



# Eksperimentalne tehnike kvantne komunikacije i kvantne informatike

-  
program NT AMOP

**Dr. sc. Mario Stipčević**

**Institut Ruđer Bošković**

**IF(S) 24. siječanj 2006.**

Izmjene 31.01.2006.

# Kvantna kriptografija

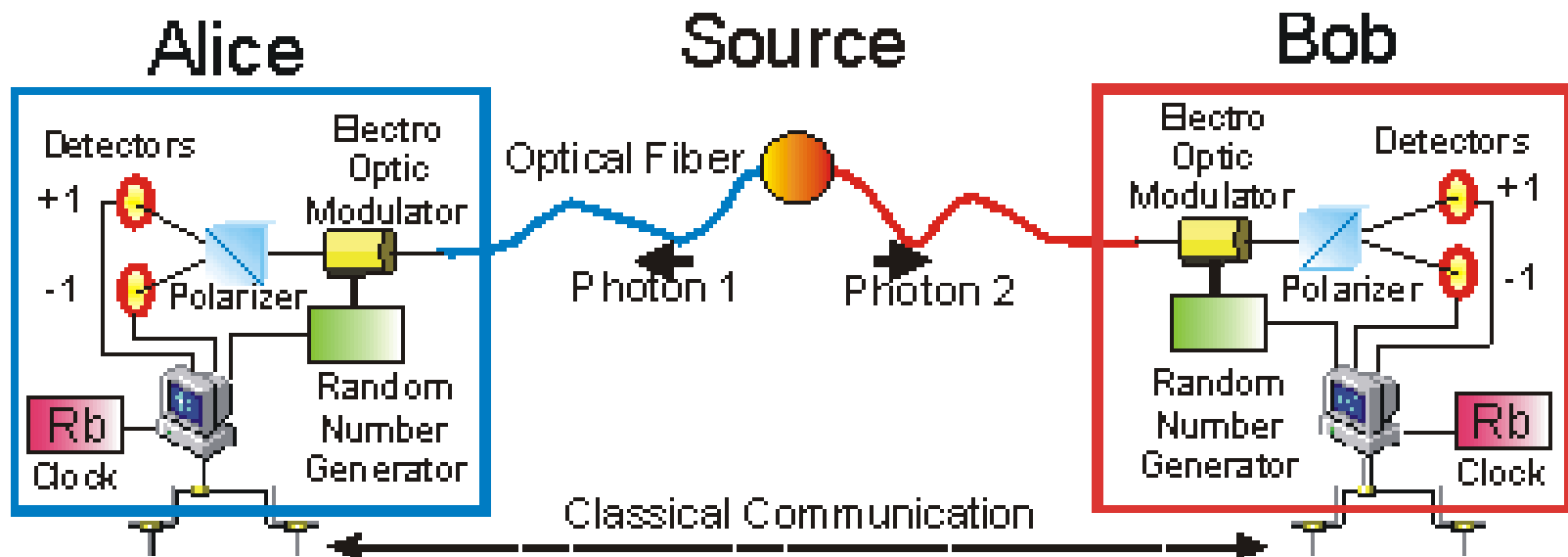
**1985.** H.C.**Bennett** (IBM) i G. **Brassard** (UniMontreal) objavom jednog “štosa” o tome kako kvantna mehanika može poslužiti za ostvarenje kriptografski sigurnog prijenosa poruka/podataka. Protokol je nazvan **BB84**.

**1991.** Ostvaren je prvi uređaj koji je utjelovio BB84

Kvantna kriptografija je prvi eksperiment zasnovan na kvantnoj informatici i ujedno prvi primjer kvantne komunikacije. Također i prvi uređaj QI koji je komercijaliziran.

**1992. Eckert** modificira BB84 i uvodi (teorijski) uređaj za **entanglement**

# Kvantna kriptografija



Svrha kvantne kriptografije je da Alice i Bob uspostave generiraju identični tajni ključ kojim mogu javni kanal pretvoriti u privatni

# Entanglement

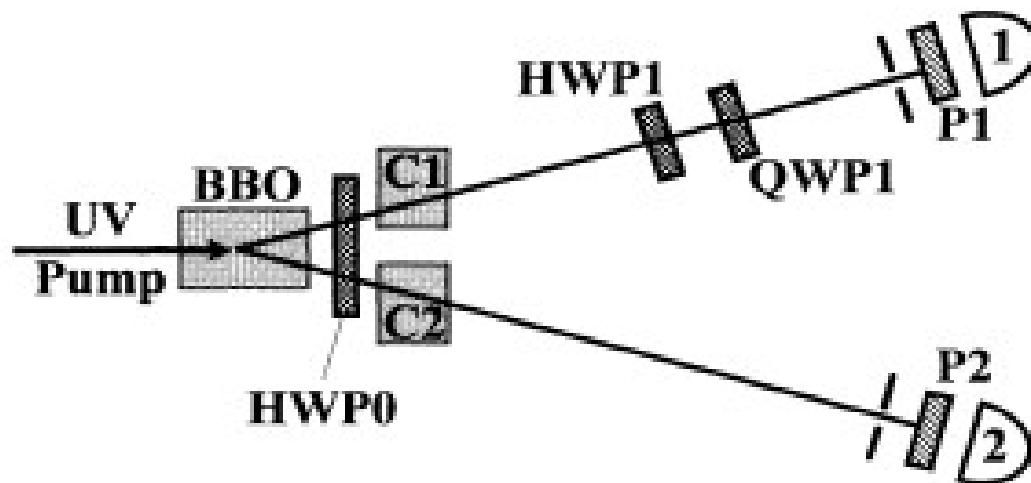
Svojstvo dvočestične valne funkcije da mjerenjem nekog svojstva jedne čestice utječemo na rezultat mjerenja tog svojstva druge čestice. Interesantni su maksimalno isprepleteni sistemi kao npr. **EPR** parovi.

U novije doba radi se najviše s fotonima. Njih je lako:

- proizvesti
- manipulirati
- Transportirati na veliku udaljenost
- detektirati
- pa čak i spregnuti.

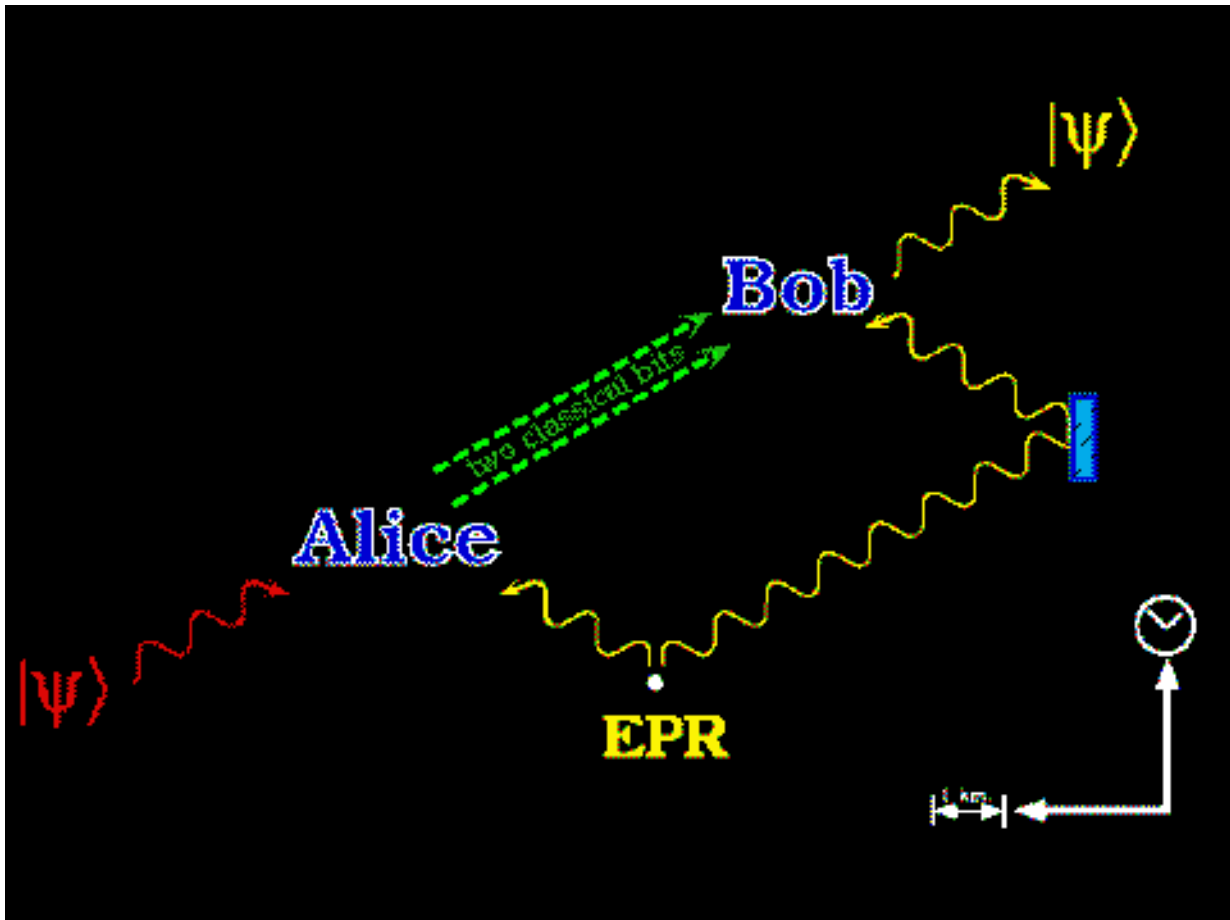
# Entanglement s fotonima

1995. P.G.Kwait, A. Zeilinger demonstriraju uređaj za obilatu proizvodnju polarizacijski isprepletenih FOTONA na principu “parametarskog cijepanja” fotona u nelinearnom kristalu.



Gledajući intenzitet upadnog svjetla na nivou kvanata, na izlazu se pojavljuju EPR fotonski parovi.

# Kvantna teleportacija



Najvažnija komponenta je uređaj za EPR parove fotona

# Kvantna informatika

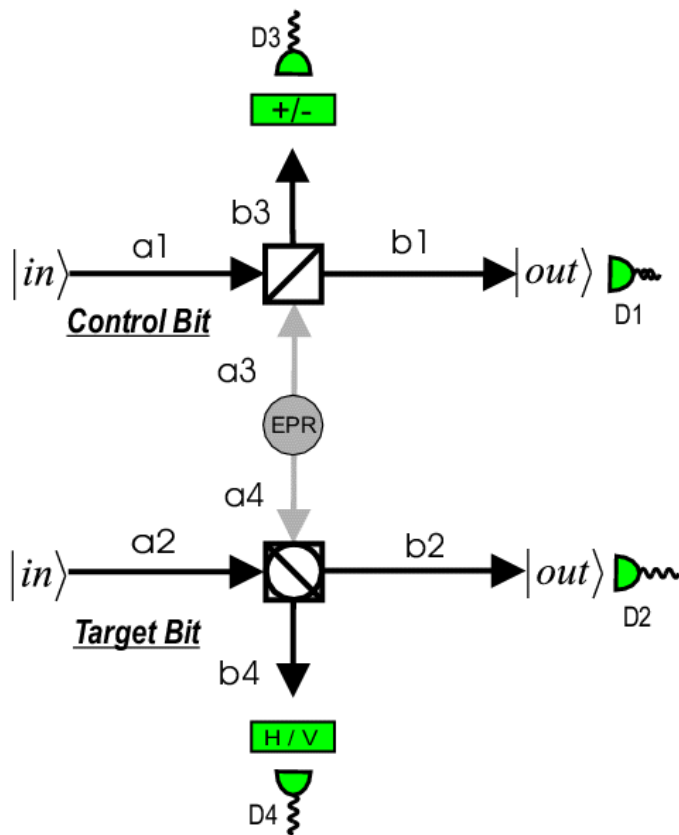
**1982.** Formuliran je “no cloning teorem” koji kaže da  $QM$  ne dopušta kloniranje/multipliciranje nepoznatog kvantnog stanja nekog sistema (npr. fotona nepoznate transverzalne polarizacije).

Istovremeno se počinju javljati ideje o mogućem odgovoru na Feynmanovo pitanje: ako je Turingovim računalima teško (sporo) računati neke kvantne sisteme, može li Kvantna mehanika omogućiti brža/drugačija računala ?

# Kvantna računala

Iz te priče razvila se grana kvantne fizike koja izučava kvantna računala i moguće algoritme koje ona može “brzo” riješiti. Za sada su to:

5. Sortiranje (Groverov algoritam)
6. Rastav cijelih brojeva na proste (prim) faktore
7. Računanje diskretnih algoritama
8. ??



Fotonska CNOT vrata,  
dovoljna za kvantno  
računanje

Centralna komponenta je  
mašina za entanglement

Zeilinger et al, 2004

# Svrha i ciljevi projekta

Svrha projekta su fundamentalna istraživanja u području kvantne komunikacije i kvantne informatike:

3. Kvantna kriptografija – cilj je izgraditi uređaj i unaprijediti postojeće razumijevanje, domet i brzinu generiranja tajnog ključa
4. Unaprijeđenje protokola za kvantnu kriptografiju
5. Exp. i theor. istraživanje novih primitiva poput kvantnog potpisa, kvantnih memorija, kvantnih logičkih vrata
6. Novi načini za postizanje efikasnog entanglementa, multiparticle entanglement
7. Kvantni generatori slučajnih brojeva
8. Čvrstostanljivi (silicijski) detektora fotona (SPAD) i razvoj novih sklopova za aktivni quenching
9. Tehnike mjerenja apsolutne kvantne efikasnosti (SPAD)
10. Single photon gun
11. Ostvarenje kvantne teleportacije

# Ljudi na projektu

Projekt se oslanja na 3 iskusna istraživača s Horvatovca:

3. Branka Medved, dr. sc. IRB, Zavod za elektroniku
4. Hrvoje Skenderović, dr. sc., IFS
5. Mladen Pavičić, dr. sc. prof., PMF, Gradjevinski faks
6. Mario Stipčević, dr. sc, IRB, Zavod za eksperimentalnu fiziku

Stanje:

Jedan student radi diplomski rad iz područja

U kontaktu s dvoje završenih studenata

**Namjera:**

Tražili bi jednog doktoranda (novak, s faksa na posao, Bolonja ...)

# Metode

Tri su bitne sastavnice kvantne optike:

- Izvori svjetla (CW **laseri** (pulsni ?), laserske diode, LED)
- Klasične **optičke komponente** (dvolomci, polarizatori, filteri, lambda pločice, leće, fiber optic tehnologija)
- **Detektori** pojedinačnih fotona (Si APD, PM cijevi)

Kompjuterizirani eksperimenti, kompjuterski upravljiva mjerna tehnika, razvoj specifičnog elektroničkog sklopovlja vlastit ili u suradnji s malim tvrtkama

# Prostor i postojeća oprema

- Imamo dva laboratorijska prostora na Institutu Ruđer Bošković
- Dodatni prostor u i izvan IRB podložen dogovoru
- Opremljeni elektronički lab: NIM elektronička mjerna tehnologija (programabilni) generatori impulsa, timeri, digitalni osciloskop, izvori visokog i niskog napona, strujni izvor, AVO mjerna oprema, elektroničke komponente
- Ad-hoc mramorni optički stolovi 50x200cm + NdYAg laser 10mW
- Fotonski detektori (uglavnom PM i samogradnja SiAPD)
- Nešto malo optičkih komponenti za pod zub (tu smo tanki !)

# Potrebna oprema

Opis	Kom	Cijena
Single photon counters 400-1100nm SPCM-AQR16	4	190.000
Electrooptical modulator + Video Amplifier 95.000		2
BBO kristali za entanglement	3	23.000
Optika: filteri, prizme, sitni pribor, breadboard 160.000		-
High Voltage napajanje $\pm$ 0-2.500 V, 10mA 28.000		1
Fotodiode	11	12.000
Ostalo		134.000
	TOTAL brutto:	602.000

Uz poneku zaboravljenu sitnicu **cca 600.000 kn bto** u 5 godina.

# Moguća kapitalna oprema

Spektrometar (600-1000nm, rezolucija 1-2nm)  
(Ne treba, imaju na IFS-u, Slobodan Milošević)

# Moguća primjena istraživanja

Spektar primjena je vrlo širok, a primjena slijedi vrlo izravno iz samih eksperimenata:

- Kriptografija i informatička sigurnost (e-plaćanje, e-država, tajne službe, banke, korporacije....)
- APD tehnologija: spektrofotometrija, brzo sekvenciranje DNA, fundamentalna istraživanja u fizici.
- Razvoj APD je još vrlo intenzivan. Npr. HAMAMATSU još uvijek službeno ne proizvodi (ali istražuje !) SPAD diode => šansa za suradnju s tvrtkama koje razvijaju APD (Švic)
- Kvantna računala kao slijedeća generacija superračunala