DETEKCIJA KVANTNE UVEZANOSTI KORIŠĆENJEM POVM MERENJA SA PRIMENOM U KOMUNIKACIONIM PROTOKOLIMA

Vuk Vuković, 4. razred Matematičke gimnazije u Beogradu
Mia Mijović, 3. razred Matematičke gimnazije u Beogradu

Mentori:
Aleksandra Dimić, PhD student i istraživač, Fizički fakultet u Beogradu
Aleksandar Bukva, Dipl fizičar, Fizički fakultet u Beogradu

UVOD

Cilj ovog projekta je ispitivanje disperzija određenih kvantnih merenja radi brže detekcije uvezanosti u sistemu, kao i korišćenje dobijenih rezultata za razvijanje modela komunikacionog protokola.

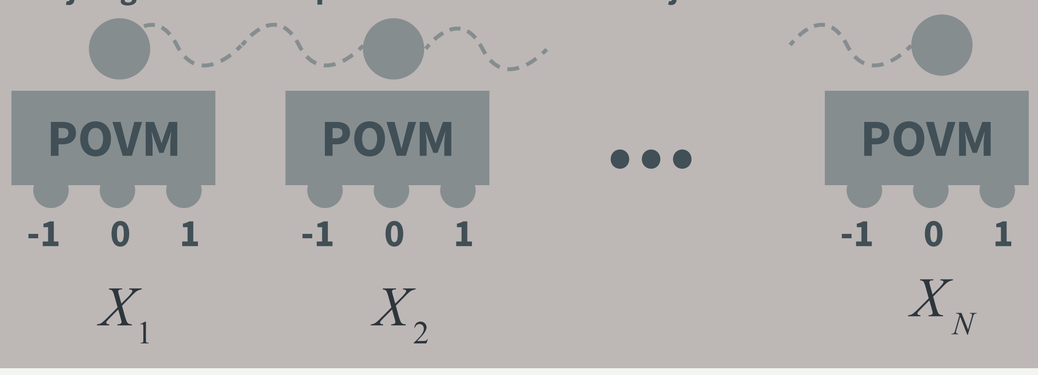
- **Osnovna jedinica kvantne informacije je qubit. Za razliku od "klasičnih" računara koji su zasnovani na binarnim brojevima koji mogu biti ili u stanju 0 ili u stanju 1, kvantni računari koriste qubite, tj. kvantne sisteme čestica sa dva moguća stanja koji su u superpoziciji.**
- **Kvantno-mehanička uvezanost (engl. *quantum entanglement*) je fizička pojava koja se javlja između više čestica, pri kojoj se stanja pojedinačnih čestica ne mogu opisati nezavisno od ostalih, već se mora opisati sistem kao celina.**
- **Korišćena su POVM merenja (engl. *positive-operator valued measure*), najopštija vrsta merenja u kvantnoj mehanici. Za razliku od projektivnih, ova vrsta merenja ne narušava uvezanost u potpunosti, već je donekle umanjuje. Korišćeni POVM merni instrument ima 3 moguće vrednosti izlaza i broj ovakvih elemenata jednak je broju qubita koji sačinjavaju posmatrano stanje.**

METOD

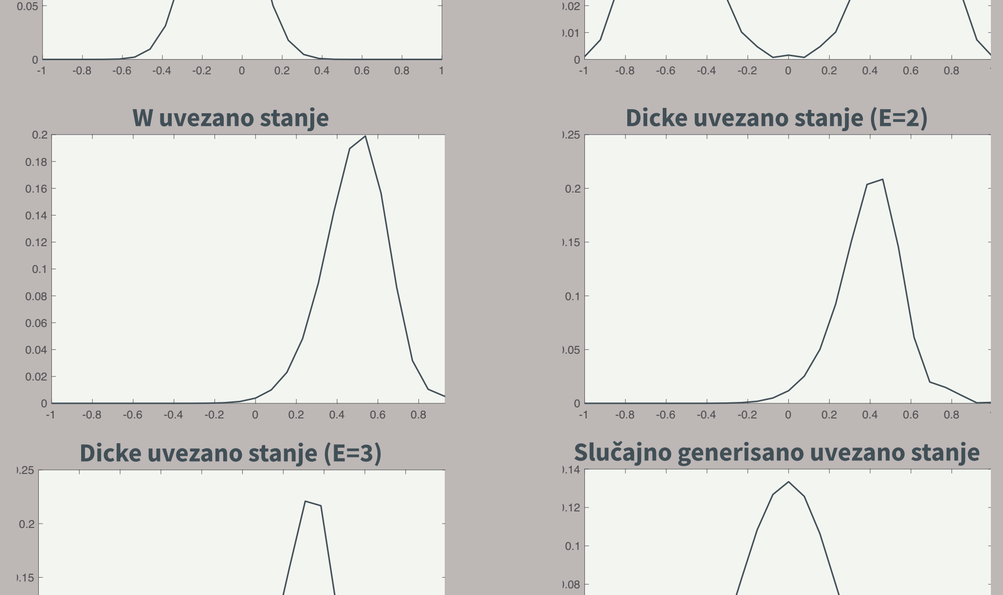
Raspodela koju smo posmatrali je:

$$X = \frac{X_1 + X_2 + \ldots + X_N}{N}$$

***N* predstavlja broj qubita, a X_i vrednost merenja na *i*-tom qubit-u (0, 1 ili -1). Simulacijom je određena pomenuta raspodela za poznata uvezana stanja kao i slučajno generisana separabilnia i uvezana stanja.**

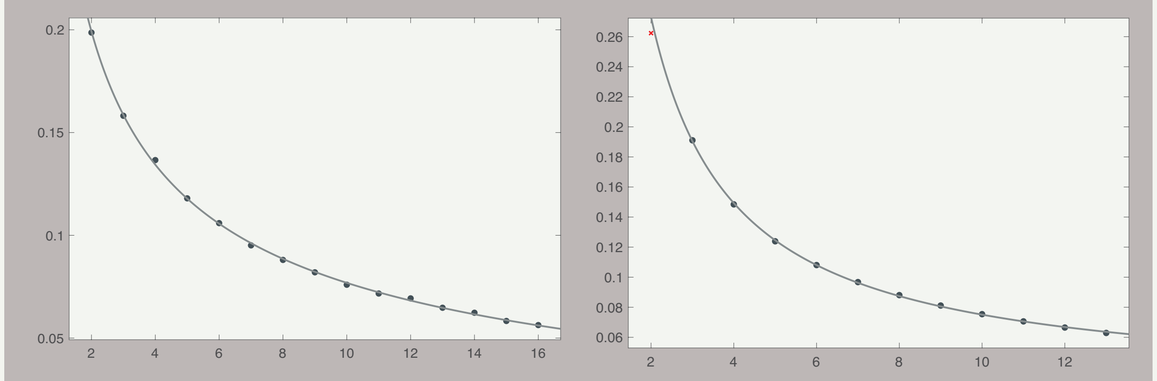


REZULTATI



***X* osa - Vrednost ishoda merenja, *Y* osa - Verovatnoća ishoda merenja**

REZULTATI



$$\frac{A}{\sqrt{N}} + B$$

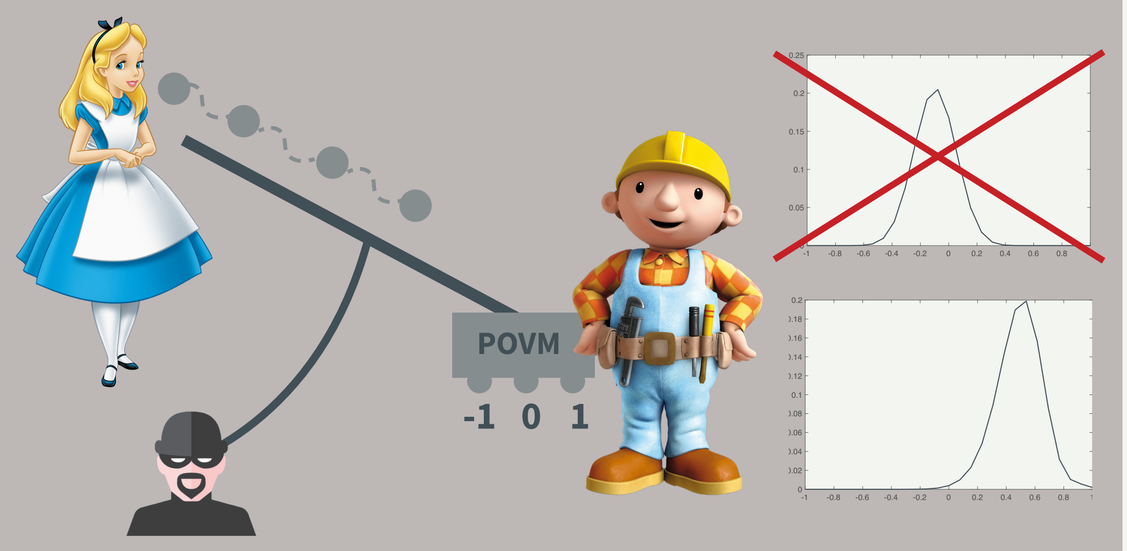
Separabilna stanja

$$\frac{A}{N} + B$$

Uvezana stanja

PROTOKOL

Ideja je da Alice i Bob koji žele da prenesu kvantni ključ, a kasnije i komuniciraju, provere da li Alice stvarno komunicira sa Bobom i da li postoji prisluškivač u kanalu, Eva, slanjem određenih kvantnih stanja. Nakon provere, Alice i Bob mogu koristiti neki od poznatih kvantnih protokola za prenos ključa kao što su BB84 ili B92, a kasnije i bilo koji način komunikacije enkriptovan prenetim ključem.



1. Verifikacija jednim stanjem

Ideja je da Alice šalje Bobu W, GHZ ili Dicke uvezano stanje od N qubita na osnovu pređašnjeg dogovora i šifre. Nakon slanja određenog broja kopija ovih stanja (reda veličine nekoliko hiljada), Bob može odrediti raspodelu *X*. Na osnovu eksperimentalnih rezultata, odnosno srednjih vrednosti, disperzija, kao i koeficijenata *A* i *B* koje smo dobili, Bob može zaključiti da li se radi o poslatom stanju ili je treće lice između presrelo i izvršilo merenje.

2. Verifikacija serijama stanja

Ideja je da Alice šalje Bobu W, GHZ ili Dicke uvezana stanja od N_1, N_2, …, N_k qubita na osnovu pređašnjeg dogovora i šifre. Nakon slanja određenog broja kopija ovih stanja (reda veličine nekoliko hiljada), Bob može odrediti raspodelu *X* za svako N_i. Bob zatim određuje da li se rezultati skaliraju sa $A/\sqrt{N} + B$ ili sa $A/N + B$, na osnovu čega može odrediti da li se radi o uvezanom stanju i njegovoj vrsti, a samim tim i to da li je treće lice između preslelo i izvršilo merenje.

ZAKLJUČAK

Određene su srednje vrednosti merenja i disperzije na zadatoj POVM postavci za slučajno generisana separabilna, kao i za GHZ, W, Dicke i slučajno generisana uvezana stanja sa različitim brojem qubita (do 13). Na osnovu dobijenih rezultata zaključuje se da se disperzije separabilnih stanja skaliraju sa $A/\sqrt{N} + B$, dok se disperzije uvezanih stanja skaliraju sa $A/N + B$. Dobijeni zaključci se poklapaju sa referentnim radovima. Prethodno pomenuti rezultati i zaključci iskorišćeni su za predlog implemetnacije verifikacionog protokola prilikom komunikacije.