

# 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 pozna le prejemnik in ga nato uporabi za dešifriranje prejetega 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 svetlobnih delcev - fotonov. 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 prisluškovalec in po potrebi pripravimo nov ključ za šifriranje. [2]

## 2 Polarizacija fotonov

## 3 BB84 protokol

## 4 Kvantna razdelitev ključa

## 5 Sudoku

**Definicija 1** *Sudoku je logična uganka, pri kateri je cilj zapolniti mrežo velikosti  $9 \times 9$  s števili od 1 do 9 tako, da se vsako število v vsakem stolpcu,*

vrstici in  $3 \times 3$  kvadratu znotraj mreže pojavi natanko enkrat. [3]

Slika 1: 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]

Število vseh možnih sudoku mrež, pri velikosti  $9 \times 9$  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 za sistem s 16 podanimi števili niso našli rešitve. [3]

Skozi leta so se razvile različne oblike sudokujev 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  $3 \times 3$  kvadratov, temveč različne geometrijske like sestavljene iz devetih polj. [3]

## 6 Sudoku ključ

Slika 2: 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