Kvantna kriptografija

Tehničko i naučno pisanje

Igor Glišović, *mi22292@alas.matf.bg.ac.rs*
Željko Zekavičić, *mi22130@alas.matf.bg.ac.rs*
Nađa Lazarević, *mi22175@alas.matf.bg.ac.rs*
Ana Mladenović, *mi22119@alas.matf.bg.ac.rs*

Matematički fakultet
Univerzitet u Beogradu

Beograd, 2022.

Literatura

- Zasnovano na seminarskom radu:
  Kvantna kriptografija; Igor Glišović, Željko Zekavičić, Nađa Lazarević, Ana Mladenović

Uvod

- Kriptografija - očuvanje tajnosti podataka
- Razvoj klasične kriptografije - OneTimePad
- Problem moderne kriptografije: **"Kvaka 22"**

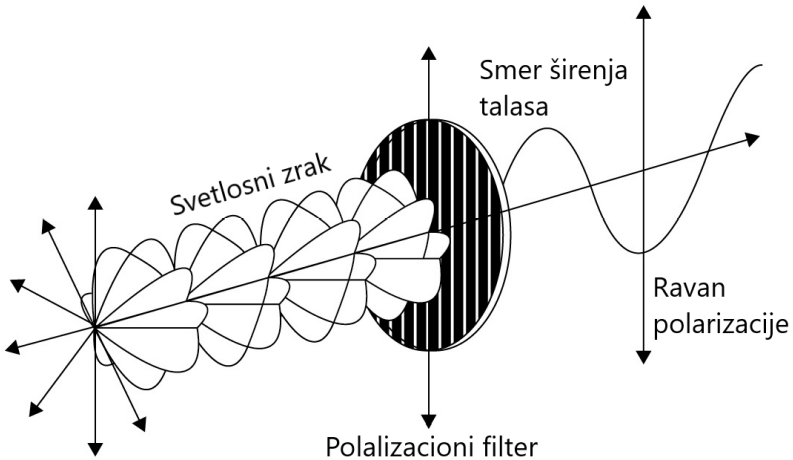
Komunikacija između pošiljaoca i primaoca je sigurna

$$\Longleftrightarrow$$

Kriptografski sistem je siguran

Istorijat

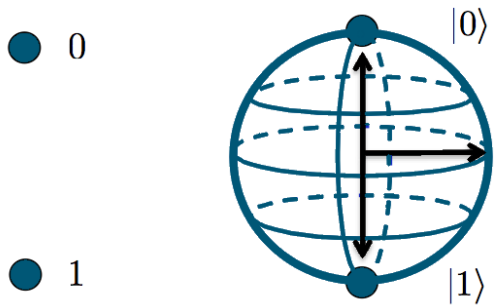
- Sigurna komunikacija - pitanje sve od praistorije pa do XX veka
- Stephen Weisner - tvorac kvantne kriptografije
- C.H.Bennet, G. Brassard - kvantna kriptografija na delu
- Arthur Ekert - kvantna isprepletanost



Slika 1: *Polarizacija fotona - osnova kvantne kriprografije*

Kvantna mehanika, kvantni računari

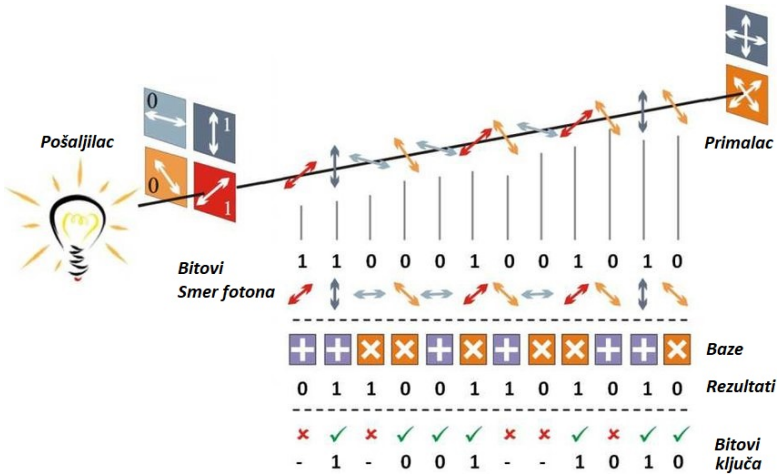
- Aspekti kvantne mehanike
  - aspekt prirodne neodređenosti
  - aspekt kvantnog sprezanja
  - uticaj međusobnog delovanja čestica
- Osnova kvantnih računara - kvantni biti, **kubiti**



Slika 2: *bit (levo), kubit (desno)*

Kvantni protokoli, kvantna razmena ključa

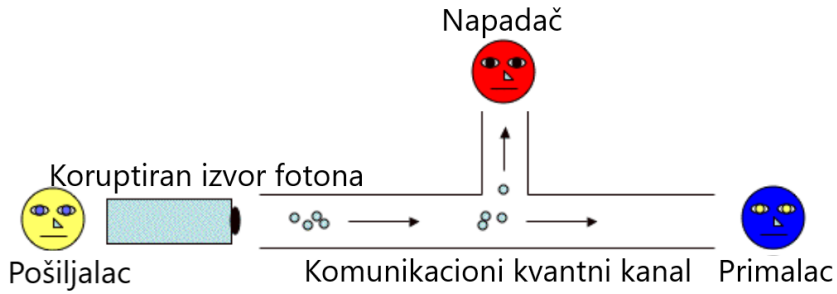
- Distribucija kvantnih ključeva (*QKD - Quantum Key Distribution*) i različiti protokoli
  - BB84 protokol ("pripremi i izmeri")
  - E91 protokol (isprepletanost kubita)



Slika 3: *Metodika rada BB84 protokola*

Vrste napada na sistem i odbrana

- Nekoliko vrsta napada na kriptografske sisteme:
  - "Middleman" napad
  - PNS (photon-number splitting) napad
  - Hakerski napad
  - DOS (denial of service) napad
- Zaštitu obezbeđujemo **sigurnim i pouzdanim sistemom**



Slika 4: *PNS napadač iskorišćava slabost sistema*

Implementacija kvantne kriptografije

- Što je veća udaljenost slanja - nesigurniji je sistem
- Kineski istraživači - "pouzdani" relejni čvorovi
- Shorov algoritam za faktorizaciju brojeva

Naziv i godina projekta	**Dužina prenosa**
Prenos novca Creditanstalt banke, Austrija 2004.	1.45 km
IdQuantique i Deckpoint kolaboracija, Švajcarska 2005.	10 km
Povezivanje Kanarskih ostrva, Španija 2006.	144 km
SECOQC, prvi kvantno-kriptografski računar, Austrija 2008.	200 km

Tabela 1: *Razvoj dužine prenosa kvantno-kriptografskih sistema*

Zaključak

- Veoma sigurni sistemi koji se razvijaju i danas
- Šira primena je trenutno nemoguća zbog **cene implementacije** potrebne infrastrukture
- Primena kvantne kriptografije u budućnosti je izvesna

Slika 5: *"Luksuz" korišćenja ovakvih sistema sada mogu priuštiti samo najimućnije firme, poput Toshibe*