceresi, sağ tarafta **2** ile gösterilen Bob ve penceresi, ortada ise **6** ile gösterilen Eve ve penceresi görülmektedir. Alice ile Bob, BB84 kuantum anahtar dağıtım protokolünü kullanarak ortak bir gizli anahtar üzerinde anlaşmak istemektedir. Eve ise araya girerek iletişimi dinlemek ve gizli anahtarı ele geçirmek istemektedir. Araya birinin girdiği durumlarda bunun belirlenmesi olasılığını arttırmak için yapılması gereken test bitlerinin sayısını arttırmaktır.

Benzetim başladığında *Ayarlar* penceresinde yapılan ayarlar **3** ile gösterilen ***Kodlama Kuralları*** ve **4** ile gösterilen ***Ayarlar*** pencerelerinde kullanıcıya gösterilir.

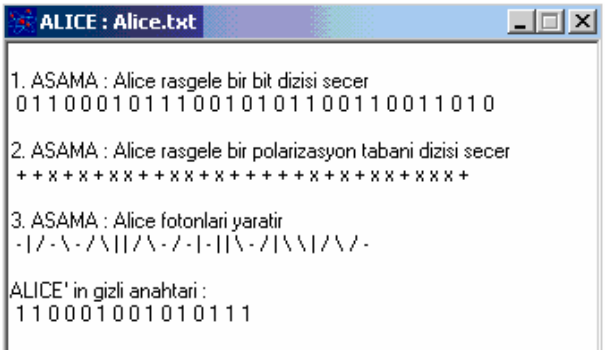
Benzetim >> butonları ile koşturulur. Benzetim sonunda elde edilen *gizli anahtar*, uzunluğu 10 biti aşmıyorsa uygulamanın ana penceresinde **5** ile gösterilen bölgede kullanıcıya gösterilir. Şekil 4'te tarafların 6 bitlik 100110 gizli anahtarı üzerinde anlaştığı görülmektedir. 10 biti aşması durumunda anahtarı görmek için ana pencerede çıkan "**Anahtar: Çift tıkla**" yazısına farenin sol tuşu ile çift tıklamak gerekir. Arada saldırganın olması durumunda, eğer saldırgan yakalanmışsa, burada "**DİKKAT ! EVE ARADA !!!**" yazar. Şekil 5'te saldırganın varlığının tespit edildiği görülmektedir.



Şekil 6. Anahtarlar.

Anahtarı görmek için bir diğer yol **Simulasyon --> Anahtarları göster** menü seçeneğinin seçilmesidir. Böyle yapıldığında benzetim sonucunda elde edilen anahtar ayrı bir pencerede kullanıcıya görüntülenecektir (bkz. Şekil 6). Yapılan en son benzetim sonucu elde edilen gizli anahtar bu pencerenin en sonunda görüntülenmektedir.

Yapılan benzetimde elde edilen gizli anahtarı görmek için üçüncü bir yol da herhangi bir anda Alice'in, Bob'un ya da Eve'in penceresi üzerinde **7** ile gösterilen boş bir alana farenin sol tuşu ile çift tıklamaktır. Bu durumda Şekil 7'deki gibi yeni bir pencere açılacaktır. Penceresine çift tıklanan kişinin benzetim esnasında gerçekleştirdiği tüm işlemler bu pencerede aşama aşama kullanıcıya görüntülenecektir.

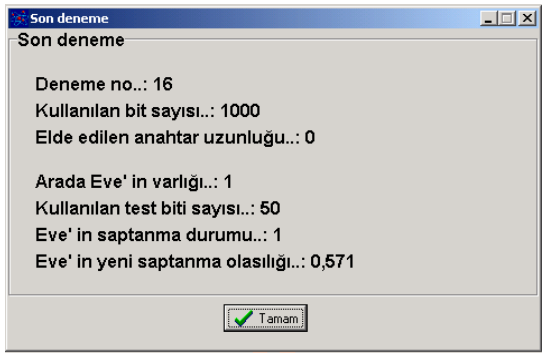


Şekil 7. Alice'in penceresi.

Benzetim esnasında rasgele seçimlerin yapıldığı **8** ile gösterilen aşamalarda seçimlere müdahale(ler)de bulunabilmek mümkündür. Ancak bu müdahale(ler) sadece rasgele seçimlerin yapıldığı ilgili aşamalarda yapılmalıdır. Bir sonraki aşamaya geçildiğinde bir daha müdahale imkanı olmayacaktır. Seçimin değerini değiştirmek için ilgili değerin üzerine farenin sol tuşu ile çift tıklanır. Bu durumda üzerine çift tıklanan değer diğer değere kurulur. Örneğin Şekil 5'te Alice, Bob ve Eve pencerelerinde bitlerin ve polarizasyon tabanlarının rasgele seçildiği aşamalarda müdahaleler yapılabilir.

Benzetimlerde sıra numaraları da altta, beyaz kutucuklar içinde, görüntülenmektedir. Bit sayısının 10'dan fazla olduğu durumlarda diğer değerleri de görebilmek için <-| ve |-> butonları kullanılabilir.

Kullanıcı herhangi bir anda ***Simulasyon --> Yeni Simulasyon*** menü seçeneğini seçerek mevcut benzetimi sonlandırabilir ve yeni bir benzetim başlatabilir.



Şekil 8. Son deneme raporu.

3.3 RAPORLAR

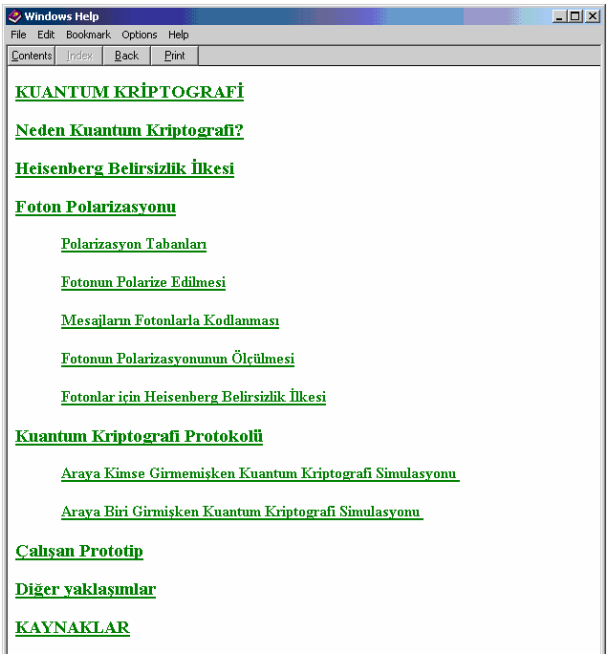
Uygulamada ayrıntılı bir rapor sistemi bulunmaktadır. Bu sistem sayesinde kullanıcı yaptığı benzetimler ve sonuçları ile ilgili kapsamlı bilgilere ulaşabilir. Raporlara ***Simulasyon --> Raporlar*** menü seçeneği ile ulaşılır. Üç farklı rapor seçeneği bulunmaktadır:

- Kullanıcı isterse sadece son benzetime ilişkin bir rapor isteyebilir (bkz. Şekil 8).

- Kullanıcı isterse yapılan tüm benzetimlerin raporlarını teker teker görebilir.
- Kullanıcı isterse tüm benzetimlere ilişkin tek bir özet rapor isteyebilir. Bu raporda yapılan tüm benzetimler için toplam sonuçları, genel ortalamaları ve olasılıkları görme imkanına sahiptir.

3.4 EĞİTİM VE YARDIM

Uygulamanın eğitsellik yönünün daha ön planda tutulması nedeni ile program yukarıda belirtilenlerin yanında ayrıntılı yardım ve bilgilendirme özelliklerine de sahiptir. **Yardım --> Kuantum Kriptografi** menü seçeneği seçildiğinde Kuantum Kriptografi ile ilgili kapsamlı yardım bilgilerine ulaşılır (bkz. Şekil 9).



Şekil 9. Yardım ekranı.

Ayrıca, benzetimler esnasında herhangi bir anda F1 tuşuna basarak o benzetim anı ya da aşaması ile ilgili yardım bilgilerine de ulaşılabilir (bkz. Şekil 10).

Şekil 10. Benzetimin o anı ile ilgili yardım ekranı.

4. TARTIŞMA

Bir kuantum kriptografi sisteminin gerçeklenmesinin maliyeti kuantum iletişim kanalı, foton üreteci, foton polarize edici, foton dedektörü ve foton polarizasyon ölçücü gibi yeni ve pahalı bileşenlere ihtiyaç olması nedeniyle günümüz koşullarında çok yüksek olup milyon YTL'ler mertebesindedir. Dolayısıyla, her yerde böyle bir ortamı sağlamak pek olası değildir. Gerçeklenen benzetim uygulamasının amaçlarından biri de bu eksikliğin az da olsa doldurulmasıdır.

Bununla birlikte, gerçeklenen uygulama sadece BB84 protokolü ile sınırlıdır ve benzetimler sadece gürültüsüz durumlar için yapılabilmektedir. İlerideki çalışmalarda kuantum kriptografi ile ilgili en son gelişmelerin takip edilerek içeriğe eklenmesi ve animasyonlarının gürültülü durumlarda da yapılabilmesi çok yararlı olacaktır. Ayrıca, görsel animasyonların yanında sesli anlatımların da eklenmesi faydalı olabilir. Bunların tümü geliştirilmeye açık konulardır.

Kuantum kriptografi ile ilgili daha ayrıntılı bilgi edinmek ve yeni gelişmeleri öğrenmek için [5-11]'deki kaynaklardan ve referanslarından yararlanılabilir.

5. SONUÇ

Bu çalışmada kuantum kriptografi ile ilgili temel kavramların anlaşılması için animasyon destekli bir eğitim yazılımı hazırlanmıştır. Uygulamanın bu konularda çalışan eğitmenlere, öğrencilere ve araştırmacılara faydalı olması ümit edilmektedir. Bu çalışmaya ve ilgili bilgilere [12]'den erişilebilir veya yazarlardan da yardım istenebilir. Bu ve benzeri çalışmaların geliştirilebilmesi için okuyucuların görüş ve önerilerini almak yazarları mutlu edecektir.

KAYNAKLAR

[1]. Odabaşı F., "Ünite 8: Bilgisayar Destekli Eğitim", www.aof.edu.tr/kitap/IOLTP/2276/unite08.pdf, Erişim Tarihi: 2006.

[2]. http://stu.inonu.edu.tr/~e040040026/Bilgi1.htm, Bilgisayar Destekli Eğitim Nedir?, E. T.: 2006.

[3]. http://www.bilkent.edu.tr/~serpilt/bde.htm, BDE - Bilgisayar Destekli Eğitim Nedir ?, E. T.: 2006.

[4]. Bennet C. H. ve Brassard G., "Quantum Cryptography: Public Key Distribution and Coin Tossing", Proc. Int'l Conf. Computers, Systems & Signal Process., CS Press, s.175–179, 1984.

[5]. Williams C. P. ve Clearwater S. H., Explorations in quantum computing, Springer, 1998.

[6]. Gisin N., Ribordy G., Tittel W. ve Zbinden H., "Quantum cryptography", Rev. Mod. Phys., vol. 74, s. 145–195, 2002.

[7]. Toyran M., Erdem S.S. ve Gedikbey B., "Kuantum Kriptografi", EMO – YTÜ – TÜBİTAK Elektrik-Elektronik-Bilgisayar Mühendisliği 11. Ulusal Kongresi ve Fuarı Bildiriler Kitabı, Cilt 1, Sayfa: 251-254, 2005.

[8]. http://www.qubit.org/, Centre for Quantum Computation, E. T.: 2006.

[9]. http://qso.lanl.gov/qc/, Quantum Computation at Los Alamos, E. T.: 2006.

[10]. http://xxx.lanl.gov/find/quant-ph, quant-ph preprint archive at Los Alamos E. T.: 2006.

[11]. http://www.csee.umbc.edu/~lomonaco/, Samuel J. Lomonaco'nun Web sayfası, E. T.: 2006.

[12]. Toyran M. ve Örencik B. "Kuantum Kriptografi", İTÜ Mustafa İnan Kütüphanesi Yüksek Lisans Tezleri Bölümü, Maslak, İstanbul, 2003.