

Kodiranje s pomočjo sudoku ključa

Klementina Pirc

Fakulteta za matematiko in fiziko
Oddelek za matematiko

26. april 2018

1 Uvod

V današnjem svetu, kjer se vsak dan preko različnih komunikacijskih kanalov preteči nepredstavljiva količina informacij, se pojavi vprašanje varovanja osebnih podatkov. Tema je še posebno aktualna na področju spletnih bančnih storitev in drugih zaupnih dejavnostih. Pomagamo si s šifriranjem podatkov, navadno s pomočjo neke metode ali ključa, ki ga poznata le pošiljatelj in prejemnik in ga uporabita za šifriranje sporočila. Pri šifriranju s ključem naletimo na problem, kako ključ za dešifriranje na varen način in v realnem času sporočiti našemu sogovorniku. Če namreč prisluškovelec prestreže naš ključ in za tem še sporočilo, bo brez težav dešifriral podatke. [2]

Kvantno šifriranje oziroma kvantna kriptografija temelji na posebnih fizikalnih lastnosti delcev. Te lastnosti omogočajo varen prenos šifrirnega ključa tudi preko javnega, nezaščitenega komunikacijskega kanala. Še več, s pomočjo te metode lahko celo ugotovimo, ali je bila med pošiljateljem in prejemnikom prisotna tretja oseba, torej prisluškovelec in po potrebi pripravimo nov ključ za šifriranje. [2]

2 Polarizacija fotonov

2.1 Foton

Definirajmo najprej nekaj osnovnih pojmov s področja fizike delcev in fizike na splošno.

Definicija 1 *Osnovni delec je delec, ki nima podstrukture, torej ni sestavljen iz manjših delcev. [7]*

Definicija 2 *Svetloba je elektromagnetno valovanje pri različnih valovnih dolžinah oziroma frekvencah. [8]*

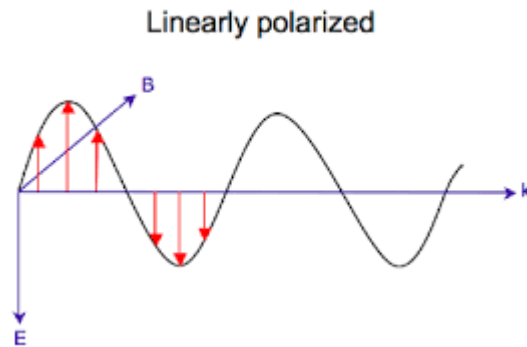
Definicija 3 *Foton je brezmasni in električno nevtralen osnovni delec, ki potuje s svetlobno hitrostjo in je osnovni gradnik svetlobe. [6],[9]*

Torej si lahko širjenje svetlobe oziroma elektromagnetnega valovanja predstavljamo kot gibanje velikega števila fotonov v določeni smeri. Energija fotonov se spreminja obratno sorazmerno glede na valovno dolžino izsevane svetlobe, tako krajša valovna dolžina pomeni več energije. [9]

2.2 Polarizacija svetlobe

Definicija 4 Polarizacija valovanja opisuje smer nihanja količine, ki valuje. [10],[11]

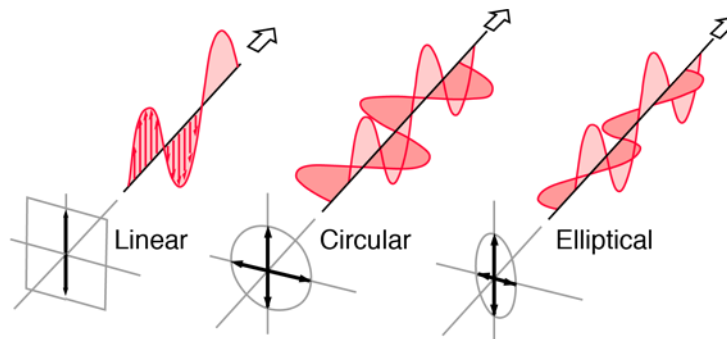
Slika 1: Primer polarizacije



S polarizacijo opisujemo le transverzalno valovanje, saj pri longitudinalnem smer nihanja količine sovpada s smerjo valovanja. Poznamo tri osnovne tipe polarizacije: linearno, krožno in eliptično. [10],[11]

Definicija 5 Val je linearno polariziran, če nihanje poteka le v eni smeri. Krožno in eliptično polarizacijo dobimo, kadar se s širjenjem vala nihanje suče. [10],[11]

Slika 2: Osnovni tipi polarizacije



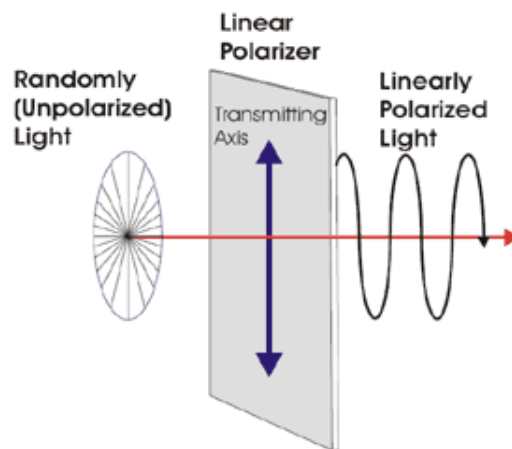
Če se smer nihanja neurejeno obrača v vse smeri govorimo o nedoločeni polarizaciji oziroma nepolariziranem valovanju. Takšno je naprimer svetloba, ki jo oddajajo navadna svetila, pa tudi Sonce. [9]

Elektromagnetno valovanje oziroma svetloba je transversalno valovanje. Sestavljeno je iz nihanja električnega in magnetnega polja, ki nihata pravokotno na smer valovanja ter pravokotno en na drugega. Po dogovoru je smer polarizacije enaka smeri nihanja jakosti električnega polja. [10],[11]

V nadaljevanju bomo potrebovali linearno polarizacijo fotonov, zato si pogledjmo kako jo lahko umetno ustvarimo. Naj še enkrat opomnimo, da polarizacija fotonov sovpada s polarizacijo elektromagnetnega valovanja.

Definicija 6 *Polarizator je naprava, ki valovanje z nedoločeno ali mešano polarizacijo spremeni v valovanje z določeno polarizacijo. [12]*

Slika 3: Delovanje polarizatorja



3 Kvantna razdelitev ključa

Definicija 7 *Šifriranje podatkov je pretvorba podatkov v obliko, ki je nepooblaščenim osebam ne razumejo. [15]*

Navadno šifriramo podatke z uporabo algoritmov ter drugih matematičnih postopkov. Čeprav je lahko tak postopek zelo učinkovit in ga morebitni vsiljivci težko dešifrirajo, pa je skoraj nemogoče preveriti prisotnost prisluškovalca. Prav to je izjemna lastnost kvantnega šifriranja podatkov. So-

govornika namreč ob koncu pogovora vesta, ali je njuno sporočila prejela še tretja oseba. [15]

Kvantna razdelitev ključa lahko poteka na več različnih načinov, ogledali si bomo postopek, ki ustreza protokolu BB84.

Za lažjo razlago postopka poimenujmo udeležence pri prenašanju sporočila.

Definicija 8 *Alica je pošiljatelj sporočila,
Bob sporočilo prejme,
Eva pa ga skuša prestreči, torej je prisluškovalka.*

Kako poteka kvantno šifriranje?

Spoznali smo že fotone, njihovo polarizacijo in izvedeli kako lahko polarizacijo spreminjamo. Torej lahko z različnimi polarizacijami fotonov predstavimo različne vrednosti. [16]

Zgled 1 Naj naprimer linearna polarizacija v smeri y osi (\uparrow) v binarnem zapisu pomeni 1, polarizacija v smeri x osi (\rightarrow) pa 0. Na ta način lahko Alica z zaporedjem fotonov, ki jim priredi polarizacijo pošlje Bobu število v binarnem zapisu. Zaporedje fotonov s polarizacijo $\uparrow \rightarrow \uparrow \uparrow \rightarrow$ tako predstavlja število 10110.

Lahko bi definirali še število 2 s polarizacijo v smeri premice pri kotu 45° (\nearrow), ter število 3 pri kotu 135° (\nwarrow). Z različnimi smermi polarizacije lahko predstavimo še druge vrednosti in tako šifriramo sporočilo. Vendar pa je bolj enostavno, če se omejimo na manjše število polarizacij in uporabimo kvantno šifriranje izključno za pošiljanje ključa, s katerim nato šifriramo nadaljna sporočila. [16]

Bob mora pri prejemu posameznega fotona uporabiti ustrezen polarizator, sicer odčitana vrednost ni nujno pravilna. Če je Alica foton polarizirala z \uparrow ali \rightarrow mora za pravilno interpretacijo Bob uporabiti polarizator oblike $+$, za \nearrow in \nwarrow polarizaciji pa polarizator \times . Taki obliki polarizatorja namreč omogočata nemoteno prehajanje fotonov z ustreznimi polarizacijami. Polarizatorjem določene oblike pravimo tudi baza polarizacije, npr. polarizator $+$ je baza polarizacije za polarizaciji \uparrow in \rightarrow . Kaj bi se zgodilo, če bi Bob pri prejemu fotona uporabil napačen polarizator? [1],[16]

Zgled 2 Recimo da Alica želi poslati vrednost 1, torej pošlje foton s polarizacijo \uparrow . Če Bob namesto polarizatorja $+$, ki bi pravilno odčital polarizacijo fotona uporabi polarizator \times , bo naključno prejel eno od \nearrow , \nwarrow polarizacij. Torej bo namesto vrednosti 1, prejel število 2 ali 3 oziroma ustrezno definirano vrednost pri posamezni polarizaciji. [16]

Pojavi se vprašanje kako naj bi Bob vedel, kateri polarizator mora uporabiti. Alice mu zaradi morebitne prisotnosti Eve seveda ne sme povedati katero polarizacijo je uporabila na fotonih. Odgovor je preprost: tudi Bob ne ve, kateri polarizator mora uporabiti, zato ga kar naključno izbere. Skoraj zagotovo torej Alice in Bob po koncu pošiljanja fotonov nimata enakega ključa. Komunikacijo lahko nadaljujeta po nevarovanem kanalu, pri čemer Alice Bobu pove, kateri polarizator je ustrezal posameznemu fotonu, ne izda pa točne polarizacije. Bob ji sporoči, pri katerih fotonih je uporabil pravilni polarizator. Fotone, pri katerih nista bila usklajena enostavno ignorirata in tako dobita končni ključ. [1],[17]

Zgled 3 Naj bo \uparrow oznaka za 1 in \rightarrow za 0 v polarizacijski bazi +, ter \nearrow oznaka za 1 in \nwarrow za 0 v bazi \times . [16]

vrednost	1	0	1	1	0	0	1	1	0	0	1	1
baza polarizacije	+	+	\times	+	\times	\times	\times	+	\times	+	+	\times
polarizacija	\uparrow	\rightarrow	\nwarrow	\uparrow	\nearrow	\nearrow	\nwarrow	\uparrow	\nearrow	\rightarrow	\uparrow	\nwarrow
Bobov polarizator	+	\times	+	+	\times	\times	+	+	\times	+	\times	\times
odčitana polarizacija	\uparrow	\nearrow	\rightarrow	\uparrow	\nearrow	\nearrow	\uparrow	\uparrow	\nearrow	\rightarrow	\nearrow	\nwarrow
odčitana vrednost	1	0	0	1	0	0	1	1	0	0	0	1
končni ključ	1	-	-	1	0	0	-	1	0	0	-	1

Zakaj nam torej tak prenos podatkov omogoča zaznavo prisluškovalca? Če Eva želi dobiti sporočilo, ki ga Alice pošilja Bobu, mora prestreči poslane fotone, pri tem pa za odčitavanje polarizacij uporabiti enega od polarizatorjev. Eva ne ve katero polarizacijo je Alice izbrala za posamezen foton in lahko le naključno izbere polarizator, s katerim bo prebrala foton in ga nato poslala naprej Bobu. Ima torej 50% možnosti, da se pri izbiri zmoti, s tem pokvari prvotno polarizacijo in zato Bobu posreduje napačno polariziran foton. Bob prejme foton in tako kot Eva naključno izbere polarizator. Sledijo štirje možni scenariji.

- Tako Eva kot Bob sta pravilno izbrala polarizatorja, zato se polarizacija ohrani in oba odčitata pravilno vrednost fotona. (prvi foton v spodnjem zgledu)
- Eva je izbrala napačen polarizator in tako pokvarila prvotno polarizacijo. Bob je izbral enak polarizator kot Eva, torej je odčital njeno

naključno spremenjeno polarizacijo, ki se razlikuje od Alicine. Ker imata Alica in Bob v tem primeru različni bazi polarizacije bosta ta foton zanemarila. (drugi foton v spodnjem zgledu)

- Eva je izbrala napačen polarizator. Bob je izbral enak polarizator kot Alica, vendar je od Eve prejel spremenjeno polarizacijo, ki ne ustreza njegovi izbiri polarizatorja. Odčital bo naključno polarizacijo iz baze, ki jo je izbral. V polovici primerov te vrste bo prišlo do razlikovanja v vrednosti kljub temu, da sta Alica in Bob uporabila enaki bazi polarizacije. (tretji foton v spodnjem zgledu)
- Zadnja možnost je enaka prejšnji, le da Bob na koncu po naključju odčita pravilno polarizacijo, torej tisto, ki jo je poslala Alica in to kljub posredovanju Eve. (šesti foton v spodnjem zgledu)

V tretjem primeru, bosta torej Alica in Bob pri pregledovanju polarizatorjev pod vtisom, da se njuni vrednosti ujemata, vendar zaradi Eve temu ni tako. V resnici nimata enakega ključa za šifriranje, zato Bob prejetega sporočila ne bo mogel dešifrirati s svojim ključem. Tako bosta vedela, da je bila med pošiljanjem ključa prisotna Eva. [1],[16]

Zgled 4 Primer z Evino prisotnostjo. [1]

vrednost	0	1	1	0	1	0	0	1
baza polarizacije	+	+	×	+	×	×	×	+
polarizacija	→	↑	↖	→	↖	↗	↗	↑
Evin polarizator	+	×	+	+	×	+	×	+
nova polarizacija	→	↗	↑	→	↖	↑	↗	↑
Bobov polarizator	+	×	×	×	+	×	+	+
odčitana polarizacija	→	↗	↗	↖	↑	↗	→	↑
odčitana vrednost	0	0	0	1	1	0	0	1
končni ključ	0	-	0	-	-	0	-	1
ujemanje ključev	✓	-	✗	-	-	✓	-	✓

4 Sudoku

Definicija 9 *Sudoku je logična uganka, pri kateri je cilj zapolniti mrežo velikosti 9×9 s števili od 1 do 9 tako, da se vsako število v vsakem stolpcu, vrstici in 3×3 kvadratu znotraj mreže pojavi natanko enkrat. [3]*

Slika 4: Primer rešenega sudokuja

	2		5		1		9	
8			2		3			6
	3			6			7	
		1				6		
5	4						1	9
		2				7		
	9			3			8	
2			8		4			7
	1		9		7		6	

4	2	6	5	7	1	3	9	8
8	5	7	2	9	3	1	4	6
1	3	9	4	6	8	2	7	5
9	7	1	3	8	5	6	2	4
5	4	3	7	2	6	8	1	9
6	8	2	1	4	9	7	5	3
7	9	4	6	3	2	5	8	1
2	6	5	8	1	4	9	3	7
3	1	8	9	5	7	4	6	2

Sudokuja se je domislil američan Howard Garns in ga prvič objavil leta 1979. Pravijo, da idejo dobil na podlagi Eulerjevega latinskega kvadrata. To je matrika velikosti $n \times n$, napolnjena z n različnimi znaki, pri čemer se vsak znak v vrstici in stolpcu pojavi natanko enkrat. Čez 5 let so uganko objavili tudi na Japonskem in jo poimenovali "Suuji wa dokushin ni kagiru", kar v prevodu pomeni "števke morajo biti edine", prvi zlogi besed pa nam podajo ravno znano ime uganke: SUDOKU. [3],[4]

Število vseh možnih sudoku mrež, pri velikosti 9×9 je približno 6,6 trilijonov natančneje 6.670.903.752.021.072.936.960. Zahtevnost uganke je obratno sorazmerna s številom že vpisanih števil. Lažji sudokuji imajo tako podanih več kot 30 števil, težji pa nekje med 20 in 30. Dolgo je bil odprt problem najmanjšega števila začetnih števil, ki še vedno podajo enolično rešitev. Leta 2012 so dokazali, da je to število 17, saj je bilo iskanje enolične rešitve s pomočjo računalnika za sistem s 16 podanimi števili neuspešno. [3],[4]

Skozi leta so se razvile različne oblike sudokuja in prispevale k težavnosti reševanja. Poznamo na primer Sudoku X, pri katerem mora poleg standardnih pogojev veljati še, da se števila tudi na diagonalah pojavijo le enkrat. Še bolj ekstremna oblika pa je geometrijski sudoku, pri katerem znotraj

mreže nimamo 3×3 kvadratov, temveč različne geometrijske like sestavljene iz devetih polj. [3],[4]

Slika 5: Geometrijski sudoku

3								4
		2		6		1		
	1		9		8		2	
		5				6		
	2						1	
		9				8		
	8		3		4		6	
		4		1		9		
5								7

5 Sudoku ključ

Na primeru si oglejmo kako poteka kvantno razdeljevanje ključa s pomočjo sudoku mreže. [1]

Alica se odloči, da bo ključ za šifriranje poslala Bobu s pomočjo fotonov tako, da bo zaporedje polarizacij predstavljalo rešitev 4×4 sudoku mreže. Poslala bo sledeč sudoku:

0	1	2	3
3	2	1	0
2	0	3	1
1	3	0	2

Pri tem pa uporabila polarizacije:

vrednost	0	1	2	3
polarizacija	\rightarrow	\uparrow	\nwarrow	\nearrow
baza polarizacije	+	+	\times	\times

Če sudoku mrežo pretvorimo v zaporedje fotonov z ustrezno polarizacijo dobimo:

vrednost	0	1	2	3	3	2	1	0	2	0	3	1	1	3	0	2
baza	+	+	×	×	×	×	+	+	×	+	×	+	+	×	+	×
polarizacija	→	↑	↖	↗	↗	↖	↑	→	↖	→	↗	↑	↑	↗	→	↖

Po prej opisanem postopku, Alice Bobu pošlje fotone, on pa jih prestreže in na vsakem uporabi naključno izbrano bazo polarizacije, torej + ali ×.

vrednost	0	1	2	3	3	2	1	0	2	0	3	1	1	3	0	2
baza	+	+	×	×	×	×	+	+	×	+	×	+	+	×	+	×
polarizacija	→	↑	↖	↗	↗	↖	↑	→	↖	→	↗	↑	↑	↗	→	↖
Bobova baza	+	×	+	+	×	×	+	×	+	×	×	+	×	×	×	×
prejeta vrednost	0	-	-	-	3	2	1	-	-	-	3	1	-	3	-	2

Bob lahko vrednosti, pri katerih sta se njegova in Alicina baza polarizacije ujemali vnese v 4x4 mrežo in na ta način dobi nerešen sudoku.

0			
3	2	1	
		3	1
	3		2

Sudoku reši po pravilih reševanja in dobi celoten ključ za šifriranje.

Minimalno število podanih števil za enolično rešitev sudokuja velikosti 4x4 je 4, kar pomeni, da mora Bob pravilno odčitati polarizacije vsaj štirih fotonov. V nasprotnem primeru morata postopek ponoviti, seveda z novim ključem. [17]

Če je bila pri prenašanju ključa prisotna tudi Eva, bo pokvarila postavitev števil, ki omogoča pravilno rešitev sudokuja in tako razkrila svojo prisotnost. Bob namreč ne bo mogel rešiti sudoku mreže na način, ki bi ustezal pravilom. [16]

6 Zaključek

Prednost pošiljanja ključa za šifriranje s pomočjo sudokuja je v tem, da Bobu ni potrebno povedati, pri katerih fotonih je izbral pravilni polarizator. Slaba lastnost se skriva v tem, da tudi Eva pozna enostaven postopek, s katerim dobi celoten ključ, če je pravilno odčitala zadostno število polarizacij. V našem zgledu potrebuje le 4 števila.

Seveda pa ne smemo pozabiti, da bo Eva s svojim posredovanjem v večini primerov pokvarila pravilno postavitve sudokuja. Bob bo zaznal njeno prisotnost v trenutku, ko bo ugotovil, da ne more rešiti sudokuja in opozoril Alico, še preden mu pošlje šifrirano sporočilo. Tako Eva sicer lahko dobi pravi ključ, vendar ne bo dobila sporočila, saj bosta Alica in Bob komunikacijo prekinila in ponovila postopek z novim ključem.

Literatura

- [1] Wikipedia, 2018. Quantum key distribution,
Dostopno na: https://en.wikipedia.org/wiki/Quantum_key_distribution [24.3.2018]
- [2] Tratnik, J., Batagelj B., 2008. Predstavitev ideje kvantnega šifriranja in pregled osnovnih tehnik kvantnega razdeljevanja ključa. Elektrotehniški vestnik. 75(5): 257-263.
Dostopno na: <http://ev.fe.uni-lj.si/5-2008/Tratnik.pdf> [2.4.2018]
- [3] Wikipedia, 2016. Sudoku,
Dostopno na: <https://sl.wikipedia.org/wiki/Sudoku> [18.4.2018]
- [4] Wikipedia, 2018. Sudoku,
Dostopno na: <https://en.wikipedia.org/wiki/Sudoku> [18.4.2018]
- [5] Wikipedia, 2017. Photon polarization,
Dostopno na: https://en.wikipedia.org/wiki/Photon_polarization [20.4.2018]
- [6] Wikipedia, 2018. Photon,
Dostopno na: <https://en.wikipedia.org/wiki/Photon> [20.4.2018]
- [7] Wikipedia, 2018. Elementary particle,
Dostopno na: https://en.wikipedia.org/wiki/Elementary_particle [20.4.2018]

- [8] Wikipedia, 2018. Svetloba,
Dostopno na: <https://sl.wikipedia.org/wiki/Svetloba>
[20.4.2018]
- [9] Kuščer, I., Moljk, A., Kranjc, T., Peternej, J., Rosina, M., Strnad, J.,
2002, *Fizika za srednje šole 3. del*, Ljubljana: DZS, d.d.
- [10] Wikipedia, 2018. Polarizacija valovanja,
Dostopno na: https://sl.wikipedia.org/wiki/Polarizacija_valovanja [20.4.2018]
- [11] Wikipedia, 2018. Polarization,
Dostopno na: [https://en.wikipedia.org/wiki/Polarization_\(waves\)](https://en.wikipedia.org/wiki/Polarization_(waves)) [20.4.2018]
- [12] Wikipedia, 2013. Polarizator,
Dostopno na: <https://sl.wikipedia.org/wiki/Polarizator>
[20.4.2018]
- [13] Wikipedia, 2018. Polarizer,
Dostopno na: <https://en.wikipedia.org/wiki/Polarizer>
[20.4.2018]
- [14] Cloud security alliance: What is Quantum Key Distribution,
Dostopno na: https://www.quintessencelabs.com/wp-content/uploads/2016/09/CSA_What-is-Quantum-Key-Distribution-QKD_QSS.pdf [21.4.2018]
- [15] Wikipedia, 2018. Encryption,
Dostopno na: <https://en.wikipedia.org/wiki/Encryption>
[21.4.2018]
- [16] Jones, S., 2016. Quantum distribution of a sudoku key, *Recreational Mathematics Magazine*, 2016(6), 87-93.
Dostopno na: <https://www.degruyter.com/downloadpdf/j/rmm.2016.3.issue-6/rmm-2016-0009/rmm-2016-0009.pdf> [7.5.2018]
- [17] Wikipedia, 2018. Mathematics of Sudoku,
Dostopno na: https://en.wikipedia.org/wiki/Mathematics_of_Sudoku [7.5.2018]