(19) REPUBLIKA SLOVENIJA
MINISTRSTVO ZA GOSPODARSKI RAZVOJ IN TEHNOLOGIJO
URAD RS ZA INTELEKTUALNO LASTNINO

(10) SI 23596 A

(12) # PATENT

(21) Številka prijave: **201000460**

(22) Datum prijave: **28.12.2010**

(51) Int. Cl. (2012.01)
H04L 9/00

(45) Datum objave: **29.06.2012**

(72) Izumitelja: **Novak Roman, 1231 Ljubljana, SI;**
Vencelj Matjaž, 1231 Ljubljana, SI

(73) Imetnik: **Institut Jožef Stefan",**
Jamova 39, 1000 Ljubljana, SI

(74) Zastopnik: **ITEM d.o.o. Zastopniška pisarna za patente in blagovne znamke, Resljeva 16, 1000 Ljubljana, SI**

(54) **METODA IN NAPRAVA ZA KVANTNO DISTRIBUCIJO KLJUČA KRATKEGA DOSEGA**

(57) Metoda za kvantno distribucijo ključa kratkega dosega temelji na prepletenih kvantnih stanjih fotonov gama. Izkorišča Comptonovo interakcijo fotonov s snovjo za vzpostavitev kvantnega kanala med legitimnima entitetama. Koreliranost detektiranih azimutnih kotov po sipanju prepletenih fotonov tvori konceptualni šumni kanal z znano mejo šuma. Protokol za distribucijo ključa z izmenjavo sporočil preko javnega komunikacijskega kanala omogoči uskladitev bitov ključa v visokošumnem okolju z uporabo izbrane sheme za korekcijo napak. Podani sta tudi dve konstrukcijski rešitvi naprave za realizacijo metode, vključno s parametri za maksimizacijo bitne hitrosti usklajenega ključa pri konstantni aktivnosti izvorov za primer binarnega kodirnika.

SI 23596 A

Metoda in naprava za kvantno distribucijo ključa kratkega dosega

Predmet izuma sta metoda in naprava za kvantno distribucijo ključa kratkega dosega v energijskem področju žarkov gama. Izum rešuje problem brezpogojnega ščitenja komunikacij, identifikacije in avtorizacije sodelujočih entitet, ko se le-te nahajajo blizu ena drugi.

1. Prikaz tehničnega problema

Kvantna distribucija ključa (QKD - Quantum Key Distribution) je alternativa matematičnim rešitvam za vzpostavitev skupnega ključa med dvema entitetama. Ključ je potreben v vseh simetričnih kriptografskih shemah, kjer se zahteva poznavanje skupne skrivnosti. Pogosto ga imenujemo tudi sejni ključ. Klasični postopki za vzpostavitev skupnega ključa, kot je na primer protokol Diffie-Hellman, gradijo trdnost ključa na računski zahtevnosti izbranih matematičnih algoritmov. Kljub temu, da danes ti postopki še veljajo za trdne, teoretična dognanja s področja kvantnih računalnikov varnost tovrstnih shem postavljajo pod vprašaj. Čeprav kvantni računalniki še niso realnost, so zahteve za močnejše kriptografske sheme vsekakor prisotne že danes.

Kvantna distribucija ključa omogoča razširitev klasičnih kriptografskih shem s postopki, s katerimi je moč izmenjati skupno skrivnost med dvema entitetama na brezpogojno varen način z uporabo zakonov kvantne mehanike. Temeljni princip delovanja kvantne izmenjave ključa se naslanja na teorem o nezmožnosti kopiranja kvantnega sistema (no cloning theorem), ki zavrača kakršnokoli možnost, da pripravimo popolnoma identično kopijo sistema, ki je v neznanem kvantnem stanju. Posledično velja, da vsaka kvantna meritev zmoti sistem, spremembe so merljive in jih je moč zaznati, kar omogoča razkritje nedovoljenega pridobivanja informacije o izmenjanem ključu.

Izmenjava ključa ne poteka vedno na večje razdalje. Aplikacija identifikacije in kontrole dostopa se tipično izvaja na kratke razdalje, kjer je dovoljen tudi neposredni kontakt med napravami. V takih aplikacijah je mehanizem distribucije, ki ne oddaja informacije širše v okolico v prednosti, saj ne

ustvarja potencialnih stranskih kanalov (side channel leakage). Podobne zahteve veljajo tudi za varno identifikacijo večjih naprav, komponent in sistemov.

Osnovni elementi protokolov kvantne distribucije ključa so dobro poznani. Dvoje entitet, običajno ju poimenujemo Ana (Alice) in Boštjan (Bob), je povezanih s kvantnim in istočasno s klasičnim komunikacijskim kanalom. Entiteti si sprva delita ključ za osnovno avtentikacijo, katerega namen je odkriti spremenjena ali potvorjena sporočila na javnem komunikacijskem kanalu ob inicializaciji protokola. Potencialni napadalec, v literaturi poimenovan Eva (Eve), ima tako dostop do vseh sporočil na javnem kanalu, ki pa jih ne more spreminjati, ne da bi bil odkrit. S postopkom kvantne distribucije ključa legitimni entiteti poljubno podaljšata začetni skrivni ključ in ga uporabita v kriptografskih aplikacijah. V postopku distribucije si izmenjata sporočila na standardnem kanalu in opravita priprave/meritve na kvantnem kanalu, pri čemer sledita natanko določenemu protokolu. Idealno se biti ključa uporabijo v kasnejši aplikaciji le enkrat z Vernamovim postopkom šifriranja (one time pad cipher), ki je dokazano popolnoma varen pri predpostavki naključnega ključa.

2. Stanje tehnike

Po pregledu dostopnih doslej znanih rešitev obravnavanega tehničnega problema, deloma zajetih v spodnjem seznamu patentov, sledi, da je predlagana rešitev v okviru te patentne prijave izvirna.

EP2248284	Optical Transmitters and Receivers for Quantum Key Distribution, 2010
US2010150553	Method and Apparatus for Generating Optical Short Pulse for Quantum Cryptography Communication, 2010
CN101645769	Optical System Sharing True Random Number Sequence between Different Places, 2010
US2010002881	Polarization-Insensitive One-Way Quantum Key Distribution Receiver, Transmitter/Receiver System, 2010
WO2009141586	Quantum Key Device, 2009
CN101572600	Plug and Play Quantum Key Distribution Device, 2009
WO2009112286	An Optical Communication System and Method for Secure Data Communication Using Quantum Key Distribution, 2009
US2010166187	QKD Using High-Altitude Platforms, 2010

GB2460252 Alignment System for Freespace QKD in Which a Receiver Transmits an Alignment Beam and Detects a Retro-Reflected Version of the Beam, 2009

Znane teoretične rešitve in komercialno dostopni produkti za kvantno distribucijo ključa so v večini zasnovani na transportnih lastnostih fotonov svetlobe. Kot prenosni medij služi klasično optično vlakno ali prazen prostor oziroma zrak v primeru neposredne vidljivosti. Naprave za kvantno distribucijo ključa v vidnem ali bližnje-infrardečem frekvenčnem območju tipično vsebujejo šibke laserje, polarizatorje, optična stikala, nelinearne optične kristale, itd.

V grobem rešitve za kvantno izmenjavo ključev delimo v dve skupini. V prvi skupini ena entiteta pripravi kvantna stanja, druga pa jih izmeri (prepare and measure), medtem ko v drugi skupini obe entiteti merita prepletena kvantna stanja (entanglement-based).

Zaradi same metode distribucije ključa in zaradi šuma, ki ga ni možno odpraviti, je naknadno potrebno izvesti protokol uskladitve ključa. Temu običajno sledi protokol ojačanja zasebnosti, ki praktično izniči še preostalo minimalno informacijo v posesti prisluškovalca. Obširen opis stanja raziskav in tehnike je na voljo v preglednem članku "The Security of Practical Quantum Key Distribution" (Rev. Mod. Phys., vol. 81, no. 3, 2009, 1301-1350).

Patentirane rešitve, ki vsebujejo tudi opis kvantnega kanala, temeljijo na optični tehnologiji (nekaj primerov: EP2248284, US2010150553, CN101645769, US2010002881, WO2009141586, CN101572600, WO2009112286). Le nekaj jih ne uporablja optičnih vlaken (US2010166187, GB2460252), temveč prazen prostor oziroma zrak.

3. Opis rešitve problema in izvedbena primera

Izum omogoča kvantno distribucijo ključa na kratke razdalje v bistveno višjem energijskem področju žarkov gama. Metoda temelji na uporabi prepletenih kvantnih stanj fotonov gama, ki nastanejo v procesu izničenja delca in antidelca. Kot princip delovanja izkorišča kvantno nedoločenost Comptonovega sipanja fotonov na elektronu, pri čemer delna koreliranost azimutnih kotov sipanja predstavlja osnovo za vzpostavitev šumnega kvantnega kanala z znano mejo šuma. Kvantna distribucija ključa v tako visokem energijskem področju je novost, prav tako je originalna uporaba v nadaljevanju opisanih fizikalnih zakonitosti za specifični namen. Izum zajema tudi dve varianti naprave,

ki predstavljata fizični nivo protokola kvantne distribucije ključa po opisani metodi ter osnovni protokol za uskladitev ključev. Protokol uskladitve omogoča aplikacijo shem za korekcijo napak iz teorije komunikacij in temelji na kodiranem prenosu kod za korekcijo napak naključno generirane vrednosti ključa, pri čemer se za kodiranje/dekodiranje uporabi izmerjeni azimutni kot, za uporabo optimalnih shem korekcije napak pa dovoljuje izmenjavo odklonskega kota sipanja.

Praktične prednosti izuma pred obstoječimi izvedbami so naslednje:

- Kvantni kanal je brezžičen in omogoča komunikacijo skozi tanke zidove, denimo v elektromagnetno ščitene prostore. Vzpostavitev kanala je preprosta tudi v močno prašnem, vibrirajočem, mokrem, kemijsko agresivnem ali kužnem okolju.
- Kratkost dosega in brezpogojna premočrtnost informacijskega toka služi kot močan dodatni varnostni element.
- Opisana metoda je bolj odporna na "napad s cepljenjem fotona" kot optične rešitve, kjer so navadno v rabi šibki laserski bliski, ki občasno vsebujejo več kot en foton. V našem primeru so ekvivalent izjemno redke trifotonske anihilacije, a so zlahka prepoznavne po smeri in energiji žarkov gama; v tipični izvedbi sistema niti ne bi prestale poti do sprejemnika.

Metoda izuma sloni na zakonitostih interakcije fotonov gama s snovjo. V področju energij, ki so značilne za fotone, nastale ob izničenju elektrona in pozitrona, torej 511 keV, je v večini konstrukcijskih materialov dominantni interakcijski proces Comptonovo sipanje. V aluminiju, denimo, je za fotone s 511 keV fotoabsorpcija okoli 600-krat manj verjetna od Comptonovega sipanja, medtem ko so ostale interakcije povsem zanemarljive.

Ob izničenju elektrona in upočasnjenega pozitrona nastaneta fotona z energijama blizu 511 keV, ki odletita v nasprotnih smereh. Fotona sta prepletena tako, da se njuni smeri polarizacije razlikujeta za pravi kot. Ob Comptonovem sipanju fotona na elektronu se polarizacija odrazi v azimutnem kotu eta, to je kotu med ravnino sipanja in električnim vektorjem vpadnega fotona. Verjetnost sipanja v smeri azimutnega kota eta pri danem kotu sipanja glede na smer vpadnega fotona opisuje dobro znani rezultat Kleina in Nishine (Z. Physik (1929), 853).

Meritvi azimutnih sipalnih kotov za prepletena fotona sta torej korelirani. Formula Kleina in Nishine določa periodično razširitev verjetnostne gostote šuma za posamezno meritev azimutnega kota glede na izvorno polarizacijo fotonov. Kvantni kanal, ki se konceptualno ustvari ob meritvah obeh fotonov prepletenega para, pri čemer se meritvi opravita v različnih entitetah, je za potrebe kvantne

distribucije ključa ekvivalenten šumnemu kanalu, za katerega je periodična razširitev verjetnostne gostote šuma enaka krožni konvoluciji prej omenjenih verjetnostnih gostot.

Distribucija ključa med entitetama zahteva kombinacijo meritev in izmenjavo sporočil preko javnega kanala na način, ki ne razkrije informacije o ključu morebitnim poslušalcem na javnem kanalu. Uporabimo lahko naslednji protokol. Naj slučajna spremenljivka S označuje dejansko polarizacijo prepletenega fotona v smeri prve entitete kot azimutni kot relativno na bazni električni vektor, pri čemer vrednost S ni znana. Entiteti dejansko izmerita azimutna kota X in Y za fotona, ki ju detektirata v koincidenci, to je sočasno. Informacijo o časovni znački sprejetega fotona za prepoznavo koincidence si lahko entiteti izmenjata preko javnega kanala, ne da bi pri tem razkrili vrednost meritve. Prva entiteta naključno generira vrednost ključa V, izračuna X + V in pošlje rezultat drugi entiteti. Ta izračuna približek V kot X + V - Y - pi/2. Približek V lahko modeliramo kot V + E, kjer E predstavlja napako z zgoraj opisano verjetnostno gostoto ekvivalentnega šuma.

Ker se X + V pojavi na javnem kanalu, je potrebno zagotoviti minimalno puščanje informacije o V. To dosežemo z uniformno distribucijo X, kar sledi iz zveze I(V;X+V) = H(X+V) - H(X), maksimalnosti entropije uniformne zvezne porazdelitve na danem intervalu in iz ujemanja intervalov podpore X + V in X, pri čemer I označuje skupno informacijo in H entropijo. Čeprav je X meritev fotonov izotropnega vira, distribucija X ni nujno uniformna. Zato mora merilni podsistem v čim večji meri odpraviti deviacije. Varnostna ojačitev ključa, ki se izvede v višjem protokolnem sloju, odpravi morebitna manjša odstopanja od te zahteve.

Bitna hitrost usklajenega ključa (secret key rate) je teoretično omejena z medsebojno informacijo I(X;Y), pri čemer merimo hitrost relativno na uporabo kvantnega kanala oziroma na koincidenčni dogodek. Približek V predstavlja neusklajeni ali surovi ključ. Naloga naslednjega višjega protokolnega sloja je uskladitev bitov surovega ključa med entitetama. Teoretični meji bitne hitrosti usklajenega ključa se približamo z optimalno shemo za korekcijo napak, ki upošteva znano verjetnostno porazdelitev šuma, pri čemer so potrebne natančne meritve tako azimutnega kota kakor tudi samega odklona od smeri izvornega fotona po sipanju. Tu je potrebno poudariti, da so protokoli za uskladitev ključa iz znanih optičnih shem kvantne distribucije, kot je npr. kaskadni protokol, v našem primeru neuporabni, saj je šum bistveno večji in presega meje uporabnosti omenjenih protokolov.

Uporabo znanih shem za korekcijo napak iz teorije komunikacij omogoči binarni kodirnik, kot je predstavljen v nadaljevanju. Kodirnik ne zahteva natančne meritve odklonskega kota. Surovi binarni

ključ K zakodiramo v V s preslikavo, ki bitu 0 priredi vrednost 0, bitu 1 pa pi/2. Dekodirnik na drugi strani vrednost V+E preslika v 0, če se nahaja v intervalu [-pi/4,pi/4), sicer pa v 1. Na ta način lahko surovi binarni ključ vsebuje poljubne kode za korekcijo napak, pri čemer ostaja izmenjava X+V na javnem kanalu popolnoma varna pri zgoraj navedenih pogojih uniformne distribucije X. Teoretična meja bitne hitrosti usklajenega ključa je v primeru binarnega kodiranja omejena z 1 - h(e), pri čemer h označuje binarno entropijo in e delež napačnih bitov surovega ključa.

V primeru binarnega kodirnika je za maksimizacijo bitne hitrosti usklajenega ključa potrebno filtrirati koincidenčne dogodke z neugodnimi odkloni sipanja od smeri izvornega fotona. Pri 1-stopinjski natančnosti je optimalni interval upoštevanih sipanj [40°,129°]. Prav tako je potrebno izločiti koincidence z neugodnimi azimutnimi koti, pri katerih razlika v azimutnem kotu ni v intervalu [-67°/2,67°/2] ali [90-67°/2,90+67°/2]. Za tak sistem je teoretični delež napačnih bitov 0,449 in bitna hitrost usklajenega ključa 0,0019.

Detekcija napada na kvantni kanal izkorišča dejstvo, da tudi za napadalca veljajo enaki fizikalni zakoni. V primeru prestrezanja fotonov in poskusa njihove replikacije napadalec inherentno poveča šum na kanalu. Ob predpostavki, da napadalec lahko izmeri polarizacijo fotona s teoretično dovoljeno natančnostjo in reproducira izmerjeno polarizacijo, se bo delež napačnih bitov z 0,449 dvignil vsaj na 0,479. Za detekcijo napadalca je dovolj naključni izbor določenega števila bitov surovega ključa v povezavi s standardnim postopkom statističnega testiranja hipotez, pri čemer velja, da število napak sledi binomski porazdelitvi.

Izum ponazarjata dva izvedbena primera - dve konstrukcijski rešitvi fizičnega nivoja naprave za kvantno distribucijo ključa, shematično prikazani na slikah 1 in 2.

Prvi izvedbeni primer zahteva uporabo prostorsko občutljivih detektorjev fotonov v energijskem razponu za izum relevantnih energij, torej vsaj med 100 keV in 1 MeV. Shema naprave je prikazana na sliki 1. Postavitev dveh detektorjev 2 enega ob drugega z virom prepletenih fotonov 1 v sredini omogoča detekcijo večine relevantnih interakcij fotonov gama. Od velikosti detektorjev 2 je odvisno, kolikšen delež fotonov bo prestrežen. Posamezni detektor 2 služi kot Comptonov sipalec in detektor obenem. Zaznati je potrebno vsaj točko prvega sipanja in točko prve naslednje interakcije sipanega fotona. Priporočljivo je izmeriti tudi odložene energije interakcij, kar omogoči filtriranje relevantnih dogodkov in izboljšanje končne bitne hitrosti izmenjanega ključa. Dejstvo, da naprava lahko prestreže večji del prepletenih fotonov in da so koti sipanja znani z načeloma poljubno natančnostjo detektorja

2, omogoča izvedbo skoraj optimalnih kod za uskladitev ključa med obema entitetama, to je kodiranja, ki temelji na znani verjetnostni porazdelitvi kotov Comptonovega sipanja.

Drugi izvedbeni primer naprave za kvantno distribucijo ključa zahteva binarni kodirnik, kot je bil opisan zgoraj. Naprava se poenostavi na račun višjega deleža napačnih bitov (0,460) in posledično nižje bitne hitrosti usklajenega ključa (0,0009). Shema naprave je prikazana na sliki 2. Tudi tu se izvor prepletenih fotonov 1 nahaja med napravama obeh entitet. Posamezna naprava se sestoji iz ščita 3, sipalca 4 in štirih monolitnih detektorjev 5. Monolitnih detektorjev 5 je lahko tudi manj, prisotna morata biti vsaj dva, ki s sipalcem 4 oklepata pravi kot. Ščit 3 je iz svinca ali kakega drugega materiala, ki učinkovito absorbira fotone gama, in vsebuje stožčast kanal, ki neovirano prepušča fotone v smeri sipalca 4. Sipalec 4 ima obliko prirezanega stožca in siplje prepletene fotone, ki priletijo skozi kanal v ščitu. Oblika in velikost monolitnih detektorjev 5, ki so v senci ščita 4 glede na izvor prepletenih fotonov 1, je prilagojena optimalnim kotom za točkovni primer sipanja.

4. Patentni zahtevki

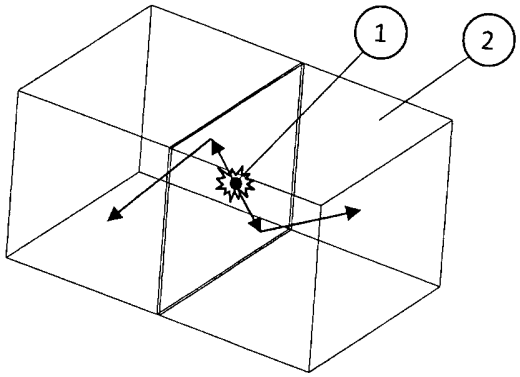
1. Metoda kvantne distribucije ključa na kratke razdalje, označena s tem, da sloni na uporabi prepletenih kvantnih stanj fotonov nastalih ob izničenju elektrona in pozitrona in kot princip delovanja izkorišča kvantno nedoločenost Comptonovega sipanja fotonov na elektronu, pri čemer delna koreliranost azimutnih kotov sipanja predstavlja osnovo za vzpostavitev šumnega kvantnega kanala z znano mejo šuma.

2. Metoda po zahtevku 1, označena s tem, da protokol za uskladitev ključa omogoča aplikacijo shem za korekcijo napak iz teorije komunikacij in temelji na kodiranem prenosu kod za korekcijo napak naključno generirane vrednosti ključa, pri čemer se za kodiranje/dekodiranje uporabi izmerjeni azimutni kot, za uporabo optimalnih shem korekcije napak pa dovoljuje izmenjavo odklonskega kota sipanja.

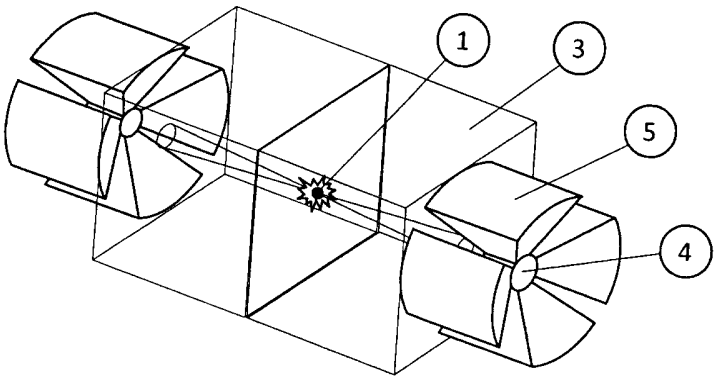
3. Metoda po zahtevkih 1 in 2, označena s tem, da filtriranje koincidenčnih dogodkov z neugodnimi odkloni kotov sipanja in z neugodnimi azimutnimi koti maksimizira bitno hitrost usklajenega ključa pri dani aktivnosti izvora fotonov (1) v primeru binarnega kodirnika.

4. Naprava za kvantno distribucijo ključa kratkega dosega za izvajanje metod po zahtevkih 1-3, označena s tem, da uporablja prostorsko občutljivi detektor (2) fotonov.

5. Naprava za kvantno distribucijo ključa kratkega dosega za izvajanje metod po zahtevkih 1-3, označena s tem, da uporablja ščit (3), sipalec (4) in vsaj dva monolitna detektorja (5).



Slika 1



Slika 2