О КВАНТНОЈ КРИПТОГРАФИЈИ

Прегледни научни рад

DOI 10.7251/ZBK1901043J	COBISS.RS-ID 8272920	УДК 003.26:004.056.55

Стево Јаћимовски[1]
Криминалистичко-полицијски универзитет, Београд

Јован Шетрајчић
Факултет за спорт, Универзитет Унион-Никола Тесла, Београд

Јелена Ламовец
Институт за хемију технологију и металургију, Београд

Апстракт: Крајем двадесетог века човечанство је ушло у еру информационих технологија. ИТ индустрија, која се бави производњом, обрадом, складиштењем и преносом информација, постала је саставни део глобалног економског система, потпуно независан и прилично значајан сектор привреде. Зависност савременог друштва од информационих технологија је толико велика да пропусти у информационим системима могу довести до значајних инцидената. Телекомуникације су кључна индустрија информационих технологија. Међутим, информације су током транспорта веома осетљиве на разне врсте злоупотреба. Јединице за складиштење и обраду података могу бити физички заштићене од недобронамерних, што се не може рећи за комуникационе линије које се протежу на стотине или хиљаде километара и које је готово немогуће заштитити. Стога је проблем заштите информација у сфери телекомуникација веома значајан. Криптологија као наука и посебно њен део криптографија управо се баве овом проблематиком. Квантна криптографија је релативно новија област која се бави обезбеђењем сигурне комуникације између пошиљаоца и примаоца информације, користећи законе квантне физике. Циљ рада је да се упознамо са принципима квантне дистрибуције кључа за кодирање информација и основним проблемима који се јављају при његовој реализацији.

Кључне ријечи: криптографија, алгоритми, кодирање, кључ, квантна физика, протоколи.

УВОД

Према англосаксонској традицији учесници у кодирању и декодирању информација се називају Алиса и Боб. Противник, који би хтео да неовлашћено сазна информације које Алиса и Боб размењују, назива се Ева од

[1] Аутор за кореспонденцију: др Стево Јаћимовски, редовни професор, Криминалистичко-полицијски универзитет у Београду. E-mail: stevo.jacimovski@kpu.edu.rs

eavedropper (прислушкивач) (Bennett, 1992). Противник, по претпоставци, располаже неограниченим рачунарским ресурсима и познаје коришћење криптографских метода, алгоритама[2], протокола[3] итд. (Dugić, 2009).

Класични задатак криптографије је да трансформише неки почетни текст (отворени текст) у произвољни низ знакова који се зове криптограм. Број знакова у отвореном тексту и криптограму се може разликовати. Тајност самог алгоритма кодирања[4] не може, у принципу, обезбедити безусловну сигурност криптограма, јер се претпоставља да Ева (противник) има бесконачно велике рачунарске ресурсе. Стога се данас користе отворени алгоритми. Безбедност савремених криптосистема се не заснива на тајности алгоритма већ на тајности неке информације малих димензија која се назива кључ. Кључ се користи за управљање процесом кодирања и требало би да се лако може променити у било ком тренутку времена. Крајем XIX века холандски научник Керкхоф је формулисао правило по коме је сигурност кода обезбеђена ако је противнику познат целокупни систем кодирања, осим тајног кључа, тј. осим информације која управља процесом криптографске трансформације (Килин, Хорошко & Низовцев, 2007).

Слика 1. Структура симетричног криптосистема

Код симетричног криптосистема пошиљалац и прималац информације користе исти тајни кључ, слика 1. Помоћу тог тајног кључа се врши и шифровање и дешифровање информације. Кључ се мора периодично обнављати и истовремено дистрибуирати и пошиљаоцу и примаоцу информације. Процес дистрибуције тајних кључева између регуларних учесника у размени информација је веома сложен процес. У рукама нелегитимног

[2] Алгоритам је скуп команди, инструкција, радњи, прорачуна које је неопходно извршити да би се из почетних података постигао неки резултат.

[3] Протокол је низ радњи (инструкција, команди, прорачуна, алгоритама) које се врше по одређеном редоследу од стране два или више субјеката са циљем постизања неког резултата.

[4] Кодирање тј. шифровање, енкрипција.

корисника (Еве) тајни кључ би омогућио познавање предатих информација између Алисе и Боба (Румянцев & Голубчиков, 2009).

Симетрични криптографски алгоритми пружају висок степен заштите све док кључ знају само пошиљалац и прималац поруке. Зато основну меру безбедности симетричних алгоритама чини метод дистрибуције кључева. Најпознатији и најраспрострањенији симетрични алгоритам је ДЕС и унапређена верзија 3 ДЕС (Čisar, 2015).

Раније је овај проблем решен некриптографском методом – преношењем кључа преко физички заштићених слушних канала. Међутим, стварање таквог канала и његово одржавање у оперативној спремности у случају хитне потребе преношења кључа је доста дуготрајно и скупо. Дакле, у условима константног повећања интензитета информационих токова, ова метода дистрибуције кључа је постајала све мање прихватљива и задовољавајућа.

Проблем је успешно решен у оквиру модерне криптографије. Постоје два начина решења дистрибуције кључа: математички и физички. Математички начин је реализован коришћењем протокола са два кључа или помоћу криптографије са отвореним кључем. Физички начин се реализује помоћу квантне криптографије.

АСИМЕТРИЧНИ МЕТОД ШИФРОВАЊА

Слика 2. Структура асиметричног криптосистема

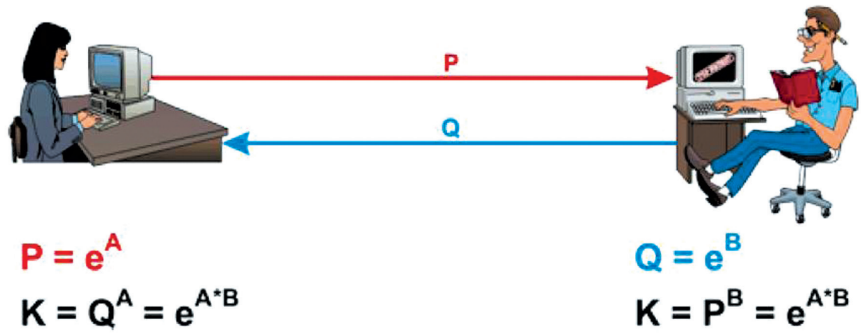
Асиметрични криптосистеми за рад користе два кључа, слика 2. Први кључ је отворен и доступан свим корисницима размене информација. Помоћу тог кључа се врши шифровање информације. Други тајни кључ поседује само прималац информације (Боб). Дешифровање информације помоћу отвореног кључа је немогуће. Такође, кључ за дешифровање није могуће одредити помоћу отвореног кључа за шифровање (Румянцев & Голубчиков, 2009).

Шему асиметричне криптографије су 1976. године предложили У. Дифи и М. Хелман са Станфорд универзитета. Ако Алиса и Боб желе да успоставе тајни кључ довољно је да следе овај протокол (Jakuš, 2016):

• Алиса генерише случајан број А и рачуна $P=e^A$ и шаље Р Бобу

• Боб генерише случајан број В и рачуна $Q=e^B$ и шаље Q Алиси

Тада Алиса и Боб рачунају тајни кључ, К, као што је приказано на слици 3.



Слика 3. Дифи-Хелманов протокол

Претпоставимо да Ева поседује Р и Q. Може ли израчунати К? Да би израчунала К, Ева мора израчунати А или В, јер тада може поновити рачун кључа на исти начин као Алиса односно Боб. Идеја је у томе што рачун А или В захтева рачунање дискретног логаритма:

$$A=\ln P,\ B=\ln Q$$

а за то не постоји ефикасан начин (Stipčević, 2007). Сигурност Дифи-Хелмановог метода заснива се на сложености дискретног логаритмовања. Најпознатији алгоритам у групи асиметричних криптографских метода је RSA.

У првом случају, у протоколу са два кључа, поступци енкрипције и дешифровања се изводе на различитим кључевима, тако да нема потребе да се тајна кључа чува. Међутим, због екстремно ниских карактеристика перформанси и излагања неким посебним врстама напада, такве шифре су се показале неприкладним за затварање директних корисничких информација. Уместо тога, асиметричне шифре се користе као део комбинованих шема, када је низ података шифрован са симетричном шифром на једнократном кључу, који је пак шифрован шифром са два кључа и преноси се у овом облику заједно са подацима.

У другом случају, код криптографије са отвореним кључем, шеме дистрибуције кључа за отворене канале комуникације решавају исти про-

блем на мало другачији начин: током интеракције, два учесника који размењују информације генеришу заједнички тајни кључ, који се затим користи за шифровање пренесених података симетричном шифром. Штавише, пресретање информација у каналу током сесије генерисања таквог кључа не дозвољава непријатељу да сам прибави кључ.

Безбедност криптосистема са два кључа заснива се на спором техничком прогресу. Њихова безбедност је заснована на проблемима факторизовања великих бројева и израчунавању дискретних логаритама у одређеним коначним групама. За те проблеме се верује да су ,,тешки" у смислу да не постоји бољи начин да реше него да се погађају сва могућа решења (кључеви) чиме број корака расте експоненцијално с дужином кључа.

Тајност се у савременом свету заснива на замисли да је нешто рачунарски безбедно тј. да је сигурно у смислу да би за проваљивање кода било потребно превише рачунарског времена и снаге (Vedral, 2014). За велике бројеве проналажење њиховог фактора је тежак проблем. Замислите број 100. Који су његови фактори? Два пута 50 једнако је 100. Али то важи и за 4 пута 25, или 5 пута 20 или 10 пута 10. Број фактора брзо расте и проналажење свих њих представља велику потешкоћу за сваки данашњи класични компјутер.

Ипак са очекиваном појавом квантних компјутера за које су разрађени алгоритми брзе факторизације, криптографски системи засновани на математичким методама криптозаштите могу бити угрожени.

Процедуру за ово је дао Питер Шор (Shor, 1994) који је дао алгоритам по коме квантни компјутер, пошто користи квантни принцип суперпозиције, може да постоји истовремено у много различитих стања. Замислите један једини компјутер у суперпозицији тако да је истовремено на више различитих места. На свакој од тих локација можете конфигурисати компјутер тако да дели ваш број са другим бројем како би трагали за факторима. На тај начин добијамо, огромно, невероватно убрзање решења проблема факторисања, пошто један квантни компјутер сада симултано обавља сва та дељења, по једно на свакој просторној локацији. Према мишљењу стручњака, квантни рачунар који може да разбије RSA крипто систем може да се створи за око 15-25 година.

Управо због овога дошло се на идеју да се заштита информација потражи у, колоквијално речено, ,,хардверу" тј. да се за заштиту искористе закони квантне механике.

Стога се јавила потреба заштите криптосистема на другим основама. Решење дистрибуције кључа се остварује у квантној криптографији која је заснована на законима физике (Jaćimovski & Šetrajčić, 2016).

Основни аргументи за ово су две чињенице:

- Немогуће је копирати непознато квантно стање

- Без пертурбације је немогуће имати информацију о неортогоналним квантним стањима (другим речима Ева прилоком било каквог приступа каналу информације мења стање носилаца информације)

Квантна криптографија користи неодређеност квантног света у акту мерења, тзв. Хајзенбергов принцип неодређености (Hajzenberg, 1974). Уз помоћ квантне физике може се успоставити комуникациони канал који није могуће прислушкивати без ометања преноса. Два корисника који међусобно комуницирају могу увек открити присуство треће стране која покушава да сазна кључ.

Такође, особа која прислушкује не може копирати непознате квантне битове такозване кубитове, тј. непозната квантна стања, због теореме о неклонирању. Квантна криптографија служи само за добијање и дистрибуцију кључа, а не за пренос порука. Тако генерисани кључ може послужити у неком криптосистему за шифровање и дешифровање поруке.

На тај начин квантна криптографија омогућава релативно брзу размену кључева и регистровање покушаја Еве да уђе у канал везе. Нагласимо да појава грешака при предаји и пријему квантних стања не доводи обавезно до губитка тајности. За сваки протокол квантне криптографије се дефинише критична грешка изнад које тајност није обезбеђена. Ако је ниво грешака (обично се изражавају у процентима) испод критичног онда се за креирање кључа користе протоколи корекције грешака И каснијег сажимања преосталих битова. После ових поступака Ева има толико мало информација о кључу колико Алиса и Боб желе (Picek & Golub, 2009).

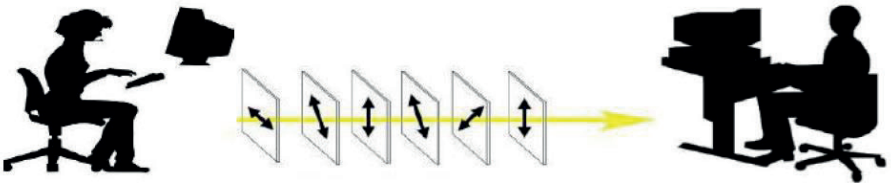
У квантној криптографији се данас користе три облика кодирања квантних стања: поларизационо, фазно и кодирање са временским померањем. У раду ће се демонстрирати поступак са поларизационим кодирањем квантних стања тзв. протокол ББ84 и објаснити протокол Е91. Постоје и други протоколи квантне криптографије који се користе.

Пример протокола ББ84 без шума

Протокол ББ84 (Bennett & Brassard, 1984) је историјски први протокол о квантној дистрибуцији кључа (Килин, Хорошко & Низовцев, 2007), чија је безбедност заснована на принципима квантне механике због чега је апсолутно безбедан уколико нема шума у квантном каналу везе. Одсуство шума у датој ситуацији претпоставља да се квантно стање честица не мења дуж квантног канала везе.

Протокол ББ84 је формулисан на језику појединачних фотона, слика 4, иако се он може применити на било коју другу реализацију кубитова. За кодирање информације у протоколу се користе четири стања поларизације која образују два међусобно неортогонална базиса: Правоугаони $|\leftrightarrow\rangle$ и $|\updownarrow\rangle$ и дијагонални

$$\left|\nearrow\right\rangle = (\left|\leftrightarrow\right\rangle + \left|\updownarrow\right\rangle)/\sqrt{2} \qquad \left|\nwarrow\right\rangle = (\left|\leftrightarrow\right\rangle - \left|\updownarrow\right\rangle)/\sqrt{2}$$



Слика 4. Приказ протокола ББ84

Суштина ББ84 протокола се састоји у томе да један од корисника (Алиса) бира случајно низ битова (етапа 1) и низ базиса (етапа 2) и затим шаље кориснику (Бобу) низ фотона (етапа 3) од којих сваки кодира један бит из изабраног низа у базису који одговара редном броју тога бита при чему стања $|\leftrightarrow\rangle$ $|\nwarrow\rangle$ кодирају (0) нулу, а стања $|\nearrow\rangle$ $|\nwarrow\rangle$ јединицу (1). При добијању фотона, Боб на случајан начин, за сваки фотон и независно од Алисе, бира базис за мерење (правоугаони или дијагонални) (етапа 4) и аналогно за сваки фотон интерпретира резултат свога мерења на два начина као нулу или јединицу (етапа 5). Сагласно законима квантне механике после мерења дијагоналног фотона у правоугаоном базису, његова поларизација се претвара у хоризонталну или вертикалну и обрнуто, при чему је резултат сасвим случајан. На тај начин Боб добија резултате који се поклапају са стањима послатих фотона приближно у пола случајева (50%), тј. када он исправно погоди базис. Следећа етапа протокола се реализује помоћу отвореног канала везе, путем кога Алиса и Боб могу отворено саопштити један другом класичну информацију. На овој етапи претпостављамо да Ева може да слуша саопштења обе стране, но не може да их мења нити да шаље обавештења уместо њих. За почетак Алиса и Боб утврђују (отвореним каналом) који су фотони успешно добијени од стране Боба и који од њих су измерени у правилном базису (етапа 6 и 7). После тога Алиса и Боб имају једнаке вредности битова, кодираних у тим фотонима, без обзира на то што та информација никада није утврђена у отвореном каналу комуникације (етапа 8). Другим речима сваки од тих фотона носи један бит случајне информације, која је позната само Алиси и Бобу и никоме више. Информације о фотонима измереним у погрешном базису се одбацују, услед чега Алиса и Боб добијају тзв. просејани кључ, који у случају да Ева није пресрела информације треба да је исти за обе стране.

Табела 1: Пример реализације ББ84 протокола. Стања $|\leftrightarrow\rangle$ $|\nearrow\rangle$ кодирају (0) нулу, а стања $|\updownarrow\rangle$ $\oplus$ јединицу (1). Правоугаони и дијагонални базиси су означени са $\oplus$ и $\otimes$.

Етапа 1	Случајни битови слања (Алиса)	0	1	1	0	1	1	0	0
Етапа 2	Случајни базиси слања (Алиса)	$\otimes$	$\otimes$	$\otimes$	$\oplus$	$\oplus$	$\otimes$	$\otimes$	$\oplus$
Етапа 3	Поларизација фотона дистрибуираних по квантном каналу	$\searrow\!\!\swarrow$	$\searrow\!\!\swarrow$	$\nearrow\!\!\swarrow$	$\leftrightarrow$	$\updownarrow$	$\nearrow\!\!\swarrow$	$\nearrow\!\!\swarrow$	$\leftrightarrow$
Етапа 4	Случајни базиси пријема (Боб)	$\oplus$	$\oplus$	$\otimes$	$\oplus$	$\oplus$	$\oplus$	$\oplus$	$\oplus$
Етапа 5	Битови које је примио Боб	0	0	1	1	1	0	0	0
Етапа 6	Боб извештава Алису о базисима пријема	$\oplus$	$\otimes$	$\otimes$	$\otimes$	$\oplus$	$\oplus$	$\oplus$	$\oplus$
Етапа 7	Алиса одговара Бобу који су им базиси усаглашени								
Етапа 8	Просејани кључ			1		1			0
Етапа 9	Боб открива део битова					1			
Етапа 10	Алиса их потврђује								
Етапа 11	Просејани кључ после процене грешке			1					0

Претпоставимо да Ева прислушкује квантни канал. Због случајног избора правоугаоног или дијагоналног базиса Ева утиче на информацију на тај начин да мења битове просејаног кључа, који би морао бити исти за Алису и за Боба, да нема Еве. Ниједно мерење фотона од стране Еве, не даје више од једне половине информације о биту који је кодиран тим фотоном; било које такво мерење даје b бита информације ($b < 1/2$) и није у сагласности са вероватноћом (која је у крајњем случају једнака $b/2$, ако мерени фотон или његова замена буде измерен у почетном базису од стране Боба. На тај начин, Алиса и Боб могу проверити да ли их неко прислушкује, отворено упоређујући део битова (етапа 9 и 10) за које морају имати исту информацију иако се ти битови, надаље, не могу користити за тајни кључ. Положај битова при том упоређивању треба да је случајни подскуп правилно измерених битова, тако да присуство Еве мора да се уочи. Ако се приликом упоређивања сви упоређивани битови поклапају, јасно је да прилушкивања није било, и остатак правилно измерених битова може се користити за тајни кључ кодирања (етапа 11) и предаје података отвореним каналом.

Када се тај кључ искористи, Алиса и Боб понављају процедуру ради креирања новог тајног кључа.

Безбедност ББ84 протокола

Протокол ББ84 би био угрожен ако би Ева могла да уради следеће интервенције на квантном каналу (Markagić, 2012):

1. Да измери поларизацију фотона који шаље Алиса, репродукује исти такав и пошаље га Бобу
2. Умножи фотоне које шаље Алиса

У првом случају Ева би имала исту информацију коју имају Алиса и Боб, па би на крају процедуре имала исти кључ. Међутим, Алиса користи фотоне из коњуговних база, тј. не постоји оријентација поларизатора којом би Ева могла са сигурношћу разликовати поларизацију фотона. У другом случају Ева жели с неколико различито оријентисаних поларизатора са сигурношћу одредити поларизацију фотона. Међутим, умножавање непознатог квантног стања није могуће због теореме о немогућности клонирања стања.

У комуникацији између Алисе и Боба може да се деси да ће део тачно измерених фотона бити детектован погрешно. Такође, ако Ева покуша да измери фотоне које је Алиса послала пре него што стигну до Боба, грешке ће настати због чињенице да Ева покушава да измери податке о поларизацији фотона. Ове две ситуације се не могу разликовати: природан или вештачки шум изгледају исто. Услед тога Алиса и Боб се договарају о мањем криптографском кључу у три фазе. Те три фазе називају се процена грешке, поравнање информација и појачање приватности.

Протокол Е91 (Ekart, 1991)

Даље побољшање поузданости криптосистема може се постићи употребом Ајнштајн-Подолски-Розен (АПР) ефекта (Einstein, Podolsky & Rosen, 1935). АПР ефекат се дешава када сферно симетрични атом зрачи два фотона у супротним правцима према два посматрача. Фотони се емитују са неодређеном поларизацијом, али су због симетрије њихове поларизације увек супротне (ефекат квантне сплетености). Важна карактеристика овог ефекта је да поларизација фотона постаје позната тек након мерења. На основу АПР-а, Екерт је предложио крипто-шему која гарантује сигурност преноса и складиштења кључа. Пошиљалац генерише бројне АПР фотонске парове. За себе оставља по један фотон из сваког пара, а другог шаље свом партнеру. Истовремено, ако је ефикасност регистрације близу јединства, када пошиљалац прими вредност поларизације 1, његов партнер ће регистровати вредност 0 и обрнуто. Јасно је да на овај начин партнери, кад год је потребно, могу добити идентичне псеудо-случајне кодне секвенце. Практично, имплементација ове шеме је проблематична због ниске ефикасности снимања и мерења поларизације једног фотона.

ЗАКЉУЧАК

Задатак криптографије је размена тајних порука. Постоје класични методи који гарантују практично сигурну (безбедну) комуникацију (између Алисе и Боба), уколико је обема странама познат тајни кључ за дешифровање, и истовремено, тај кључ није никоме другом познат, па ни потенцијалном противнику, Еви.

Управо та претпоставка о тајности „тајног кључа" је најслабија карика у класичној криптографији. Једини задатак квантне криптографије је обезбеђивање тајног кључа. Дакле, у квантној криптографији се не размењују поруке већ само тајни кључ, путем тзв. квантног канала. Данас већ постоје комерцијални уређаји као и десетине имплементација државних и корпоративних сигурних комуникационих мрежа које примењују технологије дистрибуције квантног кључа. Предности ових технологија су безусловна сигурност која се заснива на феноменима квантне механике. Данас је практично могуће, уз безусловну сигурност, генерисати и дистрибуирати тајни кључ између две стране повезане оптичким влакном на удаљеностима до 150 километара за неколико секунди. Прислушкивање комуникације од треће стране не доводи до открића тајне него искључиво до смањења брзине генерисања кључева, с тим да обе стране одмах знају да је линија активно прислушкивана. Главни недостаци ових система су ограничење брзине генерисања кључа која директно зависи од удаљености учесника, немогућност појачавања сигнала односно преношења путем неке врсте релеја, практично ограничење искључиво на комуникације путем оптичких влакана, као и цена имплементација система (Ијачић, 2014).

У идеалним системима квантне комуникације, пресретање података је немогуће, јер пресретање учесници у размени одмах откривају као грешке које се јављају у преносу. Међутим, прави системи су различити од идеалних.

За разлику од идеалног, стварни квантни комуникацијски системи нису у стању да осигурају апсолутну тајност пренесених података. То је због чињенице да у систему постоји фон сопствених грешака, иза којег се могу прикрити покушаји пресретања информација, као и пригушење у комуникацијским каналима због неопходности коришћења мултифотонских импулса. Коришћење јаких импулса фотона доводи до пригушења преноса информација што омогућава неприметно пресретање података. То је практично фактор који се не може уклонити, будући да се квалитет канала којим се информација преноси не може увек контролисати.

На путу ка практичној примени квантних комуникационих система треба решити низ техничких потешкоћа као што су развој стабилних извора појединачних фотона и једнофотонских детектора који би радили у нормалном температурном опсегу и не би требало да буду хлађени течним гасовима. За борбу против системских грешака треба користити различите корекционе кодове, а за смањење значаја пресретнутих битова користити про-

цедуре за повећање тајности. Поред тога, могу се предузети додатне мере безбедности чисто техничке природе.

Захвалност: Овај рад је урађен у оквиру пројеката Министарства просвете, науке и технолошког развоја Републике Србије, број ОИ 171039, ТР34019 и ТР32008, Министарства за научнотехнолошки развој, високо образовање и информационо друштво Републике Српске, пројекат ,,Фундирање термодинамичког инжењеринга и развој софтверског пакета за истраживање фононских наноструктура".

ЛИТЕРАТУРА

Bennett, C. H., Brassard, G. (1984). Quantum cryptography: Public key distribution and coin tossing. *Proc. IEEE Int. Conf. Computers, Systems and Signal Processing* (pp. 175-179). Bangalore, India.

Bennett, C. (1992). Quantum cryptography using any two non-orthogonal states. *Physical Review Letters, 68*, 3121-3124.

Čisar, P (2015). Opšti aspekti kvantne kriptografije. *Info M, 14*(54), 37-44.

Dugić, M. (2009). *Osnove kvantne informatike i kvantnog računanja.* Kragujevac: PMF Kragujevac.

Einstein, A., Podolsky, B., Rosen, N. (1935). Can quantum-mechanical description of physical reality be considered complete? *Physical Review*, *47*, 777- 780.

Ekart, A. (1991). Quantum cryptography based on Bell's theorem. *Physical Review Letters*, *67* (6), 661-663.

Hajzenberg, V. (1974). *Fizika i metafizika.* Beograd: Sazvežđa.

Ijačić, S. (2014). Primena kvantne mehanike u kriptografiji, kvantno računarstvo i post-kvantni šifarski sistemi, Master rad. Beograd: Univerzitet Singidunum.

Jaćimovski, S., Šetrajčić, J. (2016). Physical Fundamentals of Quantum Cryptography. *Archibald Reiss Days* (pp. 276-292). Belgrade: Academy of Criminalistic and Police Studies.

Jakuš, M. (2004): Kvantna kriptografija, Faculty of Electrical Engineering and Computation, Zagreb, http://os2.zemris.fer.hr/kvant/2004_jakus/

Килин С.Я., Хорошко Д.Б., Низовцев А.П. (2007). *Квантовая криптография: идеи и практика.* Минск: Беларуская навука.

Markagić, M. (2012). Protokoli i pravci razvoja kvantne kriptografije. *Vojnotehnički glasnik*, *LX* (1), 250-265.

Picek, S., Golub, M. (2009). Kvantna kriptografija: razvoj i protokoli. *Proceedings of the Information Systems Security* (str. 122-127). Opatija: MIPRO.

Румянцев К. Е., Голубчиков Д. М. (2009). *Квантовая связь и квантовая криптография.* Таганрог: ТТИ ЮФУ.

Shor, P. (1994). Algorithms for quantum computation: Discrete logarithms and factoring. *35nd Annual Symposium on Foundations of Computer Science* (pp. 124-134). Los Alamos: IEEE Computer Society.

Stipčević M., Kvantna kriptografija, http://www.irb.hr/users/stipcevi/download/fer/171203.pdf (2003)

Vedral, V. (2014). *Dekodiranje stvarnosti.* Beograd: Laguna.

Рад примљен: 20. 02. 2019.

Рад прихваћен: 29. 03. 2019.