■ *Pregledni znanstveni članek*

Uroš Hudomalj, Franc Smole

Kvantna kriptografija

Povzetek. Zaradi množičnega nadzora in trgovanja z informacijami ima zasebnost vedno večji pomen. Za zagotavljanje zasebnosti pri izmenjavi informacij se uporablja šifriranje sporočil. V dobi informacijske tehnologije uporaba šifriranja vse bolj narašča. Ustrezni postopki šifriranja omogočajo elektronske storitve od spletnega bančništva do elektronskega glasovanja, med najbolj občutljiva področja, ki zahtevajo uporabo šifriranja, pa sodi tudi medicina. Članek podaja pregled klasičnih načinov šifriranja, s poudarkom na njihovih slabostih. Te pomanjkljivosti odpravljajo novi kriptografski postopki v sklopu post-kvantne in kvantne kriptografije, ki predstavlja teoretično nezlomljivo šifriranje. Predstavljena so načela delovanja kvantne kriptografije, in sicer na podlagi praktično najbolj razširjenega algoritma kvantne izmenjave ključa BB84. Opisane so pomanjkljivosti algoritma in predstavljeni možni vdori, nakazane pa so tudi izboljšave, ki preprečijo vsakršne zlorabe.

Quantum Cryptography

Abstract. In the era of mass surveillance and information trading, privacy is increasingly gaining importance. Encryption of messages is used to provide privacy while exchanging information. Data encryption is becoming widespread with the rise of information technology. Encryption enables various applications from online banking to electronic voting. Another sensitive area that requires the use of encryption is medicine. The paper presents an overview of the classic encryption methods, with an emphasis on their weaknesses. These are overcome using new cryptographic methods, namely post-quantum and quantum cryptography. The latter represents theoretically unbreakable encryption. The principles of quantum cryptography are presented based on the most widely used algorithm for quantum key distribution, the BB84. Its weaknesses are described, together with potential threats and improvements that prevent them.

■ **Infor Med Slov** 2018; 23(1-2): 18-25

Institucije avtorjev / Authors' institutions: Fakulteta za elektrotehniko, Univerza v Ljubljani (UH, FS).

Kontaktna oseba / Contact person: Uroš Hudomalj, Preglov trg 13, 1000 Ljubljana, Slovenija. E-pošta / E-mail: uh3370@student.uni-lj.si.

Prispelo / Received: 27. 6. 2018. Sprejeto / Accepted: 29. 6. 2018.

Uvod

Zaradi množičnega nadzora in trgovanja z informacijami ima zasebnost vedno večji pomen.[1] Za zagotavljanje zasebnosti pri izmenjavi informacij se uporablja šifriranje sporočil.[2] Namen tega je preprečiti nenaslovljeni osebi, da bi razbrala pomen sporočila, četudi ga prestreže, in preprečiti, da bi sporočilo ponaredila.

V dobi informacijske tehnologije uporaba šifriranja vse bolj narašča. Ustrezni postopki šifriranja omogočajo elektronske storitve od spletnega bančništva do elektronskega glasovanja.[1] Med občutljiva področja, ki zahtevajo uporabo šifriranja, sodi tudi medicina. Primer rabe šifriranja tam najdemo v informacijskih sistemih za medicinsko oskrbo na daljavo, ki omogočajo spremljanje pacientovega zdravstvenega stanja od doma. S tem zagotavljajo hitrejšo, sprotno in cenejšo obravnavo. Posebej pomemben je hiter razvoj medomrežja stvari (angl. *Internet of Things, IoT*) v medicinske namene,[3] kamor sodijo npr. priročni in nizkocenovni sistemi za beleženje srčnega utripa ali merjenje sladkorja v krvi. Vse te podatke je potrebno varno prenesti od pacienta do medicinskega centra. Pri tem moramo zagotoviti, da lahko do teh podatkov dostopajo le pooblaščene osebe, in onemogočiti njihovo ponarejanje. To zagotavlja ustrezna uporaba kriptografije.[4,5] V sklopu zagotavljanja učinkovitega e-zdravja uvajajo tudi elektronske kartoteke pacientov, ki omogočajo celovitejšo obravnavo posameznika. Tudi tu mora biti omogočen dostop do teh kartotek le določenim osebam.[6] V bolnišnicah pa se že uporabljajo sistemi za avtomatizirano dajanje zdravil in njihovih ustreznih doz pacientom, kar zmanjša človeške napake. Da pri tem ne pride do zlorab, je prav tako potrebno ustrezno šifriranje.[7] V nadaljevanju podajamo pregled klasičnih načinov šifriranja, s poudarkom na njihovih slabostih. Te pomanjkljivosti odpravljajo novi kriptografski postopki v sklopu post-kvantne in kvantne kriptografije, ki predstavlja teoretično nezlomljivo šifriranje. Zato so kasneje predstavljena načela delovanja kvantne kriptografije, njene pomanjkljivosti in izboljšave.

Kriptografija

Sporočilo lahko varno prenesemo na dva načina. Prvi je, da izvirno sporočilo prenesemo preko zaupanja vrednega medija. Tu tvegamo, da mediju prisluškujejo oziroma nanj vplivajo nepovabljeni gostje. Primer takega pošiljanja sporočila je uporaba zaupanja vrednega kurirja, ki mu fizično izročimo sporočilo, ki ga dostavi naslovniku. Naslovnik mora vedeti, da bo naše sporočilo prišlo le preko tega kurirja, da s tem zagotovimo avtentičnost sporočila. A že tu se vidi pomanjkljivost tega načina komuniciranja. Kurir je lahko nepošten ali pa ga na poti oropajo. Sodobnejša izvedba takšnega načina prenosa sporočil je izgradnja namenske komunikacijske linije, npr. iz optičnih vlaknen, neposredno od pošiljatelja do naslovnika. A tudi te niso povsem varne, saj je praktično nemogoče zagotoviti, da nihče ne prisluškuje prenosnemu mediju.[1]

Pogosteje se uporablja varnejši način prenosa sporočil, ki je uporaben tudi pri t. i. nezavarovanem kanalu, ki mu lahko prisluškujejo. Vsebino sporočila zakrijemo pred prisluškovalci z uporabo raznih šifrirnih postopkov. Z razvojem teh postopkov se ukvarja kriptografija. Šifrirni postopki lahko tudi zagotovijo dokaz o avtentičnosti sporočila. S tem prejemnik lahko preveri, ali je bilo sporočilo ponarejeno in ne izhaja od pravega pošiljatelja.

Seveda zagotavlja največjo varnost kombinacija obeh opisanih postopkov. Toda prvi se zaradi velikega finančnega vložka le redko uporablja v vsakdanji praksi.

Osnovno načelo šifriranja je, da originalno sporočilo pošiljatelj spremeni v obliko, ki jo zna razbrati le naslovnik. Da lahko naslovnik edini razbere sporočilo, mora imeti dodatno informacijo, ki je ostali nimajo. Ta se v kriptografiji imenuje *ključ*. Ključ se uporabi tudi pri formiranju šifriranega sporočila. Šifrirano sporočilo naj bi bilo možno razbrati (v omejenem času) le s pomočjo pravega ključa in z vnaprej dogovorjenim šifrirnim algoritmom. Ločimo dva načina šifriranja, in sicer *simetrično* in *asimetrično*. Vsak način ima svoje prednosti in slabosti.

Simetrična kriptografija

Simetrični šifrirni postopki uporabljajo isti ključ tako za šifriranje kot za dešifriranje sporočila. Šifriranje in dešifriranje s simetričnimi postopki je veliko hitrejše kot pri uporabi asimetričnih, a imajo veliko pomanjkljivost: pošiljatelj in naslovnik morata poznati ključ. Prenos tega mora biti povsem varen, sicer je vsa nadaljnja komunikacija ogrožena. Za zagotavljanje dolgotrajne varne komunikacije je potrebno ključe pri simetričnemu šifriranju dovolj pogosto menjati.[1,8] Problem prenosa ključa pa odpravljajo asimetrični postopki.

One-time pad

Oznaka *one-time pad* pomeni poseben simetrični šifrirni postopek, ki zagotavlja popolno varnost pošiljanja sporočil. Takšno varnost lahko zagotovimo le, če

uporabimo povsem naključen ključ, dolžine večje ali enake kot je poslano sporočilo. Ključ pa smemo uporabiti le enkrat. Če so ti pogoji izpolnjeni, je takšno sporočilo nemogoče razbrati brez poznavanja ključa.[9] Največja slabost tega postopka je ravno generacija povsem naključnega ključa in njegov prenos do naslovnika. To težavo odpravlja kvanta kriptografija.

Asimetrična kriptografija

Asimetrično kriptografijo imenujemo tudi kriptografija z javnim ključem. Pri tem načinu se za varno komunikacijo uporabljata dva različna ključa – en zasebni in en javni. Javni ključ da uporabnik na voljo vsem, zasebnega pa skrije. S pomočjo javnega ključa prejemnika lahko vsak šifrira svoje sporočilo, ki ga želi poslati prejemniku. S svojim zasebnim ključem pa lahko le prejemnik dešifrira sporočilo, ki mu ga je pošiljatelj poslal z uporabo prejemnikovega javnega ključa.

Asimetrična kriptografija omogoča tudi avtentikacijo sporočila. Pošiljatelj se poleg poslanega sporočila podpiše, za kar uporabi svoj zasebni ključ. Podpis lahko prejemnik enostavno dešifrira z javnim ključem pošiljatelja. Pri tem ugotovi, ali je sporočilo pristno (tj. poslano od pravega pošiljatelja).

Pri asimetričnih šifrirnih postopkih ni težav s pošiljanjem ključev. Toda tudi asimetrični postopki imajo svojo slabost, in sicer računsko zahtevnost. Ker so veliko počasnejši kot simetrični algoritmi, niso uporabni za dolga sporočila. Zato se v praksi uporablja kombinacija obeh šifrirnih postopkov. S pomočjo asimetričnega postopka šifriramo ključ za simetrično šifriranje, s katerim šifriramo sporočilo. S tem lahko hkrati varno in hitro pošljemo naslovniku tako ključ kot tudi sporočilo. Z asimetričnim šifriranjem dodamo sporočilu še podpis, s čimer zagotovimo avtentikacijo.[1,10]

Asimetrični šifrirni postopki se samostojno ali v kombinaciji s simetričnimi uporabljajo v ogromno različnih aplikacijah, ki segajo od šifriranja elektronske pošte do povezav VPN (angl. *virtual private network).*[11] Zaradi narave komunikacije v e-zdravstvu se tudi tu množično uporablja asimetrično šifriranje.[4,5]

Asimetrični šifrirni postopki temeljijo na matematičnih problemih, za katere ne obstajajo hitri računalniški algoritmi. Eden takih problemov je iskanje praštevil, na čimer temelji tudi eden izmed najbolj razširjenih asimetričnih šifrirnih postopkov, imenovan RSA. Pri postopku RSA se (poenostavljeno rečeno) zasebni ključ sestavi iz dveh naključno izbranih praštevil, javni pa iz njunega produkta. Če bi javni ključ razbili nazaj na njegove prafaktorje, bi s tem razkrili zasebni ključ. A slednje je v praksi malo verjetno. Tudi najhitrejši algoritmi iskanja prafaktorjev imajo namreč eksponentno časovno odvisnost (e^x). To pomeni, da če vzamemo za javni ključ dovolj veliko število, praktično ni verjetno, da bi našli njegove prafaktorje. Za velikosti števil iz 1024 ali 2048 bitov bi za izračun prafaktorjev potrebovali več časa, kot je staro vesolje, četudi bi hkrati uporabili vse računalnike na svetu.[1,12]

Kvantni računalniki – nevarnost dosedanji kriptografiji

Kvantni računalniki predstavljajo grožnjo komunikaciji, ki uporablja široko razširjene asimetrične postopke, kot je RSA (poimenovan po avtorjih Rivestu, Shamirju in Adlemanu). Sicer so šele v začetnem razvoju, a napredujejo hitro in vztrajno. Gonilo tega napredka so tudi nova dognanja na področju kvantne mehanike, kjer sodelujejo tudi slovenski znanstveniki. Nedavno so ravno strokovnjaki z Instituta Jožef Stefan potrdili obstoj posebnih kvazidelcev – anyonov, za katere je pričakovati, da bodo zaradi svoje stabilnosti pomembni za razvoj kvantnega računalništva.[13,14]

Kvanti računalniki uporabljajo drugačne algoritme kot klasični in za nekatere probleme so kvantni algoritmi znatno hitrejši. Eden izmed takšnih je Shorov kvantni algoritem za iskanje prafaktorjev, ki ima polinomsko časovno zahtevnost (x^3) za razliko od eksponentne časovne zahtevnosti klasičnih algoritmov.[15-17]

Sicer kvantni računalniki še niso dovolj obsežni, da bi lahko tudi kljub znatno hitrejšim algoritmom strli RSA in podobne asimetrične šifrirne algoritme, a v prihodnjih 10 do 15 letih se bo to zelo verjetno zgodilo.[11,17] Tedaj bo ogrožena tudi vsa varnost in zasebnost pri obstoječih komunikacijah v medicinske namene. Zato že danes iščejo nove šifrirne postopke, ki bi bili odporni na napade s kvantnimi računalniki. Ponujata se dve rešitvi. Prva rešitev je uporaba t. i. post-kvantne kriptografije, drugo rešitev pa omogoča ravno kvantna mehanika, ki je pripeljala do kvantnih računalnikov in ogrozila varnost dosedanje kriptografije.

Trenutno stanje še ni kritično. Google je nedavno objavil, da so razvili računalnik s 72 qubiti.[18] A predvideva se, da bi bilo za zlom šifriranja RSA z dolžino ključa 2048 bitov v doglednem času potreben kvantni računalnik s 4000 qubiti in 100 milijoni vrat[17] oziroma po drugih predvidevanjih 10000 qubitni računalnik,[19] za kar pa bo potrebnih še kar nekaj let.

Post-kvantna kriptografija

Post-kvantna kriptografija se osredotoča na razvoj kriptografskih metod v času, ko bodo imeli kvantni računalniki dovolj računske moči, da zlomijo obstoječe asimetrične načine šifriranja podatkov. Predvideva, da kvantni računalniki ne bodo sposobni razbiti vseh obstoječih metod šifriranja. Simetrične šifrirne algoritme naj bi bilo enostavno narediti odporne proti napadom s kvantnimi računalniki z enostavnim povečanjem (podvojitvijo) dolžine ključa.[17] A kot smo že omenili, imajo ti slabost zaradi potrebne razdelitve ključev preko varnega kanala. Tudi nekateri načini šifriranja z uporabo javnih ključev naj bi bili sicer odporni na napade s kvantnimi računalniki. Primer takšnih postopkov je šifriranje, ki temelji na enosmernih zgoščevalnih funkcijah, a te imajo omejitev v številu uporabe enega kompleta ključev za šifriranje.[20] Obstajajo še drugi načini šifriranja, odporni na kvantne napade,[11] vendar imajo za enkrat še vsak svojo pomanjkljivost (zelo dolgi ključi, časovno zahtevni šifrirni postopki, ne omogočanje avtentikacije itd.[21]), zato še niso splošno razširjeni. Ključna prednost post-kvantne kriptografije pred ostalimi tehnikami, odpornimi na napade s kvantnimi računalniki, kot je uporaba kvantne kriptografije, je njena preprostost in poceni implementacija na obstoječih sistemih.[21]

Glede razvoja kvantnih računalnikov je sicer še veliko vprašanj, predvsem glede kvantnih algoritmov. Dejstvo je, da je to področje zelo novo v primerjavi z razvojem klasičnih algoritmov. Tako obstaja možnost, da bodo razvili tudi kvantne algoritme, ki bi lahko razbili predlagane post-kvantne algoritme šifriranja. Na srečo se ponujajo še drugi načini šifriranja, odporni na napade s kvantnimi računalniki, z uporabo kvantne kriptografije.

Kvantna kriptografija

Kvantna kriptografija predstavlja drugi način šifriranja podatkov, ki bi bil odporen tudi na napade s kvantnimi računalniki. Še več, kvantna kriptografija vsaj teoretično omogoča nezlomljivo šifriranje.

Kot smo že omenili, je za vsako varno komunikacijo potrebno podatke šifrirati s ključem. Ta ključ mora biti znan le naslovniku in pošiljatelju. Najbolje je, da je ključ povsem naključno generiran, ker ga je tako najtežje uganiti, a popolno naključnost je težko zagotoviti. Primeri povsem naključnih pojavov so kvantne narave. Te uporablja kvantna kriptografija in z njimi odpravlja težave na področju generiranja naključnega ključa.[1]

Ko je ključ generiran, se ga lahko uporabi za komunikacijo preko nezavarovanega kanala z znanimi šifrirnimi postopki. Če se pri teh uporabi šifriranje po načelu one-time pad, lahko zagotovimo povsem nezlomljivo komunikacijo.[17,22-24]

Obstaja več protokolov za t. i. kvantno izmenjavo ključa (angl. *quantum key distribution, QKD*). Najbolj razširjena je uporaba protokola BB84 oziroma njegovih izvedenk. Te protokole so že uporabili za šifriranje podatkov pri telemedicinski oskrbi na daljavo.[25] Protokol BB84 deluje na podlagi oddajanja in sprejemanja posamičnega fotona. Ta protokol, njegovo fizično izvedbo in trenutne pomanjkljivosti predstavljamo v nadaljevanju. Na voljo so še drugi protokoli, ki delujejo npr. na podlagi kvantne prepletenosti, a so zaradi težavne praktične izvedbe le eksperimentalno uporabni.[22,26-28]

Delovanje

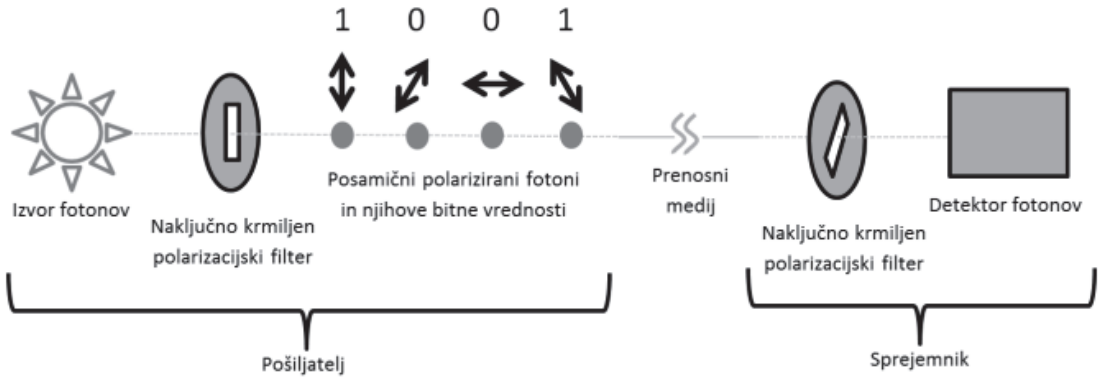
Kvantna kriptografija deluje po načelu oddajanja in sprejemanja posamičnih fotonov z različnimi polarizacijami (slika 1).

Uporabimo dve polarizacijski bazi, in sicer premočrtno in diagonalno. Pri premočrtni bazi so fotoni lahko polarizirani v vodoravni smeri (kot polarizacije 0°) ali v navpični smeri (kot polarizacije 90°), pri diagonalni bazi pa je kot polarizacije 45° ali 135°. Pri tem po ena polarizacija fotona v vsaki bazi predstavlja bit z vrednostjo 0 (na primer horizontalna polarizacija s kotom 0° v premočrtni bazi in polarizacija s kotom 45° v diagonalni), druga polarizacija pa bit z vrednostjo 1 (navpična polarizacija in polarizacija s kotom 135°).

Bazi sta tako izbrani s posebnim namenom. Če namreč pri detekciji polarizacije fotona uporabimo napačno bazo, je verjetnost 50 %, da zaznamo foton, kot da bi bil polariziran s polarizacijo, ki predstavlja bit z vrednostjo 0, verjetnost 50 % pa tudi, da ga zaznamo kot foton, ki nosi bit z vrednostjo 1. Zato z uporabo napačne baze pri detekciji ne moremo pravilno razbrati bitne vrednosti fotona.

Postopek generacije ključa poteka tako, da pošiljatelj zaporedoma oddaja posamične fotone. Pri vsakem fotonu se naključno odloči za polarizacijsko bazo in prav tako za njegovo vrednost. S tem naključno izbere polarizacijo fotona in njegovo bitno vrednost. Prejemnik sprejema oddane fotone. Pri tem želi razbrati vrednost bita. Ker ne ve, s katero polarizacijsko bazo je bil foton oddan, se naključno odloči za eno od možnih. Tako razbere bitno vrednost nekaterih fotonov pravilno, drugih napačno. Ko pošiljatelj neha oddajati, mu sprejemnik pošlje

njegovo zaporedje uporabljenih baz. Ta preveri, pri katerih fotonih sta uporabila enako bazo (za oddajo in sprejem), kar sporoči prejemniku. Nato ohranita le tiste bite, pri katerih sta uporabila enako bazo, saj imata pri teh oba pravilno razbrano vrednost. Ti sprejeti biti predstavljajo ključ. Ta je naključen, ker se je pošiljatelj naključno odločal za posamično vrednost bita. Za nadaljnjo komunikacijo preko nezavarovanega kanala uporabita dobljeni ključ, kjer lahko uporabita klasične simetrične postopke šifriranja.



Slika 1 Poenostavljen shematski prikaz kvantne izmenjave ključa.

Velika prednost takega načina pridobitve ključa je, da tretja oseba, ki morda prisluškuje kanalu, ne more ugotoviti ključa, ne da jo pri tem odkrili. To izhaja iz Heisenbergovega načela nedoločenosti. Posledica načela nedoločenosti je, da je nemogoče narediti kopijo neznanega kvanta, ne da bi z njegovo meritvijo spremenili njegove lastnosti.[23,29]

Tudi če v predstavljenem primeru prisluškovalec prisluškuje komunikaciji in prestreže vsak foton, ne ve, v kateri bazi je bil foton oddan. Tako se mora tudi on naključno odločiti. Če slučajno izbere pravo bazo, bo pravilno razbral tudi poslani bit. Ko pa se odloči za napačno, lahko pravilno razbere bit ali ne. Toda pri tem bo spremenil polarizacijo fotona v napačno bazo. Če pri sprejemu tega fotona sprejemnik uporabi enako polarizacijsko bazo za sprejem fotona, kot jo je pošiljatelj pri oddajanju, je 50 % verjetnosti, da bo kljub pravi bazi zaznal napačno vrednost bita. Zato po koncu postopka določanja ključa pošiljatelj in sprejemnik naključno primerjata nekaj bitov, pri katerih sta uporabila enako bazo. Zaradi enake baze bi morala dobiti enako vrednost. Če vrednosti primerjanih bitov niso povsem enake, vesta, da je nekdo prisluškoval kanalu in pri tem spremenil vrednost bita. Zato šifra ni varna. Če pa se vsi primerjani biti ujemajo, je velika verjetnost, da je bil ključ varno generiran. Iz končnega ključa se izvzamejo primerjani biti. Da se lahko določi prisotnost prisluškovalca na kanalu z verjetnostjo 0,999999999, je potrebno primerjati 72 bitov.

Zaradi povsem naključne izbire polarizacijske baze na pošiljateljevi in sprejemni strani ter naključne izbire poslanih bitov lahko poteka končno preverjanje bitov in vmesno deljenje informacij o izbiri baz po nezavarovanem kanalu. Tudi če prisluškovalec te informacije prestreže, mu nič ne koristijo. Primerjane vrednosti dobljenih bitov se namreč, kot rečeno, na koncu izvzamejo. Podatki o izbiri baz pa so prisluškovalcu prav tako nekoristni, če je sam uporabil napačne baze pri prestrezanju posamičnega fotona, saj potem ne ve, ali je pri njih razbral pravo vrednost.[30]

Izvedba kvantne kriptografije

Za kvantno izmenjavo ključa potrebujemo ustrezno opremo. Sestavljajo jo štirje deli: generator naključnih števil oziroma bitov, izvor fotonov, prenosni kanal in detektor fotonov, ki so v nadaljevanju podrobneje predstavljeni.

Generator naključnih števil oziroma bitov

Izhod generatorja naključnih števil za kvantno izmenjavo ključa mora biti povsem naključen, sicer je ogrožena varna generacija ključa v primeru prisluškovanju prenosnemu kanalu. Prisluškovalec bi lahko tako ugotovil, kakšne vrednosti bitov oddaja pošiljatelj ali kakšne polarizacijske baze uporabljata pošiljatelj in sprejemnik. Tako bi ključ lahko ugotovil zelo hitro.

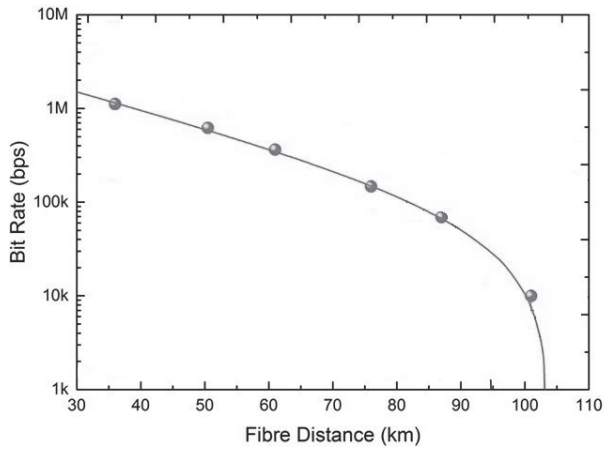
Programski generatorji psevdonaključnih števil ne delujejo povsem naključno in se zato kljub nizki ceni ne uporabljajo. Potrebno je uporabiti mnogo dražje strojne generatorje naključnih števil. Ti temeljijo na nedeterminističnih fizikalnih pojavih, kot so termični in Zenerjev šum, radioaktivni razpad in prehod fotona skozi polprepustno zrcalo.[24,31]

Izvor fotonov

Za idealno kvantno izmenjavo ključa, ki je povsem varna, bi potrebovali izvor posamičnih fotonov. V praski se pogosto uporabljajo atenuirani laserji, ki sicer ne omogočajo izvora posamičnega fotona. Nevarnost te neidealnosti lahko do neke mere odpravimo z dopolnjenimi protokoli. Kljub temu te nadgradnje niso povsem varne, zato se veliko raziskuje na področju eno-fotonskih izvorov. Cilj je, da delujejo pri valovnih dolžinah v infrardečem spektru, ki se najmanj absorbirajo v optičnih vlaknih, ki so najbolj pogost medij prenosa pri kvantni izmenjavi ključa.[22,24,32,33]

Prenosni kanal

Najbolj pogosto je izveden kot optično vlakno. Po njih se dosegajo največje hitrosti izmenjave kvantnega ključa. Nedavno so dosegli 13,7 Mbit/s na razdalji 10 km,[33] na daljših razdaljah pa 1 Mbit/s na 50 km[34] oziroma 12,7 kbit/s na 307 km (slika 2).[22] Vedno bolj se razvijajo tudi načini izmenjave kvantnega ključa preko satelitov.[24,27]



Slika 2 Primer izmerjene odvisnosti hitrosti prenosa kvantnega ključa od dolžine optičnega vlakna.[36]

Detektor fotonov

Za detekcijo fotonov se pogosto uporabljajo diode s plazovno ionizacijo, kot so InGaAs diode. Te delujejo pri valovnih dolžinah v infrardečem spektru, kakršni so pogosto tudi viri fotonov pri kvantni izmenjavi ključa.[35,37] Veliko pa se raziskuje tudi na eno-fotonskih detektorjih, narejenih npr. iz superprevodnih nanocevk.[32]

Trenutne pomanjkljivosti kvantne kriptografije

Čeprav naj bi kvantna kriptografija zagotavljala popolnoma varno komunikacijo, je trenutno še ne. Elementi, uporabljeni za izgradnjo sistema za kvantno izmenjavo ključa, niso idealni. Neidealnosti v izvirih in detektorjih fotonov lahko izrabijo napadalci.[22-24,28] Da se izognemo takšnim napadom, je potrebno nadgraditi protokole kvantne izmenjave ključa. Kot smo že omenili, potekajo raziskave eno-fotonskih izvorov in detektorjev, ki bi odpravili te pomanjkljivosti.[32]

Nezmožnost oddaje posamičnega fotona

Praktično uporabljeni fotonski izvori ne proizvedejo le enega fotona, ampak lahko več, ki vsebujejo enako informacijo. To neidealnost lahko izkoriščajo prisluškovalci tako, da detektirajo le en poslani foton. Ker je bilo teh več, lahko sprejemnik še vedno pravilno zazna foton in informacijo. Zato je potrebno predstavljen protokol BB84 nadgraditi. Najbolj razširjena je nadgradnja z vabami (angl. *decoy-state QKD*). Pri tem pošiljatelj naključno pošlje vabo – namensko drugačno število fotonov, ki ne vsebujejo sporočila. Prisluškovalec ne ve, kdaj je poslana vaba in kdaj ne. Če prestreže vabo, potem do sprejemnika prispe napačno število fotonov. Na koncu komunikacije pošiljatelj sporoči sprejemniku, kdaj je poslal vabo. Če je takrat ta zaznal nepravilna števila zaznanih fotonov, sta odkrila prisotnost prisluškovalca.[28,30,37-39]

Trojanski konj

Napad s trojanskim konjem v kvantni kriptografiji poteka tako, da napadalec z močnim svetlobnim snopom obsveti sprejemnik. Iz odbite svetlobe lahko napadalec pravilno sklepa o uporabljeni polarizacijski bazi sprejemnika, s čimer enostavno zlomi šifriranje. Kot ustrezna zaščita proti takšnim napadom se uporabljajo optični izolatorji in filtri.[22]

Napad na kalibracijski postopek

Napadalci lahko izrabijo tudi neidealnosti v detektorjih fotonov. V procesu kalibracije pred začetkom dejanske komunikacije lahko prestrežejo kalibracijski proces in vsilijo svojega. Z njim lahko vsilijo oziroma spremenijo polarizacijsko bazo detektorja. S tem lahko napadalec kasneje med izmenjavo ključa prestreže več fotonov, ne da bi ga odkrili. To pomanjkljivost naj bi v prihodnosti odpravili s samo-preizkuševalnimi metodami za detektorje fotonov v sistemu, kar pa naj bi dodatno dvignilo njihovo ceno.[23,28]

Drugi možni vdori in zlorabe

Kot pri drugih varnostnih sistemih, je tudi tu potrebno preprečiti fizični dostop napadalcev do komunikacijskega sistema. Zagotoviti je potrebno

tudi povsem naključne generatorje števil. Če ta pogoja nista izpolnjena, je verjetnost uspešnega vloma v sistem bistveno večja.

Trenutna pomanjkljivost kvantne kriptografije je tudi avtentikacija pošiljatelja in sprejemnika. Z njo ugotovimo oziroma potrdimo identiteto sogovorca. Doslej še niso razvili kvantnih metod avtentikacije, zato se uporabljajo klasične. Če se napadalcu uspe izdajati za zaupanja vrednega sogovornika, je varna komunikacija zlomljena.

Poleg tega je pri kvantni kriptografiji potrebno imeti vzpostavljen neprekinjen kanal med pošiljateljem in sprejemnikom. Napadalec lahko enostavno prekine ta kanal in tako izvede napad zavrnitve storitve (angl. *Denial of Service*, *DoS*). Komunikacijski kanali so trenutno še tudi zelo omejeni glede dolžine, na kateri je mogoče zagotoviti prenos uporabne hitrosti. Da bi jo povečali, raziskujejo v smeri satelitske kvantne izmenjave ključa in razvoja omrežij za kvantno izmenjavo ključa. Slednja bi tudi povečala zahtevnost izvedbe napada DoS, saj bi lahko komunikacija potekala preko različnih kanalov. Toda za zdaj še niso uspeli izdelati kvantnega usmerjevalnika, ki bi bil v takih omrežjih potreben. Moral bi namreč za nekaj časa shraniti foton, ga pri tem ne spremeniti, in poslati naprej, česar pa za zdaj še ne znamo.[17,22,24,27]

Zaključek

Trenutno še ni razloga za preplah zaradi mogočega padca klasične kriptografije in kaosa, ki bi temu sledil – zloma finančnih sistemov, kraje osebnih identitet in zdravstvenih kartotek, manipulacije z osebnimi podatki itd. Kvantni računalniki, ki predstavljajo največjo grožnjo tradicionalni kriptografiji, še niso dovolj razviti. To naj bi se po nekaterih ocenah spremenilo v roku 10 do 15 let. V sklopu post-kvantne kriptografije in kvantne kriptografije se že pojavljajo načini šifriranja, ki so odporni tudi na napade s kvantnimi računalniki.

Obe tehnologiji sta novi in še ne povsem uporabni v praksi. Post-kvantna kriptografija predstavlja cenejšo rešitev, saj naj bi le nadgradili kriptografske postopke, ki so sedaj v uporabi. Zanjo ni potrebna nobena nova strojna oprema. A tudi ta se bo mogoče izkazala za zlomljivo, saj je razvoj kvantnih računalnikov in kvantnih algoritmov šele v povojih. Tako se bo morda kljub višji ceni in potrebni novi strojni opremi izkazala kvantna kriptografija za boljšo rešitev, saj je teoretično nezlomljiva. Za zdaj pa ima še kar nekaj pomanjkljivosti, predvsem zaradi praktičnih omejitev izvorov in detektorjev fotonov.

Reference

1. Singh S: *Knjiga šifer: umetnost šifriranja od starega Egipta do kvantne kriptografije*. Tržič 2008: Učila International.
2. Anon: *History of crypthography*. https://en.wikipedia.org/wiki/History_of_cryptography (4. 5. 2018)
3. Thibaud M, Chi H, Zhou W, Piramuthu S: Internet of Things (IoT) in high-risk environment, health and safety (EHS) industries: a comprehensive review. *Deci Support Syst* 2018; 108: 79-95. https://doi.org/10.1016/j.dss.2018.02.005
4. Tan Z: A user anonymity preserving three-factor authentication scheme for telecare medicine information systems. *J Med Syst* 2014; 38(3): 16-25. https://doi.org/10.1007/s10916-014-0016-2
5. Chaudhry SA, Mahmood K, Naqvi H, Khan MK: An improved and secure biometric authentication scheme for telecare medicine information systems based on elliptic curve cryptography. *J Med Syst* 2015; 39(11): 175-187.
6. Odelu V, Das AK, Goswami A: An Effective and Secure Key-Management Scheme for Hierarchical Access Control in E-Medicine System. *J Med Syst* 2013; 37(2): 9920-9938. https://doi.org/10.1007/s10916-012-9920-5
7. Jin C, Xu C, Zhang X, Li F: A secure ECC-based RFID mutual authentication protocol to enhance patient medication safety. *J Med Syst* 2016; 40 (1): 12-18. https://doi.org/10.1007/s10916-015-0362-8
8. Anon: *Symmetric-key algorithm*. https://en.wikipedia.org/wiki/Symmetric-key_algorithm (6. 5. 2018)
9. Anon: *One-time pad*. https://en.wikipedia.org/wiki/One-time_pad (6. 5. 2018)
10. Anon: *Public-key cryptography*. https://en.wikipedia.org/wiki/Public-key_cryptography (6. 5. 2018)
11. Mulholland J, Mosca M, Braun J: The Day the Cryptography Dies. *IEEE Security & Privacy* 2017; 15(4): 14-21.
12. Anon: *RSA (cryptosystem)*. https://en.wikipedia.org/wiki/RSA_(cryptosystem) (7. 5. 2018)
13. Janša N, Zorko A, Gomilšek M, *et al*: Observation of two types of fractional excitation in the Kitaev honeycomb magnet. *Nat Phys* 2018; 14: 786-790. https://doi.org/10.1038/s41567-018-0129-5 (3. 10. 2018)
14. Masten A: *Raziskovalci IJS-ja potrdili obstoj delcev, o katerih je razmišljal že Nobelov nagrajenec*. https://www.rtvslo.si/znanost-in-tehnologija/raziskovalci-ijs-ja-potrdili-obstoj-delcev-o-katerih-je-razmisljal-ze-nobelov-nagrajenec/454399/ (9. 5. 2018)
15. Smole F: *Nanoelektronika*. Ljubljana 2014: Založna FE in FRI.
16. Anon: *Shor's algorithm*. https://en.wikipedia.org/wiki/Shor%27s_algorithm (7. 5. 2018)

17. Moses T: *Quantum Computing and Cryptography: Their impact on cryptographic practice*. Addison 2009: Entrust Inc.
18. Oberhaus D: *Google Engineers Think This 72-Qubit Processor Can Achieve Quantum Supremacy*. https://motherboard.vice.com/en_us/article/pam958/bristlecone-google-quantum-computer-72-qubits/ (7. 5. 2018)
19. Ziegler L: *Online security, cryptography, and quantum computing*. Forum Lectures, paper 119. https://digitalcommons.csbsju.edu/cgi/viewcontent.cgi?referer=&httpsredir=1&article=1118&context=forum_lectures/ (7. 5. 2018)
20. Anon: *Post-quantum cryptography*. https://en.wikipedia.org/wiki/Post-quantum_cryptography (7. 5. 2018)
21. Sendrier N: Code-Based Cryptography: State of the Art and Perspectives. *IEEE Security & Privacy* 2017; 15(4): 44-50.
22. Anon: *Quantum key distribution*. https://en.wikipedia.org/wiki/Quantum_key_distribution (10. 5. 2018)
23. Xu F, Curty M, Qi B, Lo HK: Measurement-device-independent quantum cryptography. *IEEE J Sel TopQuantum Electron* 2015; 21(3). https://doi.org/10.1109/JSTQE.2014.2381460
24. Lo HK, Curty M, Tamaki K: Secure quantum key distribution. *Nat Photonics* 2014; 8: 595-604. https://doi.org/10.1038/nphoton.2014.149
25. Lai H, Luo M, Qu Z, Xiao F, Orgun MA*:* A hybrid quantum key distribution protocol for tele-care medicine information systems. *Wirel Pers Commun* 2018; 98(1): 929-943. https://doi.org/10.1007/s11277-017-4902-z
26. Stein B: *Cost Effective QKD System Developed By NIST*. https://www.nist.gov/information-technology-laboratory/cost-effective-qkd-system-developed-nist/ (10. 5. 2018)
27. Bedington R, Arrazola JM, Ling A: Progress in satellite quantum key distribution. *NPJ Quantum Infmn* 2017; 3(30). https://doi.org/10.1038/s41534-017-0031-5
28. Fei YY, Meng XD, Gao M, *et al*: Quantum man-in-the-middle attack on the calibration process of quantum key distribution. *Scientific Reports* 2018; 8(4283). https://doi.org/10.1038/s41598-018-22700-3
29. Anon: *No-cloning theorem*. https://en.wikipedia.org/wiki/No-cloning_theorem (8. 5. 2018)
30. Anon: Quantum cryptography. https://en.wikipedia.org/wiki/Quantum_cryptography (8. 5. 2018)
31. Stipčević M: *Quantum random number generators and their use in cryptography*. https://arxiv.org/ftp/arxiv/papers/1103/1103.4381.pdf (9. 5. 2018)
32. Takemoto K, Nambu Y, Miyazawa T, *et al*: Quantum key distribution over 120 km using ultrahigh purity single-photon source and superconducting single-photon detectors. *Sci Rep* 2015; 5(14383). https://doi.org/10.1038/srep14383
33. Slachter A: *Single Photon Emitters*. https://www.rug.nl/research/zernike/education/topmasternanoscience/ns190slachter.pdf (9. 5. 2018)
34. Anon: *Toshiba Pushes Quantum Key Distribution Speed Beyond 10Mbps*. https://www.toshiba.co.jp/about/press/2017_09/pr1501.htm (9. 5. 2018)
35. Anon: *Toshiba QKD system*. https://www.toshiba.eu/eu/Cambridge-Research-Laboratory/Quantum-Information/Quantum-Key-Distribution/Toshiba-QKD-system/ (9. 5. 2018)
36. Dynes JF: Ultra-high bandwidth quantum secured data transmission. *Sci Rep* 2016; 6(35149). https://doi.org/10.1038/srep35149
37. Pljonkin A, Rumyantsev K, Singh PK: Synchronization in Quantum Key Distribution Systems. *Cryptography* 2017; 1(3): 18.
38. Maroy O, Makarov V, Skaar J: Secure detection in quantum key distribution by real-time calibration of receiver. *Quantum Sci Technol* 2017; 2(4).
39. Huang A, Sun SH, Liu Z, Makarov V: *Decoy state quantum key distribution with imperfect source*. https://arxiv.org/abs/1711.00597/ (11. 5. 2018)