Компарација и можности на QKD техники

Томислав Шуминоски[1], Маја Кукушева[2], Митко Богданоски[3] , Александар Ристески[4]

[1,2,3,4] Универзитет „Св. Кирил и Методиј“, Факултет за Електротехника и Информациски Технологии, Карпош 2 бб, 1000 Скопје, Република Македонија, [1] tomish@feit.ukim.edu.mk, [2] maja.kukuseva@gmail.com, [3] mitko.bogdanoski@gmail.com, [4] acerist@feit.ukim.edu.mk.

***Апстракт* — Во овој труд се разгледани современите Техники за дистрибуција на квантен клуч (Quantum Key Distribution) во областа на сигурносните комуникации, кои претставуваат еден огромен чекор напред во развојот на криптографијата и безбедносните комуникации воопшто. Со невидениот развој на квантната физика, преку самата дистрибуција на квантен клуч кој е речиси невозможно да се пробие со класичните технологии, се јавија низа нови можности, особено во сферата на криптологијата. Даден е и осврт на актуелните QKD принципи и уреди со конкретна компарација помеѓу QKD техниките. Претставени се и новитетите и можностите на истите преку низа на експерименти и апликации каде што се употребуваат.**

***Клучни зборови* —Фотон, Quantum bit (Qubit), Quantum Key Distribution (QKD), сигурносни комуникации и др.**

1. ВОВЕД

Поради огромниот напредок на квантната физика, и пред сè поради брзиот развиток на квантната криптографија, техника кој ги користи принципите на квантната механика и Хајзенберговиот принцип на неопределеност, се разви еден нов аспект во современите телекомуникациски области, преку појавата на дистрибуција на квантен клуч. Овој нов вид на дистрибуција на сигурносен клуч воведе невидена сигурна и доверлива комуникација помеѓу крајните корисници и барем за сега, отпорност од било какви напади од трета страна.

Токму поради тоа, во рамките на овој труд ќе бидат анализирани и споредени различните техники на QKD (Quantum Key Distribution), со посебен осврт кон апликациите во кои можат истите да бидат применети. Самата квантната криптографија своите зачетоци ги има со предлогот за истата од постдипломецот на Универзитетот во Колумбија во Њу Јорк, Стивен Вајзнер, во раните 1970-ти години. Тој го претставил концептот на квантно конјугирано кодирање, но неговиот труд “Конјугирано кодирање” бил одбиен од списанието IEEE Information Theory, за сепак подоцна, во 1983 година, истиот да биде публикуван во списанието SIGACT. Од друга страна, самите почетоци на QKD датираат од експериментите на Бенет и Брасард во раните 1980 години, преку BB84 протоколот [1].

Иако е предвидено сите осум нивоа според OSI моделот да бидат квантни, сепак „квантноста“ на нивоата, до сега, е имплементирана до третото ниво. Тоа значи дека имаме квантно прво (преку изворите на единечни фотони, квантните логички порти, квантната меморија и сл.), второ (квантната проверка на парност, рипитерите) и трето ниво (дел од посложените четири-qubit-ните кодови за корекција на грешка на заглавија).

Трудот е организиран на следниот начин: во глава II е даден осврт на актуелните QKD техники, додека во III глава е дадена споредба на истите. Понатака, во глава IV се прикажани некои од поактуелните апликации и експерименти во кои се применува QKD и на крај во глава V е даден заклучокот за перформансите на QKD и квантната криптографија.

2. ОСВРТ НА QKD ТЕХНИКИТЕ

Во рамките на оваа подглава ќе бидат објаснети основните принципи и уреди при QKD и ќе биде даден осврт на главните техники на самата QKD. Во таа насока, за да можат да се разберат основните принципи на размената на квантниот клуч, на Сл.1 е дадена една поедноставена шема на QKD. На истата може да се забележи дека во рамките на еден линк во кој што се дистрибуира квантниот клуч, постојат два вида на канали: канал за размена на квантниот клуч и класичен канал за комуникацијата која следува после размената на квантниот клуч. При ова, Алиса и Боб (од сега па натаму вака ќе ги означуваме двете валидни страни на комуникација) се поврзани на уредите за QKD, додека Ева (натрапникот или напаѓачот на QKD линкот)

прислушкува. Самите елементи на овие QKD уреди се доста сложени, па нивна детална разработка би ги надминала границите на овој труд. Од тие причини ќе ги објаснеме само принципите на нивното функционирање и истите накратко ќе ги опишеме. Имено, самите операции во овие уреди имаат квантната логика и може да се каже дека тие се есенцијално нелинеарни по самата своја природа, бидејќи еден qubit ја управува состојбата на друг qubit и се доста сложени и меѓусебно поврзани со сложени равенки кои владеат во квантниот свет [2].

Генерално земено, фотоните (генерално земено, нивната поларизација или состојба) се земаат како главните единици на квантната информација, т.н. qubit-и. Според тоа, главните уреди кои се употребуваат при QKD имаат оптичка природа, што за нијанса ни ја поедноставува проблематиката и меѓу другото во нив како поглавни се среќаваат: изворите на поединечни-фотони (single-photon source), квантните логички порти, квантната меморија и репитерите.

Така, како суштински елемент од QKD се имплементирање на квалитетни и стабилни по состојба single-photon извори (извори на поединечни фотони). Како најпопуларен од овие извори се јавува параметарскиот down-conversion уред, кој на многу наврати се смета за идеален генератор на единечни фотони (според [2]). Како што е прикажано на Сл. 2, врз самиот нелинеарен кристал, пулсирачкиот ласерски зрак индицира појавување на парови од фотони. На тој начин, доколку се детектира еден член од парот на фотони, тоа ќе сигнализира присуство на друг фотон од истиот пар. При тоа, со цел да се зачува истоимениот фотон во оптичката мемориска јамка (јамка за доцнење) сè додека е тоа потребно, т.е. се дотогаш кога ќе треба да се пушти од мемориската јамка на самиот излез, се користи оптичкиот комутатор со голема брзина. Сепак, овој вид на извор на единечни фотон не може да произведува фотони било кога т.е. истиот продуцира фотони на одреден специфичен временски интервал, па заради тоа може да се употреби синхронизација со референтен временски часовник на квантниот компјутер, кој и онака е неопходен за беспрекорно функционирање на практичните апликации. Освен горенаведениот извор, како еден од најновите високо ефикасни, испитани single-photon извори е и изворот прикажан во [3]. Истиот спаѓа во групата на полупроводнички quantum dot (QD) извори, лоцирани внатре во фотонската жица.

Сл. 1- Илустрација на шема за QKD

Сл. 2 - Илустрација на шема од single-photon извор со parametric down-conversion (PDC)

Овој извор се разликува од останатите single-photon извори од оваа област по тоа што има одлично каплирање (coupling > 95%) на QD спонтана емисија, колекцијата на единечни фотони е ефикасна со над 80 % со 0,5 нумерички отвор (нумеричката апертура е добиена со користење на Bragg-ово огледало на дното од инженерираниот photonic wire и заостреност од нано-бранов тип). Истовремено овие single-photon извори се далеку подобри според перформансите од претходните стандардни single-photon извори.

Освен фотонските извори, други суштински елементи се логичките квантни порти (некаде сместени на Layer 2 ниво според OSI моделот), базирани на линеарната оптика. Истите одат во комбинација со оптички мемориски јамки (optical storage loops) за да се имплементираат уреди за квантна меморија за еден фотон [4,5]. И овде, заради фотонската дефиниција на qubit-ите, неизбежно се јавуваат нелинеарни оптички ефекти, кои се карактеристични за зраци со висок интензитет на светлина во нелинеарни материјали. Сепак и во овие случаи може да се моделираат веројатносни квантни логички операции со помош на користење на линеарни оптички елементи, дополнителни фотони (помошни) и пост-селекција врз база на измерените резултати направени на помошните фотони (според Knill, Laframme и Milburn во [6]).

Основната идеја на линеарните оптички порти е прикажана во [1], каде имаме два qubit-и (два поединечни фотони), како влез во уредот и два qubit-и кои излегуваат, кои ја имаат поминато посакуваната логичка операција. Дополнително, имаме одреден број на помошни и контролни фотони кои што влегуваат во самиот уред, за контрола. Самата квантна состојба на двата дополнителни контролни qubit-и (фотони) се мери откако ќе го напуштат уредот и на тој начин, со помош на пост-селекција врз база на овие мерења, се проектира и одредува точната состојба на двата излезни qubit-и. Од мерењата на состојбите од помошните qubit-и произлегуваат следните три можни случаи:

i. Откако ќе се добијат конкретните резултати, се знае дека логичката операција била исправно имплементирана и излезот од уредот се прифаќа без измени.
ii. Откако ќе се добијат други мерни резултати, излезот од самиот уред е некоректен (погрешен), но сепак може да се поправи на добро познат начин со користење на корекции во реално време

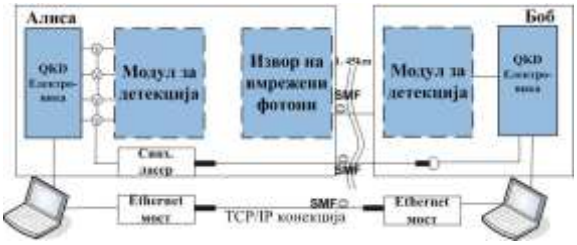
(познати како feedforward контрола дадени во [7]).

iii. Доколку се добијат било какви други резултати, излезот од уредот се смета за неисправен и истиот не може да се поправи користејќи feedforward контрола.

Сите останати настани кои не спаѓаат во горенаведените три случаи се отфрлаат и се сметаат како неуспешни. Веројатноста дека ќе се појават вакви неуспешни настани може да се скалира со $1/n$ или со $1/n^2$, во зависност од пристапот кој се користи. Како најкористен модел на вакви порти се користат познатите варијанти на контролирана NOT (Controlled NOT, т.е. CNOT) квантна логичка порта [2].

Од друга страна, овие CNOT квантни логички порти се есенцијален дел од репитерските системи (repeaters). Имено, самиот квантен репитер се состои од секвенца на кола (во кои има вакви CNOT порти) за корекција на грешки при преносот, одделени со оптички кабли со доволно кратки растојанија еден од друг, така што веројатноста од апсорпција на два или повеќе фотони на тоа растојание (на која се одделени различните степени во каскадата од овие уреди) е незначително мала. Друг начин е оптичките кабли да се групираат во множества од јамки, за да може да се креира квантен мемориски уред. На тој начин, колата за корекција на грешка би ги ублажувале фотонските загуби и би го зголемиле времето на чување на истите (за подетални информации може да се види [5]). По теорија, доколку имаме одреден идеален квантен репитер, истиот би бил способен да ги исправи сите форми на грешки кои што се јавуваат од најразлични причини при самата трансмисија на фотони низ оптичкиот кабел (вклучувајќи ги тука фазните грешки и битските грешки). Но, од практична гледна точка, најдоминантни грешки во самиот оптички кабел кај QKD системите се јавуваат поради загубите на фотони заради апсорпција или scattering. Во сите други случаи грешките од друг вид немаат никакви мерливи влијанија на тие фотони кои поминале низ оптичкиот кабел при големи апсорпциска рата. Квантни репитер се од особена важност во квантните free-space системи, со цел да се постигне посакуван опсег (бидејќи нивниот опсег е доста ограничен) и да се прошири областа на оперирање.

Факт е дека полето на квантна комуникација се повеќе се развива со нови уреди, шеми и техники кои овозможуваат генерирање и манипулација со вмрежени парови на фотони Со овие шеми се зголемува растојанието кое може да се достигне при комуникацијата, па затоа многу апликации користат криптографија базирана на вмрежување на фотоните. Една од главните придобивки е наследувањето на случајноста при кванто-механичките мерења на вмрежените фотони која води до добивање на случајни клучеви. Квантната телепортација зависи од две компоненти: вмреженоста и анализа на Беловата состојба.



Сл. 4 - Илустрација на шема за квантна криптографија базирана на вмрежување

Квантното вмрежување е својство кое ја опишува нераздвојливата состојба на одвоени системи, односно фотоните остануваат поврзани дури и ако се одделени на големи растојанија. Според ова, состојбата на еден фотон не може да се определи без да се знаат состојбите на останатите вмрежени фотони. Од друга страна, анализата на Беловата состојба се однесува на способноста да се анализира состојбата на два фотона во зависност од состојбата на вмрежување. Во квантните мрежи најчесто се користи концептот на замена на вмрежувањето. Ако разгледаме два пара од вмрежени фотони и извршиме Белови мерења на два од фотоните, по еден фотон од двата пара, ќе се постигне вмреженост на останатите два фотона, дури и ако тие фотони претходно не биле во интеракција меѓу себе и не потекнуваат од ист извор.

Овој концепт е од големо значење при воспоставување на линкови за комуникација на големи растојанија и се користат за воспоставување на вмреженост помеѓу оддалечените работни станици.

Прототип на систем за пренесување на квантен клуч базиран на вмрежување е предложен во [8], кој е развиен од Austrian Research Centers Seibersdorf (ARCS). На Сл. 4 е прикажан овој систем, кој се состои од преносliв извор на поларизирани вмрежени фотони и два модули за детекција на фотони. Вмрежените фотони се генерираат од ласер диода од виолетов GaN, од кој се добиваат континуирани бранови. Овие бранови понатаму се одвојуваат од нелинеарниот β-бариум боратов кристал. Фотоните, пред да се спојат во мономодното оптичко влакно, се пропуштаат низ леќа и филтер на виолетова боја кој ја блокира расејувачката УВ светлина. Изворот произведува парови од фотони од кој едниот фотон се анализира локално од модулот за детекција на Алиса, а другиот преку мономодно оптичко влакно се испраќа на растојание од 1,45km до Боб. Мерењата се извршуваат со една од двете основи (0^o и 45^o) со помош на сплитер на зрак, кој случајно ги испраќа фотоните до еден од двата поларизациски сплитери на зрак. Крајната детекција се извршува пасивно, со загушување на силиконската лавинска фотодиода. Кога фотон се детектира од една од четирите фотодиоди на Алиса, се креира оптички импулс, кој преку секундарното оптичко влакно се испраќа до Боб.

Овој импулс се користи за да се воспостави заедничка временска база. На двете страни, овие импулси и резултатот од детекцијата на фотодиодата се пренесуваат до генераторот на квантен клуч (QKD) за понатамошно процесирање. Денес, развивањето на квантната комуникација се насочува кон достигнување на се поголеми растојанија. Втора техника со која се постигнуваат поголеми растојанија од вмрежената на фотоните е квантна комуникација во слободен простор. Приемникот и предавателот имаат најмалку два телескопа кои се користат за испраќање на фотоните на поголеми растојанија. Меѓутоа, на растојанија поголеми од 100km сигналот значително ослабнува. Класичните оптички импулси со кои се преставени „1“ и „0“, при пропагацијата низ оптичката мрежа се засилуваат со регенератори или засилувачи, со што се зголемува растојанието кое можат да го достигнат. Меѓутоа, во квантната криптографија многу е тешко да се засили состојбата на поларизација на еден фотон, па затоа квантните репитери се многу посложени. Понатаму во трудот се приложени некои експерименти каде детално е опишана опремата која се користи.

Како што кажавме, цел на квантна криптографија е да се покријат сите растојанија на глобално ниво. Земјините линкови во слободен простор страдаат од пречки од околните објекти во линија на видливоста, слабеење поради временските услови, атмосферски турболенции и деформации на Земјата. Поради тоа, истите се лимитирани на кратки растојанија. Во отсуство на добри квантни репитери, големи растојанија се постигнуваат само со употреба на сателити. За да се достигнат растојанија поголеми од 100km се користат Low-Earth-Orbit (LEO) сателити, кои се поставуваат на висина од 300km до 500km од површината на Земјата. На поголеми растојанија, поради ефектот на дифузија кој сè повеќе доаѓа до израз, се среќаваат се поголеми ограничувања. Затоа, за квантна комуникација се користат Geo-Stationary Orbit (GEO) сателити. За да се воспостави квантна комуникација помеѓу сателитот и Земјината работна станица, потребен е само еден оптички линк. Квантната криптографија може да се овозможи дури и со користење на протоколот BB84, при што се генерира сигурен клуч. Ако терминалот генерира друг клуч со друга Земјина станица која се наоѓа на произволно растојание од неа, за да се воспостави таен клуч помеѓу нив е доволна класичната комуникација.

3. СПОРЕДБА НА QKD ТЕХНИКИ

Овде следат споредбите и табелите за основните техники за дистрибуција на квантниот клуч. Во Табела 1 е приложена споредбата на квантна криптографија со вмрежување на

ТАБЕЛА 1
СПОРЕД БА НА QKD ТЕХНИКИТЕ

Техника / Својство	Вмрежување на фотони	Слободен простор
Брзина на пренесување на клуч	80bps	35bps
Растојание	до 100km	500m-500km
QBER	8%	5,7%
Сложеност на шема	Да	Да

фотоните и квантната комуникација во слободен простор. После исправката на грешките и засилувањето на приватноста, просечната брзина на пренесување на клуч со користење на техниката со вмрежени фотони достигнува вредност до 80 бити/секунда [2]. Оваа вредност најчесто е ограничена од слабеењето во квантниот канал, ефикасноста на детекција во фотодиодата и електрониката. Додека пак, ако се користи квантна комуникација во слободен простор и ако се земат во предвид реалните можности за корекција на грешките, тогаш сигурен клуч може да се пренесува со брзина од 35 бити/секунда на растојанија до 100km. Поради сложеноста на репитерот, кој се користи за засилување на поларизацијата на фотонот, и со двете техники се достигнуваат мали растојанија. Техниката со вмрежување на фотоните достигнува сигурно пренесување на клучот до растојанија од 100km, додека со техниката во слободен простор се достигнуваат растојанија до 500km.

Меѓутоа, цел на квантната криптографија е да се достигне глобално покривање и да се достигнат многу поголеми растојанија. Затоа, квантната криптографија во слободен простор, во отсуство на добри квантни репитери, се комбинира со сателитите, при што се достигнуваат многу поголеми растојанија до кој има сигурен пренос на клучот. Од сево ова, следува дека и шемите на двете технологии се доста сложени и се изградени од голем број на елементи (електроника, модули за детекција, извор на вмрежени фотони итн.)

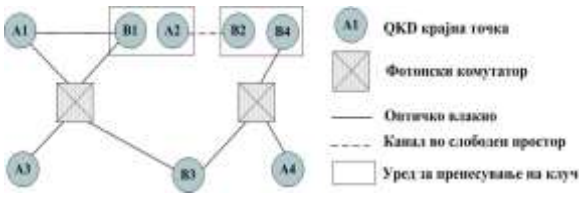
4. АПЛИКАЦИИ И ЕКСПЕРИМЕНТИ

Последните години развиени се многу апликации на квантната криптографија, како: повеќестрано квантна тајна размена [9], квантна криптографска мрежа [10] и особено внимание се посветува на QKD апликациите во оптичките безжични комуникации, кои се фокусирани на безбедносните проблеми [11]. Во споредба со класичната, квантната криптографија може да обезбеди независна безбедност. Како што веќе споменавме претходно, квантната криптографија се базира на карактеристиките на квантниот механизам, што вклучува неклонирачка теорема, квантно поврзани состојби и квантна телепортација. За да се разгледаат испраќачот и

примачот, може да телепортираме непозната квантна состојба со цел нивна за нивна меѓусебна верификација. Овде како еден позначаен протокол за безбедност би го издвоиле протоколот за квантни безбедни безжични комуникации [12]. Предноста на овој протокол се состои во тоа што користи споделени табели (нанапред и во обратна насока од текот на информациите) за квантна распределба како таен квантен клуч. Притоа, неговиот двонасочниот механизам има намена да ги испитува нападите врз каналот и други злонамерни напади, при што дизајнира многу мерки за проверка како детектирачка технологија, сè со цел да се одбрани не само од нападите врз комуникацискиот канал, туку и од напади на злонамерни јазли-посредници. Овој протокол може да постигне мала можност за измама и воспоставува безбедна рутирачка патека. Како резултат на тоа, може со сигурнсост да се телепортира квантна состојба од Алиса до Боб, а доказ за тоа се низа на измерени експериментални резултати кои може да се најдат во [12]. Секако дека опасноста не се елиминира потполно со примената на горенаведениот протокол, туку се продолжува со истражување на нови безбедносни механизми таму каде QKD системите се најслаби.

Од друга страна, се оди чекор напред со нудењето на нови апликации и сервиси, токму со развивањето на квантна комуникација во слободен простор, при што се комбинираат слободниот простор и оптиката. Еден од првите експерименти бил изведен во Данабу, Австрија, каде било демонстрирано пренесување на парови од вмрежени фотони на растојание над 600 метри [2]. Поголеми растојанија биле достигнати во експериментот кој бил извршен меѓу Ла Палма (Канарските Острови) и Тенерифе (Шпанија), кои се на растојание од 144km [13]. Поларизираните парови на вмрежени фотони биле генерирани од ласер кој емитува светлина со бранова должина од 355nm. Едниот фотон локално се детектира од Алиса, а другиот се испраќа на растојание од 144km преку слободен простор до Боб (Тенерифе). Меѓутоа, меѓу првите позначајни експерименти на поголеми растојанија биле постигнати со експериментот над Виена [2]. Изворот на фотони бил сместен во опсерваторијата Kuffner Stenwarte. Трансмитерот Алиса е исто сместен во оваа опсерваторија и се состои од мономодно оптичко влакно кое е каплирано со изворот на вмрежените фотони и телескоп за испраќање. Боб се наоѓа на растојание од 7,8km и е сместен на 46 кат од облакодерот Millennium Tower. Алиса користи четири канален детектор кој е изграден од 50.50 сплитер на зрак, полубранова рамнина и поларизиран сплитер на зрак и има за цел да ги мери фотоните од секој пар во мод А. По компресијата на поларизацијата, Алиса ги испраќа фотоните во мод В преку слободен простор до Боб. Боб има сличен четири канален детектор кој може да ја измери поларизацијата или во иста основа како Алиса или преку дополнително ротирање на полубрановата рамнина. Алиса и Боб користат временски карти за бележење на кои ги запишуваат моментите кога се случиле детекциите. Исто така, тие користат и глобален систем за позиционирање (GPS) за да се добие нула офсет за нивните временски податочни низи. Боб своите временски тагови до Алиса ги испраќа во блок, преку јавен Интернет. Меѓутоа, временскиот таг пренесува и информација за тоа кој од четирите канал бил употребен. Со ова, Алиса и Боб можат да ја определат корелацијата на поларизацијата помеѓу нивните коинцидентни парови. Но и покрај сите придобивки од традиционалниот QKD, сепак постојат и некои ограничувања. Традиционалниот QKD е лимитиран со растојанието кое може да се постигне, потоа може да се пренесува само низ еден физички канал (влакно или слободен простор, но не и низ двете истовремено), физички ранливости како што е кинењето на влакното итн. Според изнесеното, ако на пример дојде до кинење на оптичкото влакно, комуникацијата помеѓу Алиса и Боб прекинува. За да се надминат сите овие недостатоци, наместо да се користат самостојни QKD линкови се гради цела QKD мрежа. Првата мрежа за пренесување на квантниот клуч била дизајнирана и изградена од тим практиканти од Универзитетот Бостон и Универзитетот Харвард, под спонзорство на Defense Advanced Research Project Agency (DARPA), по што го добила и името. Оваа мрежа била пуштена во работа на 23 Октомври 2003 година, а до Декември 2004 година се состоела од 6 јазли, со можност за надградба до 10 јазли, а е прикажана на Сл. 5. DARPA [14] воедно е и првата метро мрежа, која обезбедува мрежна сигурност од крај до крај. Мрежата се состои од два кохеренти предаватели (Алиса и Ана), два компатибилни приемници (Боб и Борис) и 2x2 комутатор, кој го поврзува секој предавател со секој приемник. Како што е покажано на Сл. 5 Алиса, Боб и комутаторот се наоѓаат во BBN лабораторијата, Ана во Универзитетот Харвард (УХ) и Борис се наоѓа во Универзитетот во Бостон (УБ). Растојанието меѓу УХ и BBN е 10km, потоа растојанието УБ-BBN е 19km и растојанието УХ-УБ преку комутаторот е 29km.

Сл. 5 - Илустрација на првата QKD мрежа, DARPA



Сл. 6 - Илустрација на шема на QKD мрежа

Алиса содржи извор на фотони, модулатор и Mach-Zehnder интерферометар, а Боб пак, содржи модулатор, детектор на фотони, Mach-Zehnder интерферометар и фотодиода од InGaAs. Во оваа мрежа Алиса и Боб се QKD крајни точки. Алиса и Боб, парот (A1,B1), се директно поврзани преку влакно, додека пак, парот (A2, B2) е поврзан преку канал во слободен простор. Останатите парови се поврзани преку влакно и комутаторот. Па така, A1 или A3 може да се поврзе со B2 преку комутаторот. QKD мрежите работат до L3 според OSI, па со правилна употреба на QKD мрежниот протокол, јазелот A1 покрај тоа што може да се поврзе со своите директни соседи (B1 или B3), може да се поврзе и со јазлите кои се на неколку хопови. Илустрација на оваа QKD мрежа е дадена на Сл.6. Ако јазлите A1 и B4 се договорат за комуникација, таа комуникација ќе се одвива преку јазлите B1, A2 и B2. Фотонот од изворот во A1 се пренесува преку комутаторите и средишните јазли до дестинацијата B4, каде се врши мерењето. Во средишните јазли, меѓу изворот и дестинацијата, не се врши мерење на фотонот. Откако крајните точки ќе го договорат парот од клучеви, го користат за сигурна комуникација од хоп до хоп, при што енкрипцијата и декрипцијата се извршува само во крајните јазли. Откако се договорени клучевите, јазлите за комуникација меѓу себе го користат јавниот Интернет.

5. ЗАКЛУЧОК

Со воведувањето на QKD во комуникацијата значително се подобрува самата комуникација помеѓу крајните корисници и се подига на едно побезбедно и посигурно ниво.

Како што кажавме, цел на квантна криптографија е да се покријат сите растојанија на глобално ниво. Земјините линкови во слободен простор страдаат од пречки од околните објекти во линија на видливоста, слабеење поради временските услови, атмосферски турболенции и деформации на Земјата. Поради тоа, тие се лимитирани на кратки растојанија. Во отсуство на добри квантни рипери, големи растојанија се постигнуваат само со употреба на сателити. Исто така опишани се основните уреди, со посебен акцент на развојот на single-photon изворите. Така, изворот прикажан во [3] може ефикасно да се употреби на широко-појасните single-photon емитери (како што се F-центрите по потреба), токму заради тоа што неговата фотонска собирачка стратегија не го користи Purcell-овиот ефект. Покрај тоа, дадена е споредба меѓу актуелните QKD техники и видовме дека има низа на апликации каде што се употребуваат истите. Безбедноста особено е потенцирана токму преку протоколот [12] во квантната безжична комуникациска мрежа, каде што може да се постигне побезбедна рутирачка патека, со што значително ја подобрува безбедноста на повисоко ниво во рамките на безжичните мобилни мрежи, што е клучен аспект при самата комуникација воопшто.

6. РЕФЕРЕНЦИИ

[1] C.H. Bennett, F. Bessette, G. Brassard, L. Salvail, and J. Smolin, „Experimental quantum cryptography“, *J. Cryptology*, 5, 3, 1992; C.H. Bennett, G. Brassard, and A. Ekert, Quantum cryptography, *Sci. Am.*, 267, 50, 1992.

[2] Alexander V. Sergienko, „Quantum Communications and Cryptography“, CRC Press Taylor & Francis Group, New York, 2006.

[3] J.M. Gérard, N. Gregersen, T.R. Nielsen, J Claudon and J Moerk, “A novel high-efficiency single-mode quantum dot single photon source”, Viena, October 2008.

[4] J.D. Franson and T.B. Pittman, Proceedings of the fundamental problems in quantum theory workshop, D. Lust and W. Schleich, eds., Fortschritte der Physik, 46, 697–705, 1998.

[5] R.M. Gingrich, P. Kok, H. Lee, F. Vatan, and J.P. Dowling, Phys. Rev. Lett., 91, 217901, 2003.

[6] E. Knill, R. Laflamme, and G.J. Milburn, *Nature*, 409, 46, 2001.

[7] T.B. Pittman, B.C. Jacobs, and J.D. Franson, Phys. Rev. A, 66, 052305, 2002.

[8] T. Helleseth, “Secret-key reconciliation by public discussion”, ed. Vol. 765, Springer, New York, 1993, p. 410.

[9] Z Zhang, Y Li and Z Man, "Multiparty quantum secret sharing," Phys. Rev. A 71, 044301(2005).

[10] E. Biham, B. Huftner, and T. Mor, 'Quantum cryptographic network based on quantum memories," Phys. Rev. A, Gen. Phys., vol. 54, pp. 2651-2658, 1996.

[11] M. Gabay and S. Arnon, "Quantum key distribution by a free-space MIMO system," IEEE Joumal of Ughtwave Technology, vol. 24, no. 8, pp. 3114 - 3120, Aug 2006.

[12] Tien-Sheng Lin', Sy-Yen Kuo “Quantum Wireless Secure Communication Protocol”, IEEE Xplore, February, 2007.

[13] A. Zeilinger, “Long distance quantum cryptography with Entangled Photons”, IQOQI Institute for Quantum optic and Quantum Information, Austrian Academy of Sciences, Austria, 2007.

[14] C.Eliot, A. Colvin, D. Pearson, O. Pikalo, J. Schlafer, H. Yeh, "Current status of DARPA Quantum Network", 2007.