Kodiranje s pomočjo sudoku ključa

Klementina Pirc

Fakulteta za matematiko in fiziko
Oddelek za matematiko

26. april 2018

Uvod

- varovanje podatkov
- prednost kvantnega šifriranja

Polarizacija fotonov

Definicija

Osnovni delec je delec ki nima podstrukture, torej ni sestavljen iz manjših delcev.

Definicija

Svetloba je elektromagnetno valovanje pri različnih valovnih dolžinah oziroma frekvencah.

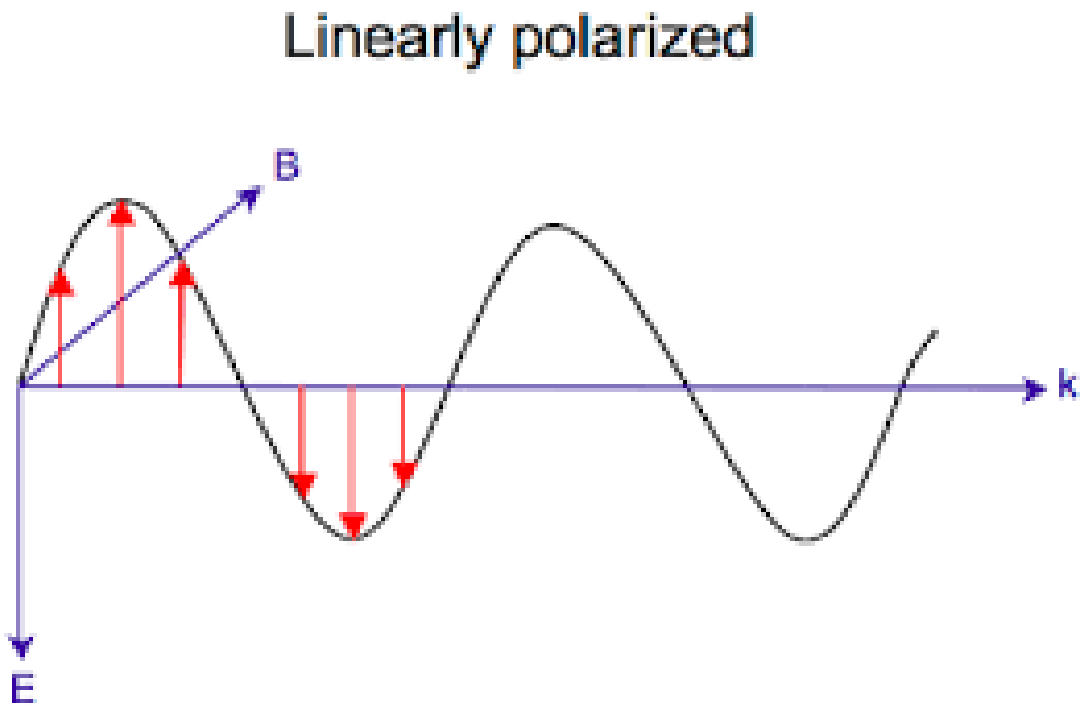
Definicija

Foton je brezmasni in električno nevtralen osnovni delec, ki potuje s svetlobno hitrostjo in je osnovni gradnik svetlobe.

Polarizacija valovanja

Definicija

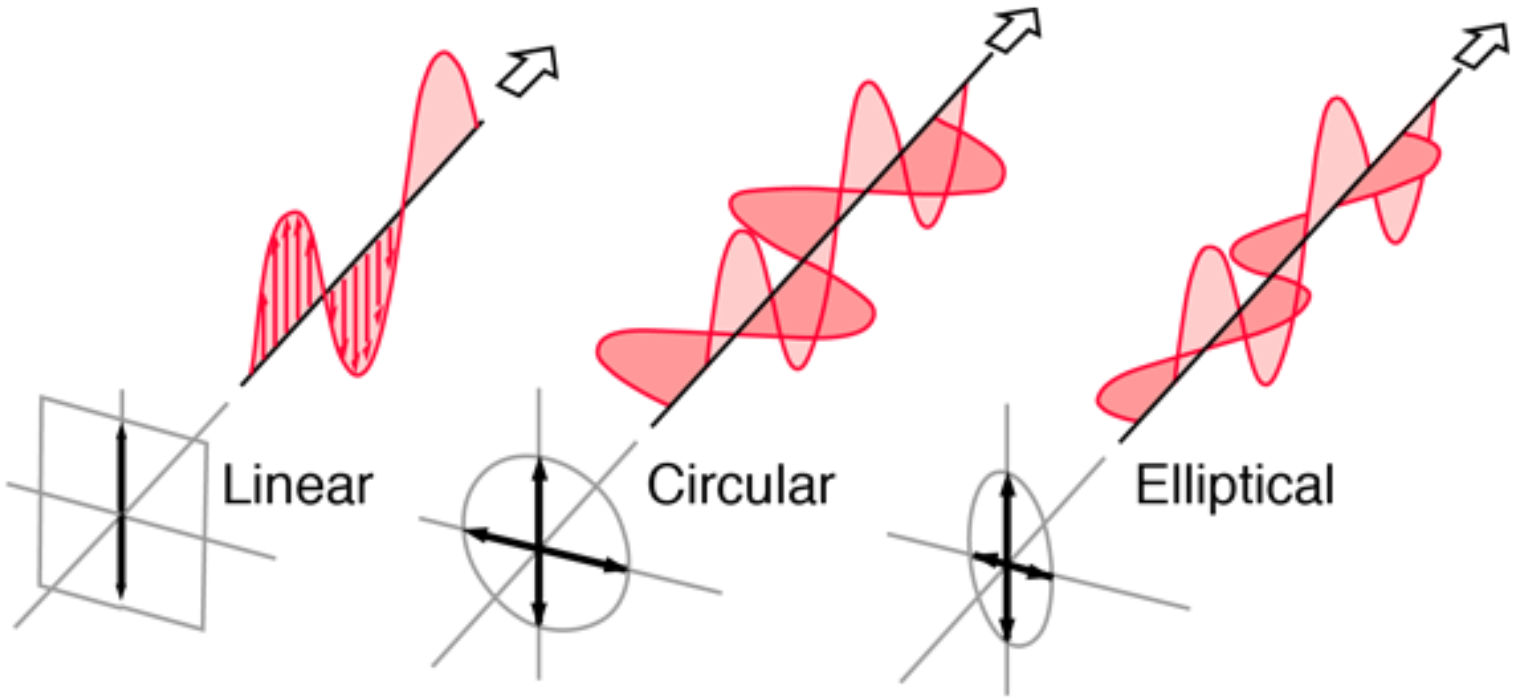
Polarizacija valovanja opisuje smer nihanja količine ki valuje.



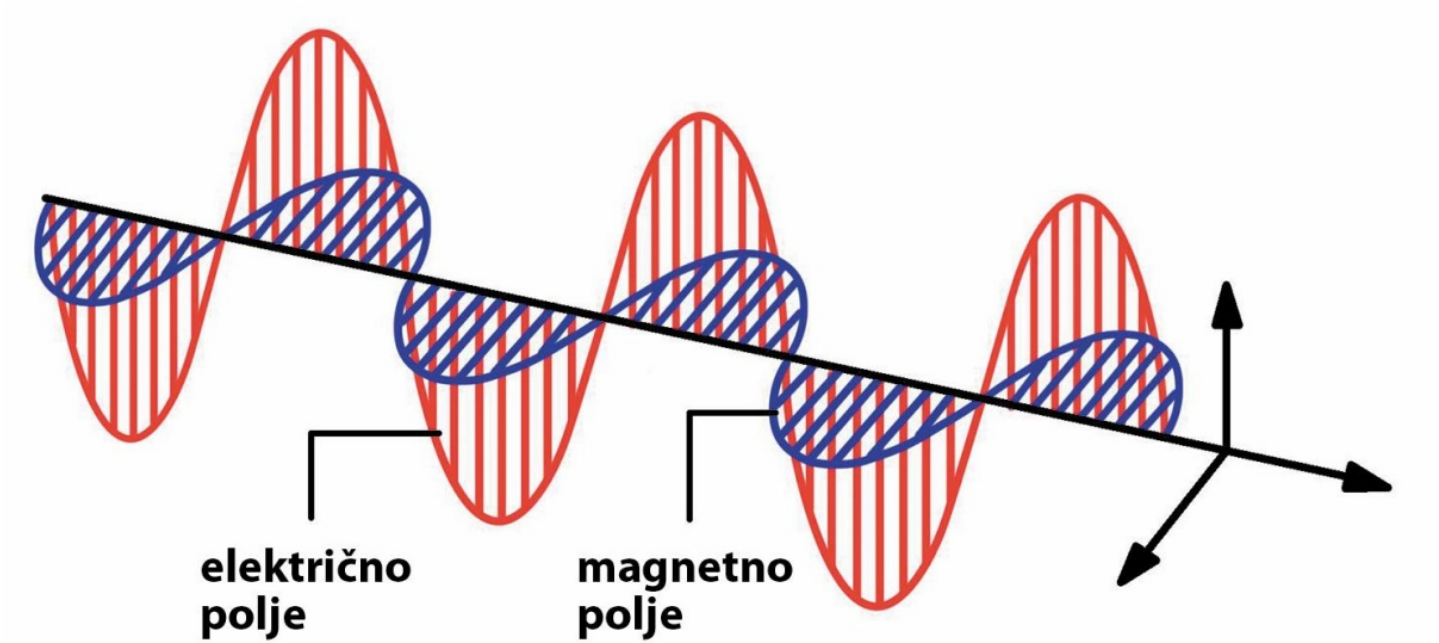
Osnovne polarizacije

Definicija

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



Elektromagnetno valovanje



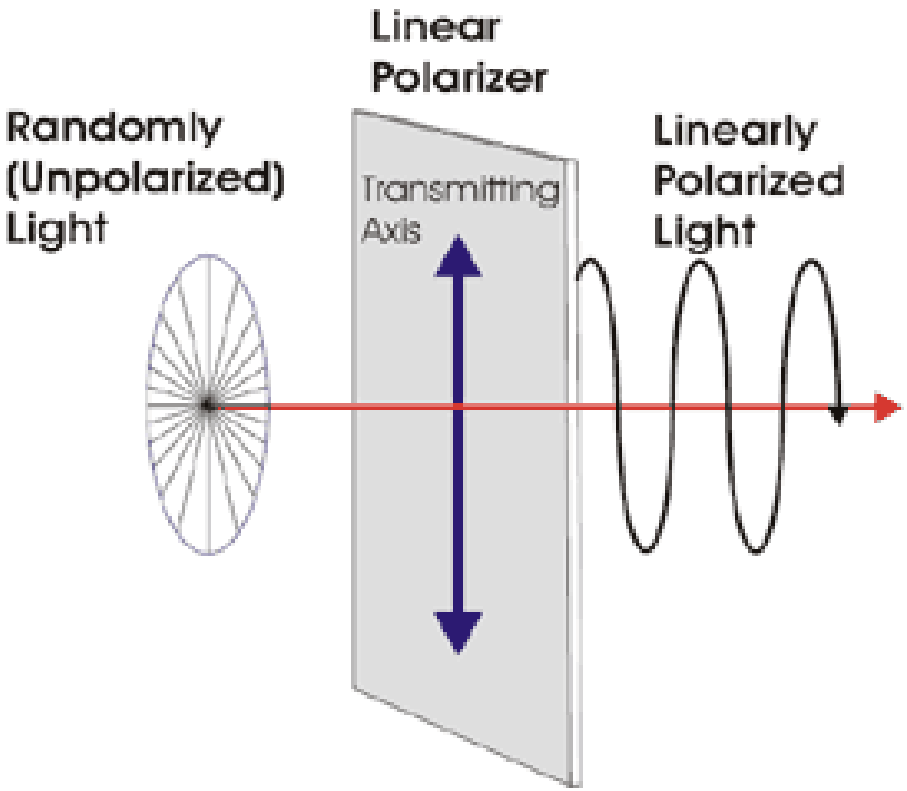
Dogovor

Smer polarizacije je enaka smeri nihanja jakosti električnega polja.

Polarizator

Definicija

Polarizator je naprava, ki valovanje z nedoločeno ali mešano polarizacijo spremeni v valovanje z določeno polarizacijo.



Kvantna razdelitev ključa

Definicija

Šifriranje podatkov je pretvorba podatkov v obliko, ki je nepooblaščene osebe ne razumejo.

Definicija

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

Zaporedje polariziranih fotonov

Vrednost in ustrezna polarizacija:

vrednost	0	1
polarizacija	$\rightarrow$	$\uparrow$

Število v binarnem zapisu kot zaporedje polariziranih fotonov:

vrednost	1	0	1	1	0
polarizacija	$\uparrow$	$\rightarrow$	$\uparrow$	$\uparrow$	$\rightarrow$

Prejemanje polariziranih fotonov

vrednost	1	0	1	0
polarizacija	↑	→	↖	↗
baza polarizacije	+	+	×	×

Alica

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

Bob

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

ključ	1	-	-	1	0	0	-	1	0	0	-	1

Primer prisluškovalca

vrednost	0	1	1	0	1	0	0	1
polarizacija	→	↑	↖	→	↖	↗	↗	↑
baza polarizacije	+	+	×	+	×	×	×	+
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	✓	-	✗	-	-	✓	-	✓

Sudoku

Definicija

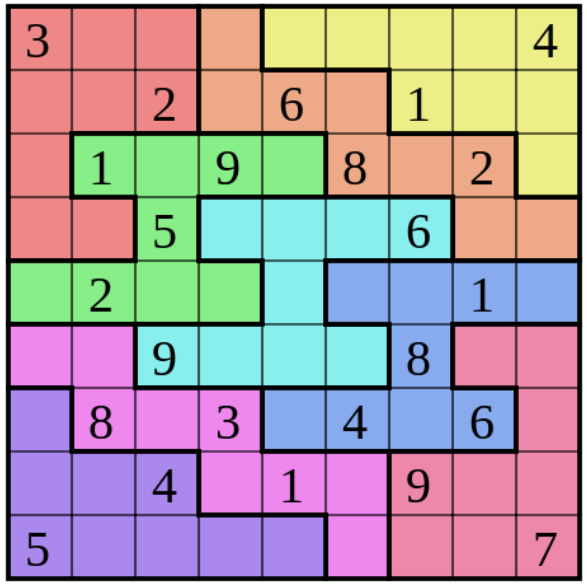
Sudoku je logična uganka, pri kateri je cilj zapolniti mrežo velikosti 9x9 s števili od 1 do 9 tako, da se vsako število v vsakem stolpcu, vrstici in 3x3 kvadratu znotraj mreže pojavi natanko enkrat.

	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*

Lastnosti sudokuja

- Howard Garns (1979)
- 6.670.903.752.021.072.936.960 mrež velikosti 9x9
- težavnost
- problem najmanjšega števila podanih števil
- Sudoku X, geometrijski sudoku



Sudoku ključ

Izbran sudoku:

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

Izbrane polarizacije:

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

Alica

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

Bob

baza	+	×	+	+	×	×	+	×	+	×	×	+	×	×	×	×
vrednost	0	.	.	.	3	2	1	.	.	.	3	1	.	3	.	2