ПРИМЕНА КВАНТНЕ КРИПТОГРАФИЈЕ У ДИСТРИБУЦИЈИ ТАЈНИХ КЉУЧЕВА У СИМЕТРИЧНИМ КРИПТОГРАФСКИМ АЛГОРИТМИМА

Борис Зејак, *Министарство спољних послова СЦГ - Центар везе, Кнеза Милоша 24-26, boris@smip.sv.gov.yu*
Михаило Кнежевић, *Министарство спољних послова СЦГ - Центар везе, Кнеза Милоша 24-26, mihailo@smip.sv.gov.yu*

Садржај: *У раду је представљен нови приступ решавања проблема дистрибуције тајних кључева код симетричних криптографских система. Ова савремена метода која за пренос бита користи квантна својства фотона назива се квантна криптографија. Описана је прва квантна криптеографска шема, позната као протокол BB84.*

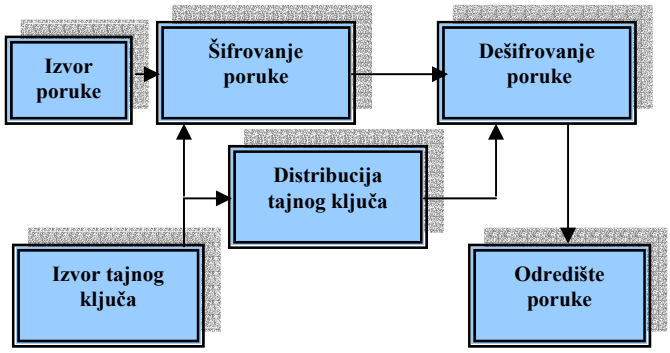
1. УВОД

У условима развоја глобалних комуникација појачава се потреба за криптографском заштитом података, која није више део само специјализованих, већ и многих комерцијалних комуникационих система (системи пословних и финансијских комуникација). Стога криптографија доживљава нову димензију у којој се криптографски системи пројектују за заштиту података у једном окружењу у коме су они изложени интензивним и разноврсним нападима. Постоји низ добро познатих криптографских алгоритама који подржавају различите безбедносне операције и могу се поделити у две велике групе, и то симетричне и асиметричне криптографске алгоритме. Избор алгоритама у процесу имплементације зависи од типа заштитног механизма и најчешће се, да би заштита била потпуна и ефикасна, примењује комбинација симетричних и асиметричних у којој се они међусобно допуњавају.

2. СИМЕТРИЧНИ КРИПТОГРАФСКИ АЛГОРИТМИ

Групу симетричних криптографских алгоритама представљају алгоритми код којих је кључ за шифровање идентичан кључу за дешифровање (слика 1). Алгоритми из ове групе се такође називају и алгоритми са тајним кључем јер је тајност кључа који се користи и за шифровање и за дешифровање есенцијална за безбедност порука у систему. Посебно је осетљива његова дистрибуција од извора кључа до учесника у заштићеној комуникацији. Ови системи представљају основу традиционалне криптолошке теорије и развијају се већ веома дуги низ година. С обзиром да заштита информација тежишну примену има у пословима везаним за државне структуре, ови системи су били искључиво тајни системи, наменски дефинисани и реализовани од стране надлежних државних институција.

Са порастом интензитета и примене електронских облика комуникација јавила се потреба за дефинисањем јавних симетричних криптографских алгоритама па је у последњих десетак година дефинисано више јавних симетричних криптографских алгоритама за примену у апликацијама у којима за то постоји потреба.



Слика 1. *Симетрични криптографски систем*

Основни проблем у реализацији ових система представља дистрибуција тајног кључа. Наиме, тајни кључ мора бити познат искључиво примаоцу и пошиљаоцу заштићене поруке и мора бити потпуно идентичан на обе стране. Његово генерисање се базира на случајним непоновљивим процесима на страни пошиљаоца и потребно га је дистрибуирати до примаоца. Та дистрибуција, са једне стране, мора да буде апсолутно сигурна, да на преносном путу не би дошло до компромитовања кључа и тако се нарушила безбедност комуникације. Са друге стране дистрибуција треба да се обави у прихватљивом времену и са прихватљивим материјалним трошковима. До данас, међутим није пронађен метод који у потпуности задовољава све аспекте овог проблема.

Као резултат тежње да се пронађе право решење откривени су асиметрични криптографски алгоритми који представљају једно од највећих достигнућа криптологије у другој половини двадесетог века. Основни принцип код асиметричних шифарских системима је да се користе различити кључеви за шифровање и дешифровање, тзв. јавни и тајни кључеви, који се генеришу као пар. Један кључ из тог пара (јавни кључ) је јавно доступан свим учесницима у комуникацији, док је други (тајни кључ) доступан само власнику пара кључева. Порука шифрована једним кључем из овог пара може се дешифровати искључиво другим кључем из тог пара кључева. Најчешћи облик примене овог шифарског система је када пошиљалац поруке врши њено шифровање помоћу јавног кључа примаоца поруке. Тако шифровану поруку може дешифровати искључиво прималац поруке, пошто једино

он поседује тајни кључ који одговара јавном кључу којим је порука шифрована .

Међутим, висока рачунарска захтевност ових алгоритама у односу на симетричне криптографске алгоритме, битно утиче на перформансе система у којима се примењују, тако да се не препоручује примена за заштиту тајности информација у системима са великим протоком информација. Ово наравно не елеминише аутоматски ове алгоритме јер за поједине примене (нарочито у комерцијалним комуникационим системима) имају несумњиву предност над традиционалним техникама.

3. КВАНТНА КРИПТОГРАФИЈА

Проучавајући необичне законе квантне механике, истраживачи су дошли на идеју да се проблем дистрибуције тајних кључева код симетричних шифарских система може ефикасно решити применом тзв. квантне криптографије. Ови системи се још увек налазе у фази развоја, и нису доживели своју комерцијалну употребу, али досадашња истраживања дају обећавајуће резултате. У овом процесу користе се фотони, тј. њихова поларизација, као основна квантна особина, за представљање 0 и 1 у бинарној секвенци која носи садржај кључа. На тај начин сваки фотон носи бит квантне информације, који физичари називају квибит (qуибит).

Да би правилно примио квибит примаоц мора одредити поларизацију фотона и у том процесу он неизбежно мења његове карактеристике. Управо та особина фотона је пресудна са аспекта заштите од прислушкивача. Наиме, да би прочитао садржај квибита, прислушкивач мора да одреди поларизацију фотона. На тај начин он неминовно мења квантне особине фотона, тако да пошиљалац и прималац кључа лако могу да установе да ли је дошло до прислушкивања и да одбаце компромитоване делове секвенце, тј. да их не користе у процесу криптовања поруке.

Процес се састоји из тога што пошиљалац шаље серију фотона са случајном поларизацијом. Та секвенца се на пријему користи за генерисање секвенце бројева која се користи у процесу криптовања. Овај процес је познат као процес квантне дистрибуције кључева. Ако се утврди да је део кључа на свом путу преноса био прислушкиван, тај низ случајних бита се одбацује и пошиљалац генерише нови кључ. Тек када се утврди да је примљени кључ сигуран, пошиљалац поруке га користи у процесу шифровања помоћу симетричних криптографских алгоритама. Тако шифрована порука се може проследити до примаоца путем класичних комуникационих средстава

4. ПРОТОКОЛ BB84

Прву примену квантне дистрибуције кључева објавили су 1984. године Charles H. Bennet из IBM лабараторије и Gilles Brassard са универзитета у Монтреалу. Та њихова прва квантна криптографска шема постала је позната као BB84 протокол.

По том протоколу, пошиљалац покушава да пошаље заштићену поруку примаоцу. Процес почиње слањем случајне серије квибита од стране пошиљаоца. Приликом слања фотона, као носилаца информације он их може кодовати на два различита начина:

- применом линеарне поларизације, где вертикална оријентација представља бинарно 1, а хоризонтална бинарно 0,
- применом дијагоналне поларизације, где оријентација од +45 степени представља бинарно 1, а оријентација од –45 степени представља бинарно 0.

Чињеница да он има могућност избора између две различите врсте поларизације приликом формирања квибита веома је битна.

Да би примио квибит од пошиљаоца, примаоц користи поларизациони beam-splitter, уређај који правилно прима фотоне само једне врсте поларизације (или линеарне или дијагоналне), а не и њој ортогоналне. На основу тога који тип поларизованих фотона прима, може бити линеарни или дијагонални. Фотони ортогоналне поларизације због њихове квантне природе, такође се региструју, али погрешно, са једнаком вероватноћом па се, без обзира који садржај носи, такав квибит на пријему региструје као 0 или као 1.

На пример, ако примаоц поседује линеарни beam-splitter, он дијагонално поларизовани фотон са оријентацијом +45 може са једнаком вероватноћом да прими као вертикално или хоризонтално поларизовани квибит, тј. или као 0 или као 1. Протокол BB84 омогућава да он касније одреди те погрешно примљене квибите и да их одбаци.

Пошиљаоц приликом слања може да употреби било који тип поларизације да кодира квибит, али је неопходно да се тај избор врши на случајан начин. Слично томе, примаоц прима сваки фотон, случајно претпостављајући врсту поларизације квибита на пријему. Јасно, када они изаберу исту поларизацију добиће исти резултат, у случају да су изабрали међусобно ортогоналне поларизације, резултати могу бити неодговарајући.

Након тога примаоц јавно, без потребе за заштитом и шифровањем, саопштава пошиљаоцу којим редоследом је случајно вршио избор поларизације на пријему (нпр. дијагонална, дијагонална, линерна, дијагонална, линеарна, линеарна, линеарна,...). При томе он не саопштава садржај секвенце коју је примио. Након тога пошиљаоц, такође јавно, обавештава примаоца за које квибите се њихови избори поларизације слажу. Они затим задржавају само бите који су послани и примљени по истој поларизацији, док одбацују фотоне који су послати по једној а примљени по другој, њој ортогоналној поларизацији.

На тај начин примаоц и пошиљаоц добијају серију случајних бита која је краћа од почетне, али која је позната искључиво њима и може се искористити као тајни кључ у сврхе шифровања симетричним алгоритмом. Нити пошиљац, нити примаоц не могу

унапред одредити садржај кључа, пошто је он производ њихових случајних избора.

У реалним условима, на преносном путу може доћи до поремећаја у квантим карактеристикама фотона, а и детекциони уређај на пријему није савршен, тако да може да се деси да пошиљаоц и примаоц не добију потпуно идентичне секвенце. Да би се то избегло морају се применити неке од стандардних метода за корекцију грешака, као што је провера парности. Она се састоји из тога да и примаоц и пошиљаоц деле свој кључ у блокове од по десетак секвенцијалних бита и рачунају и упоређују парност за сваког од њих. Ако је за одређени блок парност одговарајућа, претпоставља се да у том блоку нема грешака. Али ако се парност разликује за одређени блок, онда се тај блок дели даље на краће низове чија се парност такође упоређује све док се не пронађе погрешан бит.

Да током овог процеса не би открили сувише информација о кључу, примаоц и пошиљаоц одбацују по један бит из кључа сваки пут када они упоређују парности блокова. Тај процес се понавља више пута, коришћењем различитих начина за поделу кључа, што је често праћено раличитим алгоритмима за корекцију грешака. Крајњи резултат је краћи кључ, али потпуно сигуран и прилагођен примаоцу и пошиљаоцу.

5. ОТПОРНОСТ НА ПРИСЛУШКИВАЊЕ

Постоји више начина да прислушкивачи изврше напад на кључ приликом његове дистрибуције, међутим за све нападе протоколом BB84 су предвиђене одговарајуће мере тако да ниједан од њих није успешан.

Ако прислушкивач једноставно пресретне неки фотон на преносном путу и тај фотон не стигне до примаоца. Тада примаоц о томе обавештава пошиљаоца да би он тај бит одбацио.

Други начин је да прислушкивач пресретне фотон, да га прочита, и у истом облику у коме га је примио проследи до примаоца. Та стратегија је, такође неуспешна пошто је копирање непознатог квантног стања немогуће, што су научно доказали William Woters и Wojiceh Zurek 1984. Управо та особина квантних информација представља кључну предност квантнне криптографије у односу на методе које се користе у класичним криптографским системима. Због немогућности да копира стање фотона прислушкивач би морао да претпостави поларизацију којом је пошиљаоц послао фотон, да га прими, одреди његов садржај и по истој поларизацији и са истим садржајем га проследи до пошиљаоца. С обзиром да он не зна како је на страни пошиљаоца поларизован сваки фотон, он може то само претпоставити, али свака погрешна претпоставка производи грешку или шум на пријемној страни, које ће се открити приликом формирања коначне секвенце на страни пошиљаоца и примаоца.

Грешке у секвенци на пријему које прислушкивач својим активностима узрокује откривају његово присуство. Да би проверили присуство прислушкивача, пошиљаоц и примаоц жртвују део свог кључа, јавно проверавајући вредности малог броја послатих и примљених бита. Ако се приликом тог поређења открије више грешака него што би их иначе очекивали услед несавршености њихових уређаја, онда се та секвенца одбацује пошто је очигледно да су њихови фотони били изложени прислушкивању. Из тог разлога прецизно дефинисање нивоа грешака је веома важно у квантној криптографији због тога што је то начин за откривање прислушкивача.

И поред свега прислушкивач може да покуша да прикрије своје присуство на тај начин што обрађује само мали број фотона и тако ниво грешке увећа за јако малу вредност, коју примаоц и прислушкивач не би окарактерисали као прекорачење очекиваног нивоа. Мада на овај начин прислушкивач сазнаје само мали део кључа, то би могло да му омогући увид у део заштићених података. Међутим, коришћењем тзв. протокола за појачавање тајности (*privacy amlification protocols*) може се минимизовати количина информација о кључу коју прислушкивач може да сазна. Поступак се састоји у томе што пошиљаоц, произвољно узима парове битова из кључа и над сваким од њих врши логичку операцију “ексклузивно или” (XOR) која израчунава њихову суму по модулу 2. Након тога он обавештава примаоца над којим битовима је он извршио операцију не саопштавајући резултат. Примаоц изврши исту операцију и добије исте резултате. Тако примаоц и пошиљалац замене сваки пар бита са њиховом израчунатом XOR вредношћу. У међувремену, ако прислушкивач који има много грешака у свом кључу покушава да изврши исту операцију, то само умножава његову грешку. На пример, ако је један бит из пара над којим се врши XOR операција тачан, а други не, он не може добити исправну вредност бита којим су пошиљаоц и примаоц заменили тај пар.

Доказано је да је квантна криптографија сигурна у свим случајевима прислушкивања као што су ови претходно наведени, међутим физичари нису још увек комплетирали математичке доказе који гарантују њену сигурност у свим нападима. Када би примаоц и пошиљаоц имали савршене уређаје, сигурност њихових порука би се могла гарантовати. Међутим, у пракси на постоје савршени уређаји и управо на њиховим несавршеностима се базирају потенцијални напади. Већи степен несавршености уређаја отвара прислушкивачу већи простор за нападе. Због тога су за примену квантне криптографије добре карактеристике пријемног и предајног уређаја од суштинског значаја.

6. ПРЕДАЈНИ И ПРИЈЕМНИ УРЕЂАЈИ

Основна улога уређаја на предајној страни је да генерише појединачни фотон на захтев пошиљаоца. Идеалан извор представља тзв. фотонски топ. Међутим до данас овакав уређај није произведен у пракси, мада постоје многи покушаји. Једна врста се базира на п-н спојевима који емитују светлост. Други раде са материјалима сличним дијаманту у којим је један атом угљеника замењен атомом азота. Такве супституције производе празнине сличне шупљинама у п-типу полупроводника, које емитују појединачне фотоне када се побуде ласером. Многи уређаји раде на принципу стварања појединачних јона који емитују појединачне фотоне. Ипак ниједна од тих технологија није довољно сазрела да би била коришћена у експериментима квантне

криптографије, стога се, за сада, користе извори фотона који су далеко од идеалних са становишта сигурности. Најчешће се у пракси користе уређаји који раде на принципу смањења интензитета снопа импулсног ласера до тог нивоа да сваки импулс садржи само један фотон. Проблем код оваквих уређаја је мала, али значајна вероватноћа да импулс садржи више од једног фотона. Ти екстра фотони дају могућност прислушкивачу да прочита вредност квибита, а да то остане непримећено на страни примаоца и пошиљаоца.

Основна улога уређаја на пријемној страни је да детектује појединачне фотоне. У пракси, такође, не постоје овакви уређаји за које би се могло рећи да су сигурни за примену у квантној криптографији. Најчешће су у примени уређаји који користе лавинске фотодиоде у режиму пробоја (изнад напона пробоја) тј. у тзв. Геигер-овом моду. У тој тачки енергија појединачног апсорбованог фотона је довољна да изазове лавину електрона која призводи струју која се лако детектује. Ипак, ови уређаји су далеко од идеалних. Да би се детектовао следећи фотон, неопходно је да се струја кроз диоду врати на почетну вредност тј. да се уређај ресетује у прихватљивом времену. Осим тога за ове уређаје најбољи је силикон, који остварује најбољу детекцију на таласним дужинама од 800 nm, а који није уопште осетљив на таласним дужинама изнад 1100 nm, што је прилично испод 1300 nm и 1500 nm које су стандард у телекомуникацијама. На телекомуникационим таласним дужинама морају се користити германијумски или индијум-галијум-арсенидски детектори, мада су они далеко мање ефикасни и радна температура им је далеко испод собне. Комерцијални детектори појединачних фотона који раде на телекомуникационим таласним дужинама не задовољавају потребе квантне криптографије.

7. ДОСАДАШЊИ РЕЗУЛТАТИ

Упркос ограничењима у способности уређаја, истраживачи су постигли крупан напредак у области квантне криптографије. У почетку су истраживања била базирана на атмосферу као преносни медијум, тако да прва демонстрација оваквих система потиче из раних 90-тих када су у експериментима у IBM-овим лабораторијама кроз ваздушни простор пренешени фотони на раздаљину од 30 cm. Десетак година касније већ је представљена техника за безбедну комуникацију кроз атмосферу на даљини од 2 km. Данас се у Лос Аламос нациналној лабораторији проучавају системи који би могли да користе сателитске комуникације и на тај начин обезбеде заштићену комуникацију на раздаљинама од више стотина километара. Сматра се да ће ти системи наћи своју комерцијалну примену у следеће три године.

Међутим, са развојем фибер-оптичких комуникација и њиховом све већом улогом и применом у телекомуникацијама, отвара се нови простор за развој квантне криптографије, тако да је будућност ове методе усмерена у том правцу. На универзитету у Женеви употребљен је BB84 протокол за слање порука на раздаљине веће од 60 km, користећи комерцијални фибер-оптички кабл на таласној дужини од 1300 nm. Los Almos национална лабораторија развија сличан систем за сигурну комуникацију владиних агенција у Вашингтону кроз јавну оптичку мрежу.

Ограничење представљају оптички репетитори који се постављају на дужим оптичким трасама и чија је улога да приме, апсорбују, појачају и ретрансмитују оптички сигнал. Тај процес неминовно мења квантну информацију коју носи фотон, што чини дистрибуцију кључева немогућом.

8. ЗАКЉУЧАК

Проблем дистрибуције тајног кључа у симетричним системима и даље остаје њихова најслабија тачка, нарочито у условима које диктирају савремене комуникације. Нови приступ решавања овог проблема представља квантна криптографија, која користи необичне законе квантне механике да би се дистрибуција тајног кључа извела на безбедан начин. Теоријски посматрано овакав систем је апсолутно сигуран и отпоран на прислушкивање и грешке у преносу. Међутим, примена оваквог система у институцијама као нпр. у Министарству спољних послова је још немогућа пре решавања описаних практичних проблема: несавршености пријемних и предајних уређаја као и, за комуникације са дипломатским представништвима, врло битног проблема малог домета тј. немогућности модификовања сигнала при преносу нпр. коришћењем оптичких репетитора. Са убрзаним развојем технологије, посебно у области оптичких комуникација, сматра се да би генијалност ове идеје врло брзо могла доћи до изражаја и решити проблем дистрибуције тајних кључева код симетричних криптографских алгоритама.

ЛИТЕРАТУРА

[1] *Justin Mullins, "Making Unbreakable Code", IEEE Spectrum, May 2002.*

[2] *Hideaki Matsueda*, "*Security Enhanced Quantum Criptography by Controled Spontaneous Randomness", IEEE Trans. Fundamentals, April 1999.*

Abstract - The solution for key distribution in criptography by using the strange laws of quantum mechanics, so-called quantum criptography is introduced in this paper.

APPLICATION QUANTUM CRIPTOGRAPHY IN DISTRIBUTION SECRET COMMON KEY IN SYMMETRICAL ALGORITHMS

Boris Zejak, Mihailo Knežević