Pedaqoji Universitetin Xəbərləri. Riyaziyyat və təbiət elmləri seriyası – 2023, C. 71, №3, s. 32-40
Transactions of Pedagogical University. Series of mathematics and natural sciences – 2023, V. 71, №3, pp. 32-40

UOT 2337Z349R

Z.N.Zəkəryəyev
Heydər Əliyev adına Hərbi İnstitut
zaur6622@mail.ru

RABİTƏ KANALININ KVANT KRİPTOQRAFİYASINDAN İSTİFADƏ EDƏRƏK QORUNMASI İMKANLARI

Açar sözlər: *Kvant kriptoqrafiyası, kvant hücumu, kvant rabitə xətləri, foton*

Tədqiqatın məqsədi kvant avadanlıqlarına və ümumilikdə sistemə məlum olan mümkün hücumları aydınlaşdırmaqdır. Burada əsas diqqət kvant hücumlarına yönəldilmişdir. Kvant hesablamalarında informasiya təhlükəsizliyinə qarşı gizlənən əsas təhdidlər göstərilmişdir. Məqalədə kvant kriptoqrafiyasından istifadə edərək rabitə kanalının qorunması imkanlarına baxılmış, məlumatların ötürülməsinin digər üsullarına nisbətən üstünlükləri, həmçinin kvant avadanlığının iş prinsipi, sındırılması və mühafizəsi nəzərdən keçirilmişdir. Kvant kriptoqrafiyasında istifadə olunan əsas protokollar və onların iş sxemləri, kvant kriptoqrafiyasının inkişafının əsas istiqamətləri, kvant rabitə kanalları və açarların mübadiləsi protokolu barədə geniş tədqiqatlar şərh edilmişdir. Həmçinin, məqalədə məlumatların qorunmasının yeni üsuluna - stenoqrama - kvant kriptoqrafiyasının təkmilləşdirilmiş versiyasına toxunulmuşdur. Bu tip informasiya mühafizəsinin iş üsulu təqdim olunmuş, kriptoqrafiyanın kvant kriptoqrafiyası ilə müqayisədə informasiyanı daha yaxşı mühafizə etməyə imkan verməsi əsaslandırılaraq ətraflı şəkildə araşdırılmış və təhlil edilmişdir.

З.Н.Закарьяев

ВОЗМОЖНОСТИ БЕЗОПАСНОСТИ КАНАЛА СВЯЗИ С ИСПОЛЬЗОВАНИЕМ КВАНТОВОЙ КРИПТОГРАФИИ

Ключевые слова: *Квантовой криптографии, квантовый атак, квантовые линии связи, фотон*

Цель исследования разобраться в известных в настоящее время возможных атаках на квантовое оборудование и систему в целом. Основное внимание уделяется квантовому хакингу. Показаны основные угрозы для информационной безопасности, которые кроются в квантовых вычислениях. В статье будет рассмотрена возможность защиты канала связи при помощи квантовой криптографии. Их преимущества над другими способами передачи данных, а также будет рассмотрен принцип работы, взлом и защита квантового оборудования. Рассмотрены основные протоколы, используемые в квантовой

криптографии и их схемы работы. Были обозрены основные направления развития квантовой криптографии: квантовые каналы связи и протокол обмена ключами. Также данная статья коснётся нового способа защиты данных- стенографии- улучшенной версии квантовой криптографии. Будет представлен метод работы данного вида защиты информации, а также обоснованно почему данный вид криптографии позволяет лучше защищать информацию, нежели квантовая криптография.

Z.N.Zakaryayev

COMMUNICATION CHANNEL SECURITY POSSIBILITIES USING QUANTUM CRYPTOGRAPHY

Keywords: Quantum cryptography, quantum hacking, quantum communication lines, photon.

The purpose of the study is to understand the currently known possible attacks on quantum equipment and the system as a whole. The focus is on quantum hacking. The main threats to information security, which lie in quantum computing, are shown. The article will consider the possibility of protecting the communication channel using quantum cryptography. Their advantages over other methods of data transfer, and the principle of work, hacking, and protection of quantum equipment will also be considered. The main protocols used in quantum cryptography and their operation schemes are considered. The main directions of the development of quantum cryptography were reviewed: quantum communication channels and a key exchange protocol. Also, this article will touch upon a new method of data protection - shorthand - an improved version of quantum cryptography. The method of operation of this type of information protection will be presented, as well as justified why this type of cryptography allows better protection of information than quantum cryptography.

Giriş

Hal-hazırda insanların çoxu üz-üzə görüşdən çox messencerlərdə söhbət etməyi üstün tuturlar. Belə bir zaman müddətində məlumatları mümkün sındırmalardan qoruya bilən və kənardan ən kiçik müdaxilə olmadan belə kommunikasiya xətti ilə məlumat ötürə bilən yaxşı kriptoqrafiya sisteminə malik olmaq vacibdir. Bu kriptoqrafiya üsulu ilə yalnız adi istifadəçilərdən məlumat ötürmək üçün deyil, həm də bir ölkənin və ya məsələn, bir bankın məxfi məlumatlarını ötürməyə xidmət edən rabitə kanallarını təmin etmək vacibdir. Bu günə qədər yalnız bir neçə kriptoqrafiya metodu belə bir təhlükəsizlik səviyyəsi ilə öyünə bilər. Onlardan biri kvant kriptoqrafiyasıdır.

Yaradılma tarixi

1983-cü ildə Stiven Vizner hökumət tərəfindən buraxılan dövlət kvant əskinaslarının yaradılması texnologiyasını təklif etmişdir. Texnologiyanın mahiyyəti ondan ibarətdir ki, hər bir əskinasda fotonlu tələlər var və onların hər biri iki fərqli bazisə görə müəyyən şəkildə qütbləşir. Birnci bazisdə "çarpaz formalı" qütbləşmə nəzərdə tutulurdu, yəni foton müəyyən bir vertikaldan 0 və ya 90 dərəcə bucaq altında qütbləşə bilərdi, ikincisi bazisdə isə diaqonal olaraq, yəni 45 və 135 dərəcə bucaqlarla qütbləşə bilər [2].

Vizner eyni zamanda məxfi rabitə kanallarının yaradılması üçün də oxşar mexanizmdən istifadə oluna biləcəyini təklif etmişdir. Məqaləsinin dərcindən cəmi bir il sonra elm adamları Jil Brassar və Çarls Bennet kvant rabitəsi üçün ilk protokolu işləyib hazırladılar ki, onlar bu protokolu öz adlarının ilk hərfləri və texnologiyanın yaradıldığı illə - BB84 adlandırdılar. Hal-hazırda məhz bu protokol müasir kvant rabitə şəbəkələrində geniş istifadə olunur [1].

Bu protokol əsasən aşağıdakı prinsip üzrə işləyir: Alisa bir-birinə paralel iki bazisdən birində polyarizasiya olunmuş Bob fotonlarını şaquli və ya diaqonal şəkildə göndərir. Bob, bu fotonları qəbul edərək polyarizasiyanı ölçür, bazis seçimi təsadüfi olaraq baş verir və yol boyu ölçmə nəticələrini və bazisləri yazır. Sonra, həmsöhbətlər istifadə olunan bazaları açıq kanal üzərindən dəyişdirirlər və müxtəlif bazalarda alınan məlumatlar atılır. Sonda yalnız bazislərin üst-üstə düşdüyü ölçülər qalır. Kvant açarlarının paylanmasının bu texnologiyası “açar süzməsi” adlanır [3].

Açarların paylanması üzrə kvant protokolunun iş prinsipi

Hal-hazırda mövcud olan bütün açıq açar alqoritmləri eyni şəkildə işləyir. Məsələn, RSA alqoritmi göndərilən mesajın məzmununu deşifrə edə biləcəyi açıq açardan istifadə edir. Bu alqoritmlər əsas amillərə və diskret loqarifmə parçalanmanın mürəkkəbliyinə əsaslanır [4].

Bu cür sistemlərə olduqca effektiv şəkildə hücumlar edilə bilər və bu barədə daha sonra ətraflı müzakirə ediləcəkdir. Sonra gizli açarları əsas götürən şifrləmə alqoritmləri köməyə gəlir. Bu alqoritm DES şifrələmə alqoritmini (Data Encryption Standard - IBM tərəfindən hazırlanmış simmetrik şifrləmə üçün alqoritm) özündə əks etdirir. Kodlu mesajların ötürülməsindən əvvəl hər iki tərəf açarları mübadilə etməlidir, bu açarların yalnız dialoqun iştirakçısına məlum olması vacibdir, əks halda əlaqə etibarsız olacaqdır [5].

Aydındır ki, bu vəziyyətdə təhlükəsiz açar mübadiləsi ön plana çıxır. O zaman, açarın özünün sürəti və təhlükəsizliyi baxımından xüsusilə əlverişli olmayan üsullar istifadə olunur.

Verilənlərin kvant ötürmə sistemlərinin əsas protokolları

BB84 protokolu

BB84 protokoluna əsasən, gizli açar aşağıdakı üsullarla yaradılır:

1. Alice fotonların müvafiq polyarizasiyasından istifadə edərək bu məlumatı kodlaşdırır, təsadüfi bit ardıcıllığı yaradır və təsadüfi seçilmiş bazislərin ardıcıllığından (çarpaz və ya üstəgəl) istifadə edərək onları Boba ötürür.

2. Bob təsadüfi seçilmiş bazisdən istifadə edərək hər bir qəbul edilmiş fotonun vəziyyətini ölçür.

3. Hər bir foton üçün Bob, ölçmənin nəticəsini gizli saxlayaraq, fotonun vəziyyətini hansı bazisdə ölçdüyünü açıq kanal vasitəsilə Alisanı məlumatlandırır.

4. Alice Boba açıq kanal üzərindən hansı ölçmələrin düzgün hesab edilməli olduğunu deyir. Bunlar ötürmə və ölçmə bazislərinin eyni olduğu hallardır.

5. Uyğun bazislərlə ölçmə nəticəsi bitlərə çevrilir, ondan açar əmələ gəlir [2; 4].

BB92 protokolu

BB92 protokolu 0 və 1-ləri təmsil etmək üçün iki fərqli istiqamətdə polyarizasiya olunmuş fotonlardan istifadə edir.

+450 istiqaməti boyunca qütbləşmiş fotonlar vahid bit haqqında, 0^o istiqaməti boyunca polyarizasiya olunmuş fotonlar sıfır bit haqqında məlumat daşıyır.

1. Alice bərabər ehtimallı iki qeyri-ortoqonal vəziyyətdən birində foton göndərir.

2. Bob ilkin vəziyyətlərə ortoqonal olan alt fəzalardan birinə proyeksiyadan istifadə edərək fotonların vəziyyətini ölçür. Eləcədə altfəzalar da bərabər seçilir. Əgər Alica 1 vəziyyətində bir fotonu göndərirsə və Bob isə bu vəziyyətə ortoqonal olan alt fəzaya proyeksiya etməklə onun vəziyyətini ölçürsə, o zaman yüz faiz ehtimalla fotonu qeydə almayacaq. Əgər o, başqa altfəza seçərsə, o zaman müəyyən bir ehtimalla sıfır vəziyyətini alacaq və Alisanın fotonu hansı vəziyyətdə göndərdiyini biləcək.

3. Bob açıq kanal vasitəsilə Alisə hansı ölçmələrdə müsbət nəticə aldığını deyir.

4. Bütün digər verilənlər atılır, qalanları isə vəziyyətlərdən birinin vahidə, digərinin isə sıfıra uyğun olduğu bitlərin ardıcıllığı kimi şərh olunur.

5. Ötürmə kanalında dinləmənin yoxlanılması [2; 3].

EPR Protokolu

1. Üç qeyri-ortoqonal vəziyyət seçilir ki, digər vəziyyətlərin hər birinə proyeksiyada vəziyyətlərdən birində buraxılan fotonun aşkarlanması ehtimalları bərabər olsun. Deməli, polyarizasiyadan istifadə edilərsə, bu vəziyyətlər 0, $\pi/3$, $2\pi/3$ bucaq altında polyarizasiya olunmuş olacaqdır.

2. İşıq mənbəyi bu üç vəziyyətdən birində eyni dərəcədə ehtimal olunan bir-birinə bağlı foton cütləri yaradır.

3. Alisa və Bob daxil olan fotonları eyni vaxtda və müstəqil ölçürlər. Hər kəs ixtiyari və bərabər şəkildə, ehtimal ki, proyeksiyada fotonu ölçməyə çalışacaq vəziyyəti seçir.

4. Alisa fotonun aşkarlanmasını "1", yoxluğunu isə "0" olaraq yazır. Bob bunun əksini edir.

5. Açıq kanal vasitəsilə fotonun gəlişini hansı bazada ölçdüklərini bir-birlərinə xəbər verirlər. Bazislərin üst-üstə düşdüyü ölçmələrdən bir açar əmələ gəlir. Qalan ölçmələrdən kanalda dinləməni aşkar etmək üçün istifadə olunan köməkçi açar formalaşır.

Goldenberg-Waydman protokolu

Goldenberg-Waydman protokolunda istifadəçilər Alisa və Bob əlaqə qurmaq üçün müvafiq olaraq "0" və "1" bitlərini kodlayan iki ortoqonal vəziyyətdən istifadə edirlər. Qoldenberq-Vaydman protokolunda iki vəziyyətin hər biri iki a və b lokallaşdırılmış normallaşdırılmış dalğa paketinin superpozisiyasıdır ki, onu göndərən Alisa müxtəlif uzunluqlu iki kanal vasitəsilə məlumatı alıcı Bob-a göndərir. Nəticədə, Bob dalğa paketlərinə müxtəlif zaman anlarında malik olur.

Kvant sisteminə təhrifləri təkcə casus deyil, həm də adi maneələrin edə bildiyi nəzərə alaraq, səhvləri etibarlı şəkildə aşkar etmək üçün bir yol lazımdır. 1991-ci ildə Çarlz Bennet kvant kanalı ilə ötürülən məlumatlarda təhrifləri aşkar etmək üçün bir alqoritm hazırladı. Yoxlamaq üçün bütün ötürülən məlumatlar eyni bloklara bölünür, sonra məlumatı göndərən və qəbul edən müxtəlif yollarla bu blokların paritetini hesablayır və nəticələri müqayisə edirlər. Hesab edilir ki, açardakı xətaların səviyyəsi 11 faizdən azdırsa, o zaman rabitə xəttinin təhlükəsizliyinə zəmanət vermək olar [1; 3; 4].

Praktiki tədbiqlər

1989-cu ildə Bennett və Brassard öz konsepsiyalarını sınaqdan keçirmək üçün IBM şirkətinin Araşdırma mərkəzində qurğu tikdilər. Bu qurğu, bir ucunda Alisanın ötürücü aparatı, digərində isə Bobun qəbuledici aparatı yerləşən kvant kanalı idi. Qurğular 1,5 × 0,5 × 0,5 m ölçüdə işıq keçirməyən korpusda təxminən 1 m uzunluğunda optik skamyada yerləşdirilmişdi. Sistem qanuni istifadəçilərin və təcavüzkarın proqram nümayəndəliklərinin yükləndiyi kompüterdən istifadə etməklə idarə olunurdu.

Qurğunun köməyi ilə aşağıdakıları aydınlaşdırmaq mümkün oldu:

- kvant məlumatlarının qəbulu və ötürülməsi, hətta hava kanalı vasitəsilə də tamamilə mümkündür;
- qəbuledici ilə ötürücü arasındakı məsafənin artırılması zamanı əsas problem foton qütbləşməsinin saxlanılmasıdır;
- ötürmə sirrinin təhlükəsizliyi ötürülmə üçün istifadə olunan işığın yanıb-sönməsinin intensivliyindən asılıdır: zəif yanıb-sönmələr tutulmaları çətinləşdirir, lakin qanuni alıcıda səhvlərin artmasına səbəb olur, yanıb-sönmə

intensivliyinin artması isə ilkin tək fotonu iki yerə bölməklə məlumatı tutmağa imkan verir.

2001-ci ildə vahid fotonların buraxılmasına imkan verən lazer işıq diodu hazırlanmışdır. Bu, qütbləşmiş fotonları daha böyük məsafəyə ötürməyə və ötürmə sürətini artırmağa imkan vermişdir. Təcrübə zamanı yeni işıq diodunun ixtiraçıları olan Endryu Şilds və onun TREL və Kembric Universitetindəki həmkarları ötürülmə zamanı fotonların yarıdan çoxunun itirilməsinə baxmayaraq, açarı 75 kbit/s sürətlə ötürməyə nail ola bilmişlər.

2003-cü ildə kvant kriptoqrafiyası sahəsində tədqiqatlara Toshiba şirkəti də qoşuldu. Şirkət 2013-cü ilin oktyabrında ilk sistemi təqdim etdi və 2014-cü ildə 34 gün ərzində standart optik lif üzərindən kvant açarlarının stabil ötürülməsinə nail olmaq mümkün oldu. Təkrarlayıcı olmadan fotonların ötürülmə məsafəsi maksimum 100 km idi. Kanaldakı itkilərin və maneələrin səviyyəsi xarici təsirlər nəticəsində dəyişə bildiyindən qurğunun işinin uzun müddət yoxlanılması vacib idi [1; 2; 4].

Kvant kriptoqrafiyasının mümkün sındırılma variantları

Kvant kriptoqrafiyasının imkanları əksər hallarda məlumatı ələ keçirən tərəfi problemsiz olaraq aşkarlamağa imkan verir, lakin buna baxmayaraq, indiki tərəqqi sürətində hər il bunun üçün daha çox səy tələb olunur. Cədvəldə nəzərdən keçirilən hücumlar içərisində sellivari fotodetektorların "kor edilməsi" üsulu ilə hücum daha çox maraq doğurur. Burada ələ keçirən tərəf tamamilə diqqətdən kənarda qalır ki, bu da kvant kriptoqrafiyasının müəyyən çatışmazlığı - ötürən və qəbul edən tərəflərin identifikasiyasının aşağı dəqiqliyi ilə bağlıdır. Bu problem kanal vasitəsilə və avtomatik olaraq onların biometrik şəkillərinin kiçik nümunəsinin köməyi ilə həll edilə bilər [1].

Cədvəl:

Kvant kriptoqrafiyasının sındırılması üçün hücum növləri

<table>
<tr><td rowspan="2">I. Fotonların vəziyyətinə olan hücumlar</td><td>1. Koherent
Eva bir sıra kubitlərlə qarşılıqlı əlaqədən istifadə edir.</td><td rowspan="2">2.1. Tutucu-retranslyator</td><td rowspan="2">2.2. Simmetrik hücumlar və kvant klonlaşdırılması prosesindən istifadə etməklə hücumlar</td></tr>
<tr><td>2. Qeyri- koherent
Onlar məlumatın silinməsini həyata keçirmək üçün hər bir kubitlə (açarın biti haqqında məlumat daşıyan foton) qarşılıqlı əlaqənin baş verdiyi təcavüzkarın belə bir hərəkətini nəzərdə tuturlar.</td></tr>
</table>

	3. Kombinə edilmiş hücumlar		
II. Kvant sisteminin avadanlığına olan hücumlar	**1. İşıq bölüşdürücüsünün köməyi ilə hücum** Verilmiş hücumun həyata keçirilməsi kvant sxemlərində multi faton şüalanma mənbələrindən istifadə etməklə baş verir.		
	2. Güclü impulsla hücum Klassik mənada "Troya atı" hücumlarına bənzəyir. Əsas aşarın bitlərini idarə etmək və müvafiq məlumatları əldə etmək üçün sistem zəifliklərindən, nasazlıqlardan və ya sistemin vəziyyətinin skan edilməsindən istifadə edir.		

Hücumun əsas sxemlərinin kubitlərin vəziyyətinə təsirinin təhlili

Tutucu-retranslyator strategiyası

Bu strategiya kvant rabitə kanalında məlumatı tutmağın ən sadə və mümkün yollarından biridir. Eva hər bir kubitin vəziyyətini Bob kimi müəyyən edir, lakin Boba öz vəziyyətinə görə (düzgün və ya yanlış) müəyyən dərəcədə ehtimalla mövcudluğu qeydə alınmayan başqa bir kubit göndərir.

Cinayətkar kubitlərin retranslyasiyası taktikasından istifadə edir.

Simmetrik hücum

Hücumun bu variantı qarşısına hər kubit üçün müvafiq nümunələrin qarşılıqlı əlaqəsi vasitəsilə hücumu məqsəd qoyur. Qarşılıqlı təsirdən sonra kubit daha uzağa - Bob stansiyasında qəbul edən tərəfə göndərilir və vəziyyət Alisanın kvant yaddaşında saxlanılır. İstifadə olunan qarşılıqlı əlaqə rabitə kanalına əhəmiyyətli dərəcədə təhriflər gətirməməlidir. Təcavüzkar nümunələrin vəziyyətini ölçür və adətən, strategiyanın bu şəkildə həyata keçirilməsi ilə səhvin səviyyəsi açarın uzunluğunun 15% -ni təşkil edir.

Koherent hücumlar

Bu hücumların həyata keçirilməsi simmetrik olan hücumlara bənzəyir. Yeganə fərq ondan ibarətdir ki, Eva bir kubit məlumatdan deyil, bütün ardıcıllıqdan nümunələr götürür. Bu halda, böyük həcmli bir nümunə saxlanılır, lakin yalnız Alisa və Bob arasında məlumatların uyğunlaşdırılması prosesindən sonra təhlil edilir. İnformasiyanın koherent üsulla çıxarılması zamanı səhvlərin dərəcəsi açar uzunluğunun 11%-ni təşkil edir [2].

Kvant sisteminin avadanlığına hücumlar

Şüa bölücüsü vasitəsilə hücum

Eva bütün impulsları iki hissəyə bölərək onların hər birini tərkibində 0, 1 və 2 fotonlu impulsları ayırd edə bilən foton sayma cihazlarından istifadə edərək iki əsasdan birində təhlil edir. Bu taktika çox sayda paralel birləşmiş tək foton sayğacından istifadə etməklə həyata keçirilə bilər.

“Troya atı” hücumları

“Troya atı” tipli hücumlar optik multipleksor vasitəsilə iki ötürücü stansiyaya (ya Alisaya, ya da Boba) doğru impulsun skan edilməsi yolu ilə həyata keçirilir. İmpuls sistemin elementlərindən əks olunur və təcavüzkara geri ötürülür və dekodlaşdırma sxeminə daxil olur.

Eva çox həssas dedektəetmə metodundan istifadə edir. İmpuls iki hissəyə bölünür: əsas və dayaq. Bu sxem sinxron dedektəetmə üçün lazımdır. Siqnalın skan edilənlə sinxron gəlişi üçün dayaq siqnalının gecikməsi lazımdır. Bu əks olunacaq və təcavüzkarın qəbul etdiyi məlumatı təyin edəcək impulsin parametrləridir. Multipleksorun funksiyası ötürülən fotonları təhrif etməməkdir.

Saxta vəziyyətlərlə hücumlar

Məhz bu hücum növü rusiyalı mütəxəssis Vadim Makarovun rəhbərlik etdiyi norveçli tədqiqatçılardan ibarət artıq adı çəkilən komanda tərəfindən həyata keçirilib. Nəzarət 1-10 mVt və 780 nm dalğa uzunluğunun işıq impulsları sayəsində həyata keçirilə bilər.

İmpulslarla hücum fotodiodları gələn fotonlara qarşı qeyri-həssas edəcək. Eva görünməz qalaraq məlumatı toplamaq və siqnalı təkrar ötürmək iqtidarındadır. Hakerlər yalnız təxminən 70 kHz tezliyi olan parazit impulslar verə bilirlər [3; 5].

İnformasiyanın mühafizəsinə yeni yanaşma

Bildiyimiz kimi, əlçatmaz hesab edilən kriptoqrafiya sistemi son zamanlar yeni texnologiyaların inkişafı ilə əlaqədar olaraq getdikcə daha az mühavizə olunan bir sistemə çevrilir. Ancaq yenə də ümid var ki, məlumatı kimsənin ələ keçirəcəyindən qorxmadan ötürmək mümkün olacaq. Bu ümid stenoqrafiyadır.

Stenoqrafiya, verilənlərin ötürülməsi faktının gizlədildiyi şifrləmə üsuludur. Bu üsul müasir rabitə təhlükəsizliyi sistemlərində istifadə olunan kriptoqrafik alqoritmlərin mövcud sistemlərini tamamlayır. Bu, kompüter texnologiyasının inkişafı sayəsində mümkün olmuşdur. Kvant kompüterlərinin meydana çıxması ilə kubit səviyyəsində kvant rabitə kanalı ilə ötürülən informasiyaya konteynerləri daxil etmək mümkündür. Bu halda kubitlər semantik məna qazanır. Biz təkcə Bobdan Alisaya məlumat ötürmürük, lakin biz kvant kanalında informasiya axınına lazımi (gizli) konteyneri daxil edirik [1].

Nəticə

Kvant kriptoqrafiyasını həyata keçirən qurğunun köməyi ilə kvant məlumatlarının qəbulu və ötürülməsi hətta hava kanalı vasitəsilə də mümkün olur. Bu zaman qəbuledici ilə ötürücü arasındakı məsafənin artırılması əsas foton qütbləşməsinin saxlanılması problemi meydana çıxır. Bu sistemlərdə ötürmə sirrinin təhlükəsizliyi ötürülmə üçün istifadə olunan işığın yanıb-sönməsinin intensivliyindən asılı olur. Belə ki, zəif yanıb-sönmələr qəbulu

çətinləşdirir, qəbulda səhvlərin artmasına səbəb olur. Yanıb-sönmə intensivliyinin artması isə vahid fotonu iki yerə bölməklə məlumatı təhrifsiz qəbul etməyə imkan verir.

Kriptoqrafiya sistemi son zamanlar yeni texnologiyaların inkişafı ilə əlaqədar olaraq getdikcə daha az mühavizə olunan bir sistemə çevrilməkdədir. Ancaq stenoqrafiya sayəsində məlumatın təhlükəsiz ötürülməsi perspektivləri daha inandırıcıdır.

Kvant kriptoqrafiyası hazırda informasiyanın ən böyük mühafizəsini təmin etsə də, belə mühafizə metodunun istifadəsi bahalı avadanlıq və məlumatların uzaq məsafəyə göndərilməsinin mümkünsüzlüyü səbəbindən nəinki əlverişsizdir, həm də məlumatların tam mühafizəsini təmin etmir.

ƏDƏBİYYAT

1. *Серикова Ю.И., Малыгина Е.А.* Уязвимости криптографических систем с различными протоколами квантового распределения ключа и ключевая роль биометрии в квантовой криптографии // Universum: Технические науки : электрон. научн. журн. 2017. № 11(44) .
2. *Юргин Д.Ю., Макаров А.М.* Уязвимости каналов квантового распределения ключей. 2010, 211 с.
3. https://www.kaspersky.ru/blog/kvantovye-kompyutery-i-konec-bezopasnosti/1989/
4. https://habr.com/ru/companies/toshibarus/articles/444502/
5. https://www.youtube.com/watch?v=IJhGeMYSnVY

Redaksiyaya daxil olub: 23.02.2023