Elektrotehniški vestnik 75(5): 257-263, 2008
Electrotechnical Review: Ljubljana, Slovenija

Predstavitev ideje kvantnega šifriranja in pregled osnovnih tehnik kvantnega razdeljevanja ključa

Jurij Tratnik, Boštjan Batagelj

Univerza v Ljubljani, Fakulteta za elektrotehniko, Tržaška 25, 1000 Ljubljana, Slovenija
E-pošta: jure.tratnik@fe.uni-lj.si, bostjan.batagelj@fe.uni-lj.si

Povzetek. Varnostna zagotovila v telekomunikacijah so danes odvisna predvsem od uporabljenega šifrirnega algoritma in dolžine ključa, eden glavnih problemov varnosti pa je še vedno razdeljevanje ključa. Kvantno šifriranje ali kvantna kriptografija prvič vpelje pojem absolutne varnosti, ki temelji na fizikalnih lastnostih svetlobe oziroma njenih najmanjših delcev – fotonov. Nedeljivost fotona, načelo nedoločenosti in polarizacijska stanja svetlobe lahko uporabimo v protokolih za kvantno razdeljevanje ključa. V članku je predstavljena ideja in koncepti kvantnega šifriranja, ki nas privedejo do dveh osnovnih protokolov za kvantno razdeljevanje ključa (BB84 in B92), ter do izpeljank obeh algoritmov, ki namesto polarizacije koristijo spreminjanje faze svetlobe, kar se v interferometerskih oblikah komunikacije že uporablja v komercialnih napravah.

Ključne besede: kvantno šifriranje, kvantno razdeljevanje ključa, polarizacija fotonov, BB84, B92

The Main Idea of Quantum Cryptography and Overview of Quantum Key Distribution Techniques

Extended abstract. In this paper basic ideas of quantum cryptography (QC) are presented. The QC basis are no longer based on mathematical algorithms but on physical features of light or its quanta called photons. The indivisible entity of the photon energy, described by A. Einstein (1), the uncertainty principle and polarization states of light can be used in protocols for quantum key distribution (QKD) [2].

The first protocol for QKD was the BB84 protocol. It was named after C. Bennett in G. Brassard. It works on the photon polarization principle with photons present in four different polarization states (linear vertical, linear horizontal, circular left and circular right) and measured with two techniques (linear and circular method), shown in Figures 2 and 3 [3]. The BB84 protocol is a two-point protocol where Alice (Tx) sends a random set of photons to Bob (Rx). Bob receives and defines them by using two measurement techniques. The raw key is created after changing the producing- and measurement-method data between Alice and Bob over a public channel [4]. The BB84 system components are shown in Figure 4 and the QKD method in Table 2.

The B92 protocol is similar to BB84 protocol. It uses only two photon polarization states [5]. The system components and QKD method are shown in Figure 5 and in Table 3. The important difference between them is also a possible use of phase coding instead of polarization for being easier to implement.

There have been many quantum protocol implementations developed and used in more or less useful QKD variations [6]. In each of the three fundamental ones, an optical interferometer is used. The first, which is of the interferometric-communication type, employ a single Mach-Zehnder interferometer (MZI) and two transport optical fibers (Fig. 6), whereas the second IC type uses two MZIs (Fig. 7). Besides the interferometer, the latter one relies also on the principle of Faraday orthoconjugation and is the most common type used in commercial Plug&Play devices for QKD (Fig. 8).

QC does not seem to have become a common key distribution method yet. So far it is used only as an additional service to classical security algorithms. QC is on the other hand only a by-product of the quantum-computer research.

Keywords: Quantum cryptography, quantum key distribution (QKD), photon polarization, BB84, B92

Prejet 29. februar, 2008
Odobren 16. junij, 2008

1 Uvod

V sedanjem času informacijske družbe, ko skorajda nenehno komuniciramo in prenašamo najrazličnejša sporočila po telekomunikacijskih omrežjih, se nam čedalje pogosteje zastavlja vprašanje varnosti naših podatkov. Nemalokrat so informacije, ki jih oddajamo ali sprejemamo po različnih omrežjih, zaupne narave in nikakor nočemo, da bi jih izvedel kdorkoli drug kot naš oddaljeni sogovornik. Še zlasti smo pozorni pri izvajanju bančnih storitev, internetnega nakupovanja in drugih aplikacijah, ki so vezane na našo identiteto.

Omrežje je pred neavtoriziranimi uporabniki, ki bi želeli imeti dostop do njega, zaščiteno s požarnim zidom, ki izloča sumljiv promet oziroma preprečuje dostop določeni vrsti prometa. Ker kljub uporabi požarnega zidu še vedno obstaja možnost, da malopridnež prestreza podatke, medtem ko potujejo

med pošiljateljem in prejemnikom, ter jih bere ali celo spreminja (kali njihovo verodostojnost), se uporablja šifriranje podatkov. Veda, ki proučuje šifriranje in se imenuje kriptografija, nas uči, da dobro varovanje sporočila ne temelji na tajnosti šifrirnega postopka, temveč na tajnosti šifrirnega ključa, pri čemer je sprejemljiv samo tisti postopek, ki je za poznavalca ključa izvedljiv v realnem času [1]. Nepoznavalec šifrirnega ključa kljub zelo zmogljivemu računalniku ne more izvesti postopka dešifriranja v doglednem času.

Tako rekoč nezlomljivim zaščitnim tehnikam elektronskega šifriranja, ki varujejo naše podatke na višjem nivoju omrežja, zdaj prihaja v dopolnitev kvantno šifriranje, ki omogoča tudi teoretsko nezlomljivo varovanje podatkov na samem fizičnem nivoju telekomunikacijskih povezav s pomočjo optičnega vlakna. Medtem ko klasično šifriranje uporablja različne matematične metode za zaščito sporočila pred prisluškovanjem, kvantno šifriranje temelji na uporabi zakonov kvantne fizike za doseganje absolutne varnosti prenosa podatkov.

2 Svetloba kot šifrirni medij

Svetloba je elektromagnetno valovanje, dejansko pa jo lahko obravnavamo kot delček (korpuskularno) ali kot val [2]. Najmanjši gradnik ali kvant svetlobe imenujemo foton. Foton je nedeljiv energijski del, ki se širi s hitrostjo svetlobe v mediju, ima nično mirovno maso ter lastno gibalno in vrtilno količino, kar vse mu daje izrazito korpuskularen značaj

Elektromagnetno polje fotona lahko zapišemo na več načinov glede na to, da je valovanje po svoji obliki zelo različno. Polje razvrščamo v rodove, ki so linearno neodvisne rešitve valovodne enačbe. Polje ima smer (polarizacijo), amplitudo, frekvenco in fazo ter določeno rodovno prostorsko porazdelitev.

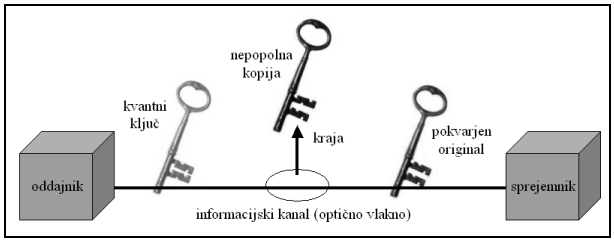
O kvantiziranosti svetlobne energije govori znana enačba (1), ki jo je leta 1905 s poskusom fotoefekta razložil Einstein. Energija elektromagnetnega polja je enaka skupni energiji fotonov

$$W_n = n \cdot h \cdot \nu, \qquad (1)$$

kjer je n število fotonov, h = 6,6262·10^{-34} Js Planckova konstanta in ν frekvenca. Enačba pravi, da s povečevanjem moči svetlobe dane frekvence narašča število kvantov energije v časovni enoti, če pa povečujemo frekvenco svetlobe, se povečuje energija posameznega kvanta. Kvant energije svetlobe je potemtakem nedeljiv.

Energijska stanja svetlobe so kvantizirana tako, da izmenjava energije poteka v kvantih (odmerkih) po enačbi (1). Hkrati v kvantni teoriji poznamo začetno (ang. zero point) vrednost energije, ki znaša $W_0 = h \cdot \nu/2$ na osnovnem nivoju. To je vakuumsko stanje svetlobe v praznem prostoru brez fotonov. Začetnemu stanju pravimo tudi kvantni šum.

Omenjene lastnosti svetlobe lahko uporabimo za kvantno komunikacijo oz. kvantno razdeljevanje ključa, pri tem pa ima najpomembnejšo vlogo prav nedeljivost fotona, katerega lastnost je, da je zelo občutljiv na vsak zunanji poseg, zato ga vsak poskus prisluškovanja poruši, pokvari informacijo in izda prisluškovalca. Ker je ključ, kodiran s kvantnim stanjem posameznega fotona, nemogoče identično replicirati, lahko prejemnik z lahkoto ugotovi, ali je bil skriti ključ ukraden (slika 1). Ta način obema stranema – pošiljatelju in prejemniku – omogoča izmenjavo kode po javnem komunikacijskem kanalu s popolno varnostjo prenosa.



Slika 1: Kraja kvantnega ključa je fizikalno nemogoča.

Figure 1: Stealing a quantum key is physically impossible.

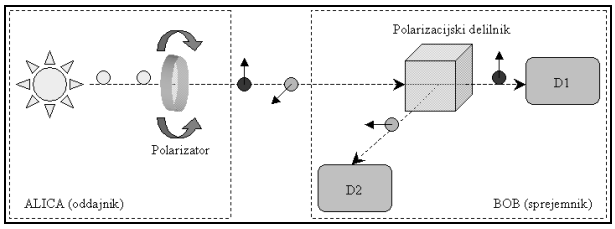
V nasprotju z obstoječimi klasičnimi shemami za razdeljevanje ključa, razdeljevanje kvantnega ključa ne potrebuje varnega prenosa, temveč lahko poteka po javnem in popolnoma nevarovanem optičnem omrežju, (ki je na primer lahko transportno optično omrežje z razvrščanjem valovnih dolžin ali dostopovno pasivno optično omrežje). Kvantni ključ je ustvarjen neposredno in sočasno pri pošiljatelju in prejemniku. Poleg tega je ustvarjen iz popolnoma naključnih zaporedij, kar je izjemno zahtevno izvedljiva naloga za klasično shemo razdeljevanja ključa.

3 Uporaba polarizacije v kvantnih komunikacijah

Sistem za kvantno komunikacijo je lahko izveden s pomočjo spreminjanja (moduliranja) polarizacije fotona, poznan pa je tudi sistem kvantne komunikacije na podlagi kvantne prepletenosti (ang. Entanglement). Glede na polarizacijsko stanje fotona ločimo linearno ali krožno polarizirano komunikacijsko metodo [3].

Na sliki 2 je prikazana osnovna struktura optičnih elementov za linearno zaznavo fotona. Linearni komunikacijski sprejemni sistem nam enoumno ločuje vertikalno in horizontalno polarizirane fotone, ki jih zaznavamo na dveh detektorjih fotonov (D1 in D2). Sestavljajo ga izvor posameznih fotonov, polarizator svetlobe, polarizacijski delilnik in detektorja fotonov. Polarizator je zmožen prepustiti svetlobo poljubno izbrane linearne polarizacije. Glavna naloga polarizacijskega delilnika je, da prepušča 100 odstotkov

svetlobnega signala, ki je vertikalno polariziran (↕), in odbije 100 odstotkov svetlobnega signala, ki je horizontalno polariziran (↔).

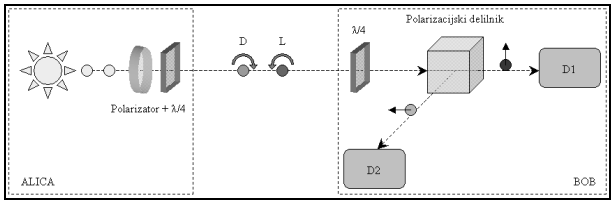


Slika 2: Linearna metoda zaznave fotona.

Figure 2: Linear photon-detection method.

Oddan foton je lahko tudi krožno polariziran. Kot vemo, je krožna polarizacija sestavljena iz dveh linearnih ortogonalnih polarizacij s fazno razliko $\pm \pi/2$ (vertikalne in horizontalne). Če krožno polariziran foton vpade na polarizacijski delilnik, z enako verjetnostjo izmerimo vertikalno oziroma horizontalno polarizacijo, ker ima krožno polariziran foton obe polarizaciji zastopani z enako, 50 odstotno verjetnostjo.

Predpostavimo, da imamo krožno polariziran foton, ne vemo pa, ali je polarizacija levo oz. desno sučna. Komunikacijski sistem na sliki 3 ločuje desno in levo krožno polarizirane fotone.



Slika 3: Krožna metoda zaznave fotona.

Figure 3: Circular photon-detection method.

Krožni komunikacijski sistem se od linearnega razlikuje po dodani oddajni in sprejemni ploščici $\lambda/4$ pred polarizacijskim delilnikom. Ploščica $\lambda/4$ je izdelana iz dvolomne snovi, v kateri se širita pravokotna linearno polarizirana valova svetlobe z različnima hitrostma. Rezultat tega je, da se njuna medsebojna fazna razlika poveča ali zmanjša. Pridobljena fazna razlika po preletu ploščice $\lambda/4$ je enaka $\pi/2$. Celotna fazna razlika v sprejemniku je 0 ali π, odvisno od tega, ali je na vhodu sprejemne ploščice $\lambda/4$ levo ali desno sučna krožna polarizacija, le-to pa je odvisno od položaja oddajne ploščice. Krožno polarizirani fotoni se ob prehodu skozi ploščico $\lambda/4$ transformirajo v linearno polarizirane in nasprotno. Na izhodu so točno vertikalno ali horizontalno polarizirani fotoni, odvisno od krožne polarizacije na vhodu. Lahko povzamemo, da sistem, prikazan na sliki 3, ločuje krožno polarizirane fotone glede na smer sukanja polarizacije na vhodu.

Povzetek rezultatov opisanih komunikacijskih metod za različna polarizacijska stanja prikazuje tabela 1. Rezultati so podani z verjetnostmi zaznave fotona na posameznem detektorju glede na polarizacijo fotona in uporabljeno komunikacijsko metodo.

Polarizacija fotona	↕	↔	D	L
Linearna metoda +	100 / 0	0 / 100	50 / 50	50 / 50
Krožna metoda O	50 / 50	50 / 50	100 / 0	0 / 100

Tabela 1: (↕= linearna vertikalna polarizacija, ↔ = linearna horizontalna polarizacija, D = desna krožna polarizacija, L = leva krožna polarizacija. P(D1) / P(D2) pove, kakšna je verjetnost zaznave fotona na detektorjih D1 in D2)

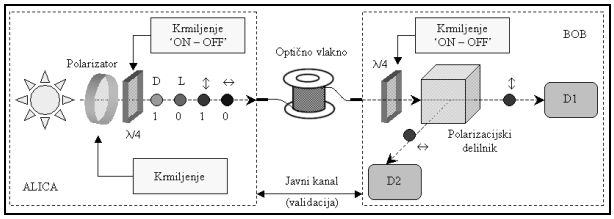
Table 1: (↕= linear vertical polarization, ↔ = linear horizontal polarization, D = right circular polarization, L = left circular polarization. P(D1) / P(D2) tells the probability of photon detection on detectors D1 and D2).

Prikazane štiri polarizacije fotona in dve komunikacijski metodi lahko uporabimo za kvantno šifriranje. Navadno se kvantno šifriranje ne uporablja za šifriranje sporočil, kot morda zavaja ime. Pošiljanje šifrirnih sporočil je lahko izvedeno prek javnega medmrežja. Sam prenos je varen, kolikor je pač varen uporabljen algoritem. Prvotni in osnovni namen kvantnega komunikacijskega kanala je razdeljevanje ključev. Za kakšen tip ključa gre (enkratni, sejni, javni, zasebni), ni pomembno, pomembno je, da se za absolutno varno pošiljanje ali izmenjavo uporabijo kvantne lastnosti polariziranih fotonov.

4 Kvantno razdeljevanje ključa po protokolu BB84

Protokol BB84 (C. Bennett in G. Brassard) je bil predstavljen že leta 1984, šele v zadnjem času pa je ponovno aktualen, saj je osnova vsem nadaljnjim različicam, ki jih je z današnjo tehnologijo mogoče realizirati [4].

Alica in Bob (tako se ponavadi poimenujeta oddajnik in sprejemnik) uporabljata izvor posameznih fotonov, krmilnik polarizacije (krmiljen polarizator ali ploščica $\lambda/4$), ki je zmožen za vsak foton posebej določiti eno od štirih polarizacij (↕,↔, D, L) in elektroniko, ki po potrebi 'vstavlja' ploščico $\lambda/4$ na sprejemu (slika 4).



Slika 4: Kvantno razdeljevanje ključa po protokolu BB84.

Figure 4: BB84 quantum key-distribution protocol.

Protokol BB84 za izmenjavo ključa je naslednji; Alica mora najprej poslati Bobu paket fotonov, npr. po 16 bitov (1 foton pomeni 1 bit, včasih poimenovan tudi kvantni bit - qubit), ki bodo naključno polarizirani glede na izbrane pogoje v oddajniku, na primer:

↕↔ D L ↔↔ D ↕ ↕L D ↔ L L D↕.

Bob nato nastavi svojo sprejemno napravo po naključnem zaporedju:

+ O + O O + + + O + O O O + + O.

Prikazana sprejemna nastavitev pomeni, da bo prvi foton (bit) merjen po linearni metodi (+), drugi prispeli foton po krožni metodi (O) in tako naprej, obe komunikacijski metodi pa sta zastopani z enako verjetnostjo. Postopek in rezultati so zbrani v tabeli 2.

Časovna okna	1 2 3 4	5 6 7 8	9 10 11 12	13 14 15 16
Aličina naključna izbira bitov	**1 0 1 0**	**0 0 1 1**	**1 0 1 0**	**0 0 1 1**
Aličina pripadajoča polarizacijska stanja	↕ ↔ D L	↔ ↔ D ↕	↕ L D ↔	L L D↕
Aličina oddajna nastavitev	+ + O O	+ + O +	+ O O +	O O O +
Bobova naključna merilna nastavitev	+ O + O	O + + +	O + O O	O + + O
Interni rezultat Bobovih meritev	↕ L ↕L	L↔ ↔↕	D↔D D	L ↕ ↔ D
Potrditev veljavnosti bitov	**1** x x **0**	x **0** x **1**	x x **1** x	**0** x x x

Tabela 2: Postopek BB84 za razdeljevanja ključa

Table 2: BB84 key-distribution procedure.

Vidimo, da je Bob ob vsakem merjenju izmeril le en foton. Če je nastavljena sprejemna metoda linearna (+), odčitek na detektorju D1, pomeni rezultat (↕) oziroma vertikalno polariziran foton in odčitek na detektorju D2 rezultat (↔) ali horizontalno polariziran foton. Podobno je pri krožni nastavitvi (O), kjer odčitek na D1 pomeni desno krožno polarizacijo fotona (D), in odčitek na D2 levo krožno polarizacijo (L). Bobovi rezultati so tako:

↕ L ↕L L↔↔↕ D↔D D L ↕↔ D.

Postopek seveda še ni končan. Bob nato pokliče Alico in ji pove, kakšno sprejemno sekvenco je uporabil (+O+OO+++O+OOO++O). Vsakokrat, ko je Bob uporabil enako sprejemno nastavitev, kot je bila Aličina oddajna, Alica sporoči Bobu, da je bit oziroma časovno okno veljavno.

Alica seveda ne ve ničesar o Bobovih rezultatih merjenja polarizacije, samo posreduje mu, ob katerih časovnih trenutkih je uporabila enako polarizacijsko metodo kot on. Malopridna Eva (oznaka za prisluškovalca), ki vedno spremlja promet na vseh javnih odprtih kanalih, si z njunim pogovorom ne more prav nič pomagati. Iz zajetih sporočil ne more izvedeti, kakšno polarizacijo je uporabila Alica, niti kakšno polarizacijo je izmeril Bob (v vsakem časovnem oknu).

Ko Bob zavrže napačne meritve, mu ostane naslednji niz:

↕ - - L - ↔ - ↕ - - D - L - - -,

kar pomeni, da so njegove izmerjene vrednosti veljavne v šestih primerih (1, 4, 6, 8, 11, 13). Še zadnja stvar, ki je potrebna, da stvar v celoti deluje, je dogovor o pripadajoči vrednosti bita (1 ali 0) za posamezno od štirih polarizacij. V tem primeru logično '1' predstavljata polarizaciji ↕ in D, logično '0' pa ↔ in L. V tem trenutku lahko Bob interpretira svoj niz pravilnih meritev kot:

1 - - 0 - 0 - 1 - - 1 - 0 - - - = 100110,

kar predstavlja začetno osnovo ključa (ang. raw key).

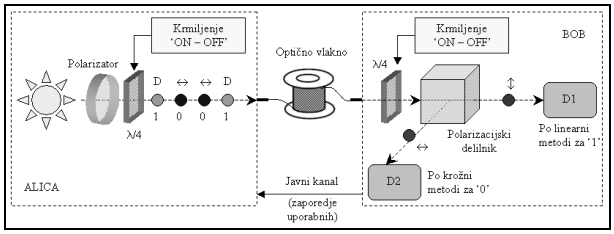
Celotna operacija se lahko ponavlja poljubno dolgo z namenom, da se poveča dolžina ključa. Zelo dolg ključ je lahko generiran tudi v enem koraku, na primer 3000-bitno sporočilo za 1024-bitni ključ. Pri tem je vredno omeniti še, da na začetku ne sprejemna ne oddajna stran ne vesta, kakšna bo končna vrednost ključa, saj nastane šele po validaciji časovnih oken.

Zaradi uporabe enofotonskih signalov je pri prisluškovanju nemogoče odkriti ključ. Če je prisluškovalec na kvantnem kanalu pasiven, s svojim merjenjem 'porablja' fotone, kar Bob zazna kot prazna časovna okna, pri aktivnem prisluškovanju pa Eva zaznava in ponareja fotone, kar se izraža v nizkem izkoristku protokola (25 odstotkov namesto 50 odstotkov). Tako se odkrije prisluškovalec, dobljeni rezultati pa se zavržejo. S tem Eva ne pridobi ključa, otežkoči ali onemogoči pa njegov prenos.

5 Kvantno razdeljevanje ključa po protokolu B92

Protokol B92 za kvantno razdeljevanje ključa je bil predstavljen leta 1992 (Charles H. Bennett). V nasprotju z njegovim predhodnikom, BB84, pri implementaciji potrebujemo le dve, toda vnaprej določeni polarizacijski stanji na oddajni in sprejemni strani. Razdeljevanje ključa na podlagi protokola B92 je danes najbolj razširjeno, saj je protokol mogoče prirediti za kodiranje bitov s fazo svetlobnega signala, kar je veliko lažje realizirati kot kodiranje s polarizacijo.

Razdeljevanje ključa poteka takole (slika 5) [5]. Alica in Bob se že vnaprej dogovorita, kakšna dva tipa polariziranih fotonov bosta oddajala. Na primer, Alica uporablja oz. pošilja horizontalno (↔) in desno krožne (D) polarizirane fotone, ki pomenijo logične '0' in '1'. Na sprejemni strani Bob detektira bodisi levo krožne (L) ali vertikalno (↕) polarizirane fotone, ki ustrezajo njegovim ničlam in enicam.



Slika 5: Kvantno razdeljevanje ključa po protokolu B92.

Figure 5: B92 quantum key-distribution protocol.

Komponente, ki teoretično omogočajo izvedbo protokola B92, so identične komponentam pri protokolu BB84. Razlika je le v tem, da Alica pošilja le fotone v dveh mogočih polarizacijskih stanjih, Bob pa jih sprejema bodisi po linearni bodisi po krožni komunikacijski metodi in pri tem želi, da foton zazna na pravem detektorju. Potek komunikacije je razvidnejši iz tabele 3.

Časovna okna	1	2	3	4	5	6	7	8	9	10	11	12
Aličina naključna izbira bitov	**1**	**1**	**0**	**0**	**1**	**0**	**1**	**0**	**0**	**0**	**1**	**1**
Aličina polar. stanja	D	D	↔	↔	D	↔	D	↔	↔	↔	D	D
Bobova merilna metoda	L (O)	↕ (+)	L (O)	↕ (+)	L (O)	L (O)	L (O)	↕ (+)	L (O)	L (O)	↕ (+)	L (O)
Bobovi pripadajoči biti	**0**	**1**	**0**	**1**	**0**	**0**	**0**	**1**	**0**	**0**	**1**	**0**
Bobov rezultat	NE	DA	NE	NE	NE	DA	NE	NE	DA	NE	NE	NE
Ključ	-	**1**	-	-	-	**0**	-	-	**0**	-	-	-

Tabela 3: Postopek B92 za razdeljevanje ključa

Table 3: B92 key-distribution procedure.

Pri sprejemanju fotonov se Bob drži dveh preprostih pravil, ki mu omogočata takojšnjo validacijo bitov. In sicer, če meri po krožni metodi (O), želi detektirati foton na detektorju D2 za logično '0', če pa meri po linearni metodi (+), želi detektirati foton na detektorju D1 za logično '1'. Vse druge kombinacije so zanj neveljavne.

Poglejmo si potek za prvih nekaj časovnih oken. V prvem časovnem oknu Alica pošlje desno krožno polariziran foton, torej logično '1'. Bob se odloči, da bo v tem časovnem oknu meril po krožni metodi. Ker iz D fotona pri njegovi meritvi nastane ↕ polariziran foton, ga zazna na detektorju D1, želel pa ga je na D2, torej je bit neveljaven. V drugem časovnem oknu Alica prav tako pošlje logično '1'. Bob se odloči, da bo v tem časovnem oknu meril po linearni metodi. Ker krožno polariziran foton vpade direktno na polarizacijski delilnik, je 50-odstotna verjetnost, da bo nadaljeval pot proti detektorju D1. Ker se to zgodi je za Boba prispela enica veljavna. Podoben primer je v tretjem časovnem oknu, kjer linarno polariziran foton meri po krožni metodi. Tudi tukaj je 50% možnosti, da ga zazna na želenem detektorju. Ker se to ne zgodi, je bit neveljaven.

Po končanem prenosu po kvantnem kanalu, Bob sporoči Alici, katera časovna okna so veljavna. V prikazanem primeru so veljavna okna 2, 6 in 9. Začetek ključa bi v tem primeru bil:

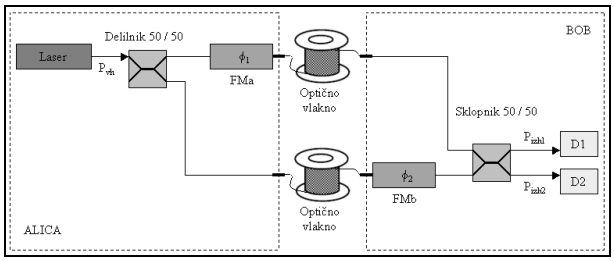
- 1 - - - 0 - - 0 - - - = 1 0 0.

Iz celotne tabele 3 je razvidno, da so od 12 bitov veljavni le trije. Izkoristek izmenjave ključa po protokolu B92 je v idealnem primeru (kot v tabeli) le 25-odstoten, med tem ko je pri protokolu BB84 50-odstoten.

6 Uporaba faze svetlobe v kvantnih komunikacijah

Kvantno razdeljevanje ključa po protokolu B92 je izvedljivo tudi s pomočjo optičnih interferometrov. Tak primer sta npr. Michelsonov ali Mach-Zehnderjev interferometer, pri čemer je slednjega z optičnimi vlakni laže realizirati. Svetlobi v tem primeru ne določamo polarizacije, temveč spreminjamo fazo. Tak način je veliko laže izvedljiv v praksi, saj je laže kontrolirati fazo kot pa polarizacijo svetlobe. Pomembno je poudariti, da zdaj ne govorimo več o operacijah nad enim fotonom, temveč nad nizom, recimo svetlobnim impulzom.

Na sliki 6 je prikazana interferometrska komunikacija, za katero potrebujemo laserski izvor svetlobe, dva optična sklopnika, dva fazna modulatorja in dva detektorja (sprejemnika) [6]. Mach-Zehnderjev interferometer je razpotegnjen in skrit v strukturi med oddajno in sprejemno stranjo.



Slika 6: Interferometrska komunikacija z Mach-Zehnder-jevim interferometrom.

Figure 6: Interferometric communication with the Mach-Zehnder interferometer.

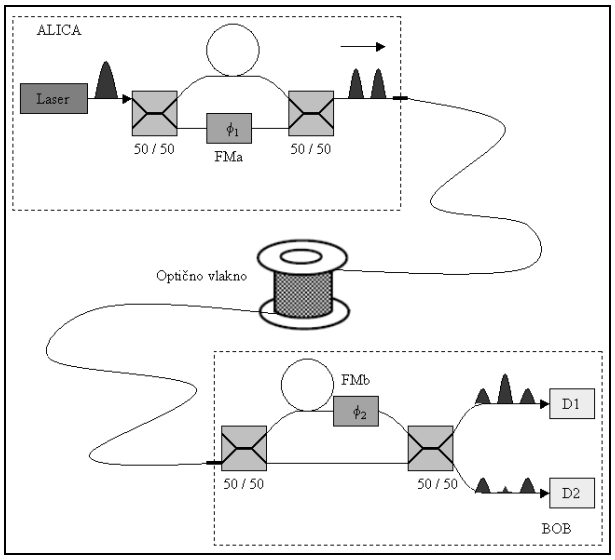
Izraz (2) je interferometrska enačba, ki nam povezuje izhodno moč na sprejemnem sklopniku v odvisnosti od spremembe faze v obeh vejah.

$$P_{izh1} = P_{vh} \cos^2\left(\frac{\Delta\phi}{2}\right) \qquad (2)$$

Alica kodira svoj podatkovni (naključni niz) s spremembo faze na svojem modulatorju FMa, in sicer z

$\Delta\phi_1 = 0$ za logično '0' in z $\Delta\phi_1 = \pi/2$ za logično '1'. Na sprejemni strani Bob v sinhroniziranih časovnih trenutkih spreminja fazo na svojem faznem modulatorju FMb z $\Delta\phi_2 = 3\pi/2$ za potrditev logične '0' in z $\Delta\phi_2 = \pi$ za potrditev logične '1'. Na podlagi treh mogočih močnostnih izhodnih nivojev (0, 0,5 in 1) se Bob odloča, katere sprejete bite bo potrdil.

Na sliki 7 je prikazana interferometrska komunikacija, ki se od prejšnjega tipa razlikuje po številu uporabljenih interferometrov in enem samem glavnem optičnem vlaknu za prenos.

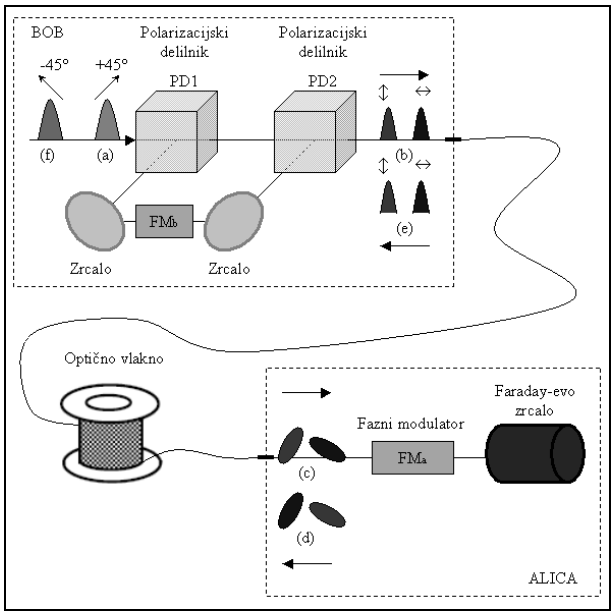


Slika 7: Interferometrska komunikacija z enim samim transportnim optičnim vlaknom.

Figure 7: Interferometric communication with only one transport optical fiber.

V tem primeru Alica pošlje močan laserski impulz, ki se na prvem delilniku 50/50 deli v dve veji interferometra, krajšo K in daljšo D. Impulzu, ki potuje po krajši veji, spreminja fazo s faznim modulatorjem FMa. Na izhodu prvega interferometra tako nastaneta dva impulza K (nosi informacijo o ključu) in D, ki potujeta po glavnem vlaknu do Boba. Bob poseduje enak interferometer kot Alica, le da s faznim modulatorjem FMb spreminja fazo v daljši veji. Na izhodu iz Bobovega interferometra zdaj nastanejo trije impulzi; prvi impulz KK in zadnji impulz DD ne nosita informacije, srednji pa je rezultat interference med potmi impulzov KD in DK. Relativna fazna razlika se izraža kot konstruktivna in destruktivna interferenca na detektorjih D1 in D2.

Kvantno razdeljevanje ključa je danes v praksi najpogosteje izvedeno z zasnovo, prikazano na sliki 8 [7]. Osnovna zamisel je v uporabi Faradayevega zrcala. Namreč, če na tako zrcalo vpade svetloba iz vlakna, ki se odbije in potuje nazaj po isti poti, se na izhodu iz vlakna pojavi ortogonalna na vhodno stanje. Na primer, vertikalno polarizirana svetloba na vhodu v vlakno se bo vrnila kot horizontalno polarizirana. Pojavu, ki nekoliko spominja na zrcaljenje iz elektromagnetike, pravimo tudi Faradayeva ortokonjugacija. Na splošno do Faradayevega zrcala pripotuje eliptično polarizirana svetloba in se kot taka odbije, na izhodu pa nastane ortogonalno polarizirana. Pri tem tudi ni pomembno, da optično vlakno ohranja polarizacijo in tudi polarizacijske karakteristike v vlaknu se lahko spreminjajo, če spremembe le niso hitrejše od potovanja svetlobe tja in nazaj.



Slika 8: Interferometrska komunikacija s Faraday-evim zrcalom.

Figure 8: Interferometric communication with a Faraday mirror.

Pri tej komunikaciji Bob pošlje linearno polariziran (+45°) impulz svetlobe na polarizacijski delilnik PD1 (slika 8 (a)). Tam se deli v dva impulza, horizontalno (↔) in vertikalno polariziranega (↕). Polarizacijski delilnik je postavljen tako, da ↕ impulz potuje po daljši poti interferometra, ↔ pa po krajši. Rezultat sta dva, časovno zamaknjena, med seboj ortogonalna impulza (slika 8 (b)), ki ju pošljemo po vlaknu na drugo stran. Na izhodu se pojavita kot dva ortogonalno eliptično polarizirana impulza (slika 8 (c)) in se odbijeta na Faradayevem zrcalu. Ortokonjugirana impulza zdaj ponovno vstopita v vlakno (slika 8 (d)) in se pri Bobu pojavita v čistih, linearno polariziranih stanjih. Prvi impulz, ki je zapustil Boba, je bil ↔ polariziran, vrnil pa se je kot ↕ polariziran in nasprotno (slika 8 (e)). Prvi impulz zdaj potuje po daljši poti (prej po krajši) in se na polarizacijskem delilniku PD1 sreča z drugim, kjer se rekombinirata v en sam impulz (-45°) linearne polarizacije (slika 8 (f)).

Vzemimo, da ima Alica fazni modulator FMa, s katerim lahko spreminja fazo ϕ_A enemu od impulzov.

Ob vrnitvi obeh impulzov nazaj k Bobu bo rekonstruirana polarizacija odvisna od dodane fazne razlike. Na primer, če Alica ne zasuka faze ($\phi_A = 0$), bo rekonstruirano stanje (-45°) linearno polarizirano, kot prej. Če pa izbere $\phi_A = \pi$, bo rekonstruirano stanje impulza (+45°) linearno polarizirano. Če izbere $\phi_A = \pm\pi/2$, pa bo rekonstruirano stanje impulza krožno polarizirano.

Da bi bila stvar uporabna za razdeljevanje ključa, tudi Bob potrebuje svoj fazni modulator FMb v zakasnitveni veji interferometra, s katerim vsili fazni zasuk prvemu impulzu na poti nazaj. Z izbiranjem zasuka $\phi_B = 0$ ali $\phi_B = -\pi/2$ lahko izbira ali bodo rekombinirani impulzi linearno ali krožno polarizirani.

Komunikacija z uporabo šibkih svetlobnih impulzov namesto enofotonskih signalov seveda ni absolutno varna, a se z razvojem enofotonskega izvora in detektorja svetlobe meja varnosti pomika proti absolutni. Kljub temu so današnji 'kvantni' sistemi varnejši od klasičnih.

7 Sklep

Tajnost prenosa šifrirnega ključa je pri kvantnem šifriranju vnaprej zagotovljena z naravnimi zakoni in omogoča varovanje podatkov na fizični ravni.

V kvantnih komunikacijah sta najbolj poznana dva protokola za kvantno razdeljevanje šifrirnega ključa. Pri protokolu BB84 potrebujemo štiri polarizacijska stanja, kar je z današnjo tehnologijo težko uresničiti. Veliko bolj uveljavljen je protokol B92, ki ga je mogoče prilagoditi za kodiranje s fazo svetlobnega signala. S tem ko komunikacijo realiziramo s svetlobnim impulzom namesto s posameznim fotonom, postavimo v negotovost pojem absolutne varnosti, saj vse teorije, ki se opirajo nanjo, pri prenosu zaradi nedeljivosti fotona postanejo neveljavne. Današnje kvantne oz. interferometrske komunikacije, zavedajoč se svoje ranljivosti, potekajo z minimalno močjo signala, kar je poznano tudi v radiokomunikacijah.

Predstavljenih metod, predvsem različice s Faradayevim zrcalom, se danes poslužujejo mnoga podjetja, ki že ponujajo naprave »Plug&Play« na trgu (id Quantique, MagiQ Technologies, SmartQuantum). Aplikacije, ki jih podpirajo naprave, so predvsem varna mostišča med omrežji Ethernet s hitrimi menjavami ključev. Poleg tega ima veliko znanih gigantov, kot so Toshiba, HP, IBM, Mitsubishi, NEC, NTT, THALES, odprte raziskovalne programe kvantnega šifriranja. Generiranje posameznih fotonov in možnost prenosa leteh na dovolj veliko razdaljo sta z vidika optičnih komunikacij dva posebno velika izziva, ki ju prinaša kvantna kriptografija.

Z raziskovalnim projektom SECOQC (2004-2008), v katerega je vključenih 11 evropskih držav (25 univerz, štirje državni raziskovalni inštituti in osem multinacionalk), želijo poleg postavitve kvantnega omrežja na Dunaju standardizirati strojno opremo in protokole, potrebne za kvantno razdeljevanje ključa [8]. Tako bi se na področju kvantnih komunikacij vzpostavila red in združljivost tehnologij, kar bi omogočalo lažje nadgrajevanje obstoječih in na novo postavljenih kvantnih omrežij.

Smernice razvoja za zdaj (še) ne kažejo na množično uporabo kvantnih komunikacij, temveč jih obravnavajo le kot dopolnilo k obstoječim varnostnim sistemom. Poleg tega je kvantno šifriranje le vmesni rezultat, ki na področju kvantne mehanike odpira nova vrata pri razvoju kvantnega računalnika.

8 Literatura

[1] T. Vidmar, *Informacijsko-komunikacijski sistem*, Založba Pasadena, Ljubljana, 2002, str. 551-578.

[2] J. Budin, *Optične komunikacije – z osnovami optike*, Fakulteta za elektrotehniko, Ljubljana, 1998, str. 71-82.

[3] E. Desurvire, *Global telecommunications*, John Wiley & Sons, Inc., New Jersey, 2004, str. 466-468.

[4] C.H. Bennet, G. Brassard, *Quantum cryptography: public key distribution and coin tossing*, Proceedings of IEEE International Conference on Computers, Systems and Signal Processing, Bangalore, Indija, 1984, str. 175-179.

[5] C.H.Bennet, *Quantum cryptography using any two non-orthogonal states*, Physical Review Letters, Vol.68, 1992, str. 3121-3124.

[6] O. L. Guerreau, J. Merolla, A. Soujaeff, F. Patois, *Long-distance QKD transmission using single-sideband detection scheme with WDM synchronization*, IEEE Journal of selected topics in quantum electronics, vol. 9, št. 6, 2003, str. 1533-1540.

[7] A. V. Sergienko, *Quantum Communications and Cryptography*, Taylor & Francis Group, 2006, str. 19-26.

[8] Raziskovalni projekt SECOQC na spletu, http://www.secoqc.net/

Jurij Tratnik je diplomiral leta 2007 na Fakulteti za elektrotehniko Univerze v Ljubljani. Trenutno je mladi raziskovalec na isti fakulteti. Njegovo raziskovalno delo je povezano s fizičnim nivojem radiokomunikacij in optičnih komunikacij.

Boštjan Batagelj je doktoriral leta 2003 na Univerzi v Ljubljani s področja optičnih tehnologij. Od leta 1997 je zaposlen na Fakulteti za elektrotehniko, Katedra za telekomunikacije v Laboratoriju za sevanje in optiko. Kot višji predavatelj in asistent predava ter vodi avditorne in laboratorijske vaje pri nekaterih telekomunikacijskih predmetih. Sodeluje pri domačih in mednarodnih raziskovalnih projektih s področja optičnih in radijskih komunikacij. Njegovo raziskovalno delo je povezano z optičnim dostopovnim omrežjem, optičnim transportnim omrežjem in nelinearnimi optičnimi pojavi.