

Kodiranje s pomočjo sudoku ključa

Klementina Pirc

26.04.2018

1 Uvod

V današnjem svetu, kjer se vsak dan preko različnih komunikacijskih kanalov pretoči nepredstavljiva količina informacij, se pojavi vprašanje varovanja osebnih podatkov. Tema je še posebej aktualna na področju spletnih bančnih storitev in drugih podobno 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 prisluškovalec 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 šifrnega 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 prisluškovalec 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]

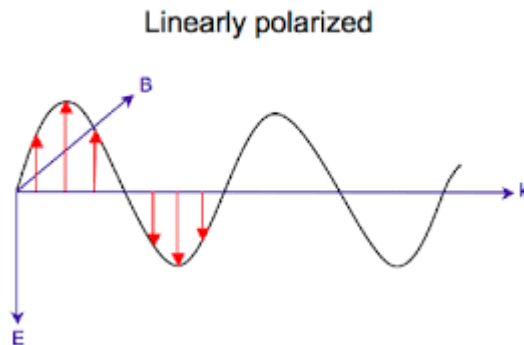
Definicija 3 Foton je brezmasni in električno nevtralen osnovni delec, ki potuje s svetlobno hitrostjo in je osnovni gradnik svetlobe. [6],[9]

Torej si lahko širjenje svetlobe oziroma elektromagnetnega valovanje 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

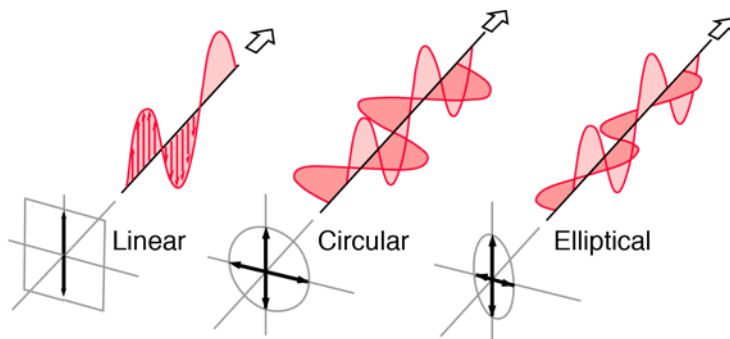


S polarizacijo opisujemo le transversalno valovanje, saj pri longitudinalnem smer nihanja količine sovpada s smerjo valovanja. Poznamo tri osnovne tipe polarizacije: linearno, krožno in eliptično. [10],[11]

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

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]

Slika 2: Osnovni tipi polarizacije

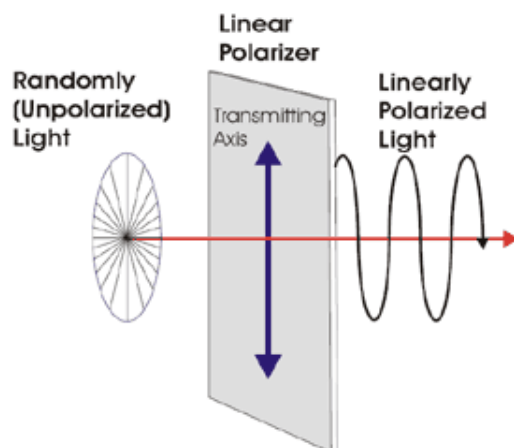


Elektromagnetno valovanje oziroma svetloba je transverzalno valovanje. Sestavljeno iz nihanja električnega in magnetnega polja, ki nihata pravokotno na smer valovanja ter pravokotno en na drugega. Po dogovoru je smer polarizacije enaka smeri nihanja jakosti električnega polja. [10],[11]

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.*

Slika 3: Delovanje polarizatorja



3 Kvantna razdelitev ključa

Definicija 7 Šifriranje podatkov je pretvorba podatkov v tako obliko, da je nepooblaščen oseba 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, sogovornika namreč ob koncu pogovora veta, ali je njuno sporočila prejela še tretja oseba. [16]

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 preštréči, 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. [17]

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 1 0 1 1 0.

Lahko bi definirali še število 2 s polarizacijo v smeri premice pri kotu 45° (\nearrow), ter število 3 pri kotu 135° (\nwarrow) itd., potrebujemo le ustrezni polarizator. Bolj enostavno je, če se omejimo na manjše število polarizacij in uporabimo kvantno šifriranje izključno za pošiljanje ključa, s katerim nato šifriramo nadaljna sporočila. [17]

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 . Kaj bi se zgodilo, če bi Bob pri prejemu fotona uporabil napačen polarizator? [1],[17]

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. [17]

Pojavi se vprašanje kako naj bi Bob vedel, kateri polarizator mora uporabiti. Alica 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 Alica in Bob po koncu pošiljanja fotonov nimata enakega ključa. Komunikacijo lahko nadaljujeta po nevarovanem kanalu, pri čemer Alica 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 \nwarrow oznaka za 1 in \nearrow za 0 v bazi \times . [17]

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 Alica pošilja Bobu, mora prestreči poslane fotone, pri tem pa uporabiti enega od polarizatorjev. Eva ne ve katero polarizacijo je Alica 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. Pri preverjanju uporabe polarizatorjev in po potrebi tudi manjših delov ključa bosta Alice in Bob ugotovila, da prihaja do odstopanj. [1],[17]

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	✓	-	✗	-	-	✓	-	✓

Opazimo, da je pri tretjem fotonu prišlo do razlikovanja v vrednosti kljub temu, da sta Alice in Bob uporabila enaki bazi polarizacije. To jima pove, da je bila Eva prisotna pri pošiljanju ključa.

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 naprimer 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 4x4 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	→	↑	↖	↗
baza polarizacije	+	+	×	×

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, Alica 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.