Vuk Vuković i Mia Mijović

Detekcija kvantne uvezanosti korišćenjem POVM merenja sa primenom u komunikacionim protokolima

Cilj ovog projekta su ispitivanje raspodela POVM merenja radi brže detekcije uvezanosti u kvantnom sistemu, kao i moguće primene dobijenih rezultata za verifikacioni protokol u kvantnoj komunikaciji. Ispitivana su separabilna i uvezana stanja do 13 qubita. Simulacijom su određene raspodele separabilnih stanja, kao i raspodele pojedinih klasa uvezanih i slučajno generisanih uvezanih stanja. Dobijeni rezultati prikazuju specifične karakteristike pomenutih stanja što omogućava klasifikaciju nekih od njih. Takođe, u skladu sa teorijskim predviđanjima, zaključuje se da se disperzije separabilnih stanja skaliraju sa recipročnom vrednošću kvadratnog korena broja qubita u posmatranom sistemu. Sa druge strane, disperzije uvezanih stanja se skaliraju sa recipročnom vrednošću broja qubita koji čine posmatrani sistem. Potencijalna primena podrazumeva korišćenje uvezanih stanja, zajedno sa dobijenim rezultatima, za izradu protokola za prenos verifikacionog ključa prilikom komunikacije. Osmišljen je princip rada protokola, kao i jedna od mogućih implementacija u budućnosti. Primalac verifikacionog ključa na osnovu rezultata POVM merenja zaključuje u određenom pragu pouzdanosti da li postoji treće lice koje prisluškuje komunikaciju. Prednost ovog metoda jeste verifikacija sigurnosti iz malog broja kopija stanja i sistema srednje veličine.

Uvod

Razvojem kvantne mehanike dolazi i do razvoja kvantnog računarstva. Kvantno računarstvo je oblast koja izučava računarske sisteme koji direktno korsite kvantno-mehaničke fenomene. Najčešće korišćeni fenomeni su superpozicija i (kvantna) uvezanost (engl. entanglement).

Qubit. 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. Primer su polarizacija fotona ili spin elektrona.

Qubit se može predstaviti kao superpozicija dva stanja – $|0\rangle$ i $|1\rangle$

$$|\psi\rangle = a|0\rangle + b|1\rangle$$

gde a i b predstavljaju amplitude verovatnoća nalaženja qubita u stanjima $|0\rangle$ ili $|1\rangle$.

Na sličan način možemo posmatrati i sistem više qubita. Sledeći primer prikazuje dva qubita:

$$|\psi\rangle = a|00\rangle + b|01\rangle + c|10\rangle + d|00\rangle$$

Broj mogućih stanja (bazisnih vektora) u sistemima više qubita je 2^N, ukoliko je broj qubita u sistemu jednak N.

Kvantna uvezanost. Kvantna uvezanost (engl. entanglement) je pojava u kojoj čestice interaguju tako da se stanja pojedinačnih čestica ne mogu opisati nezavisno od ostalih, već se mora opisati stanje čitavog sistema. Na primeru

Vuk Vuković (1998), Beograd, Trajka Stamenkovića 1, učenik 4. razreda Matematičke gimnazije u Beogradu

Mia Mijović (1999), Beograd, Mileve Marić Ajnštajn 44, učenica 3. razreda Matematičke gimnazije u Beogradu

MENTORI:

Aleksandra Dimić, Fizički fakultet Univerziteta u Beogradu

Aleksandar Bukva, Fizički fakultet Univerziteta u Beograd

dva elektrona sa suprotnim spinovima, svaki od elektrona se opisuje kao superpozicija spinova ↑ i ↓. Ono što je zanimljivo jeste da kada izmerimo spin jednog elektrona, jednoznačno je određen i spin drugog, ma koliko on bio udaljen. To je potvrđeno Bell-ovim eksperimentom.

Matematički, uvezana stanja su ona stanja koja se ne mogu predstaviti kao tenzorski proizvod stanja pojedinačnih qubita. Stanja koja nisu uvezana nazivaju se separabilna stanja i mogu se predstaviti kao tenzorski proizvod pojedinačnih qubita.

Uvezanost se primenjuje u različitim oblastima kvantne informacije, od kvantnog novca (engl. quantum money) do konstruisanja komunikacionih protokola.

Poznata uvezana stanja. Najkorišćenija i najpoznatija uvezana stanja su GHZ (Greenberger *et al*. 2007), W uvezana stanja (Dür *et al*. 2000) i Dicke uvezana stanja (Toth 2005).

$$|\mathrm{GHZ}\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle^{\otimes N} + |1\rangle^{\otimes N}\right)$$

$$|\mathrm{W}\rangle = \frac{1}{\sqrt{N}}\left(|100\ldots0\rangle + |010\ldots0\rangle + \ldots + |00\ldots01\rangle\right)$$

$$|\mathrm{Dicke}\rangle = \frac{1}{\sqrt{\binom{N}{E}}}\sum_{j=1}^{\binom{N}{E}} \mathrm{perm}_j\left(|0\rangle^{\otimes (N-E)} \otimes |1\rangle^{\otimes E}\right)$$

(*N* predstavlja broj qubita, a *E* broj ekscitacija, tj. broj jedinica u qubitu)

Radi lakšeg razumevanja Dicke sranja, primer za $N = 4$, $E = 2$:

$$|\mathrm{Dicke}\rangle = \frac{1}{\sqrt{6}}\left(|0011\rangle + |0101\rangle + |1001\rangle + |0110\rangle + \right.$$
$$\left. + |1010\rangle + |1100\rangle\right)$$

Kvantna merenja. U kvantnoj mehanici merenja menjaju stanje sistema.

Najpoznatija vrsta merenja su projektivna merenja koja projektuju stanje na jednu od ortogonalnih osa sistema sa određenim verovatnoćama (Nielsen i Chuang 2010). Nakon projektivnog merenja, stanje postaje usmereno duž merene ose. Samim tim gubi se uvezanost u sistemu i stanje postaje separabilno.

POVM (engl. positive-operator valued measure) je najopštija vrsta merenja u kvantnoj mehanici. Matematički, POVM je skup operatora u Hilbertovom prostoru kvantnog sistema koji se sumiraju u jediničnu matricu (Nielsen i Chuang 2010). Verovatnoća nalaženja datog sistema u određenom stanju jeste očekivana vrednost merenja tog sistema na POVM elementu.

Razlika projektivnih i POVM merenja dobro se oslikava sledećim primerom. Dva ortogonalno polarizovana fotona mogu se razlikovati jednim projektivnim mernjem. Međutim, ukoliko se radi o neortogonalno polarizovanim fotonima, jedno projektivno merenje nam ne može dati korisne informacije. Sa druge strane, jednim POVM merenjem je moguće razlikovati fotone u ovom slučaju.

Fizička implementacija. Postoje razne implementacije prethodno pomenutih pojmova. Qubiti se najčešće implementiraju pomoću elektrona različitih spinova ili fotona različito orijentisanih polarizacija. Projektivna merenja u slučaju fotona mogu biti polarizatori i detektori. Implementacija POVM merenja je dosta zahtevnija. Jedna od mogućih implementacija pomoću optičkih instrumenata za merenja na fotonima detaljnije je opisana u referentnom radu (Brandt 2003).

Primena uvezanih stanja u protokolima za komunikaciju se još uvek pretežno teorijski razmatra. Verifikacioni protokol predstavlja verifikaciju sigurnosti kanala kojim dve strane komuniciraju, odnosno dobijanje informacije ima li presretača (špijuna) na datom kanalu. U teorijskom modelu koji smo predložili za protokol se koriste uvezana stanja i POVM merenja.

Metod

POVM merenje korišćeno u ovom radu jeste merenje „na jednakostraničnom trouglu" (Dimić i Dakić 2016). Ovo merenje ima tri moguća ishoda: –1, 0 i 1. Moguće je korišćenje i bilo kog drugog seta POVM merenja kako bi se dobio isti ishod. Ovaj set je izabran jer se često koristi i jednostavno se predstavlja. POVM merenje se matrično dobija na sledeći način:

$$E_i = \frac{1}{3}(1 + \vec{m}_i \cdot \vec{\sigma})$$

$$m_0 = (1, 0, 0)^{\mathrm{T}}$$

$$m_{\pm 1} = \left(-\frac{1}{2}, 0, \pm\frac{\sqrt{3}}{2}\right)^{\mathrm{T}}$$

$\sigma = \{\sigma_x, \sigma_y, \sigma_z\}$, gde su σ_x, σ_y i σ_z Paulijeve matrice.

Samim tim, matrice E_i imaju sledeći oblik:

$$E_{-1} = \frac{1}{3}\begin{bmatrix} 1-\frac{\sqrt{3}}{2} & -\frac{1}{2} \\ -\frac{1}{2} & 1+\frac{\sqrt{3}}{2} \end{bmatrix}$$

$$E_0 = \frac{1}{3}\begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix}$$

$$E_1 = \frac{1}{3}\begin{bmatrix} 1+\frac{\sqrt{3}}{2} & -\frac{1}{2} \\ -\frac{1}{2} & 1-\frac{\sqrt{3}}{2} \end{bmatrix}$$

Raspodela koju smo posmatrali je:

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

gde N predstavlja broj qubita, a X_i vrednost merenja na i-tom qubitu (0, 1 ili –1).

Posmatrali smo verovatnoće da je zbir rezultata merenja sistema sa N qubita jednak K:

$$\langle \psi | E_{k_1} \otimes E_{k_2} \otimes \ldots \otimes E_{k_n} | \psi \rangle$$
$$k_1, k_2, \ldots, k_N \in \{-1, 0, 1\}$$
$$k_1 + k_2 + \ldots + k_N = K$$

gde ψ predstavlja mereno stanje.

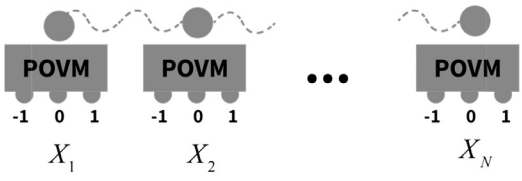
Na primer, za stanje od 4 qubita, izraz

$$\langle \psi | E_1 \otimes E_0 \otimes E_1 \otimes E_{-1} | \psi \rangle$$

bi predstavljao verovatnoću da qubiti redom daju rezultate 1, 0, 1, –1 na POVM uređaju (slika 1).

Takođe, posmatrano je kako disperzija gustine raspodele X zavisi od uvezanosti i broja qubita u stanju.

Merenja su vršena na poznatim uvezanim stanjima GHZ, W i Dicke, kao i na slučano generisanim uvezanim i separabilnim stanjima.



Slika 1. Šematski prikaz POVM merenja

Figure 1. Schematic view of POVM measurement

Separabilna stanja od N qubita smo generisali kao tenzorski proizvod slučajno generisanih qubita.

$$|\psi\rangle = |\psi_1\rangle \otimes |\psi_2\rangle \otimes \ldots \otimes |\psi_N\rangle$$
$$|\psi_i\rangle = a_i|0\rangle + b_i|0\rangle$$

gde a_i i b_i predtsavljaju slučajno generisane realne brojeve takve da je $a_i^2 + b_i^2 = 1$.

Pri slučajnom generisanju uvezanih stanja, verovatnoća da 2^N koeficijenata bude u takvom odnosu da stanje bude separabilno ravna je nuli. Zbog toga su uvezana stanja generisana kao 2^N realnih brojeva čiji se kvadrati sumiraju u 1.

Rezultati i diskusija

Simulacijom su dobijene raspodele X za sledeća stanja:

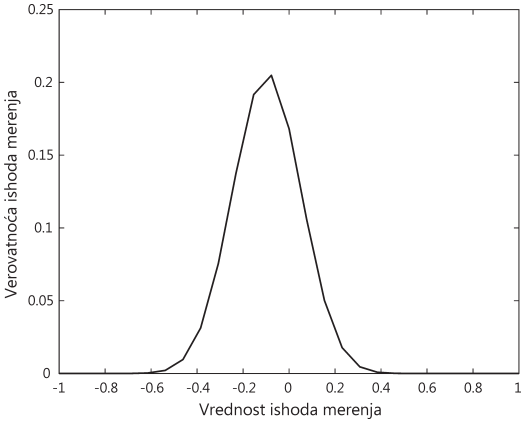
1. Slučajno generisana uvezana stanja od 2 do 16 qubita
2. GHZ uvezana stanja od 2 do 13 qubita
3. W uvezana stanja od 2 do 13 qubita
4. Dicke uvezana stanja (2 ekscitacije) od 3 do 13 qubita
5. Dicke uvezana stanja (3 ekscijacije) od 4 do 13 qubita
6. Slučajno generisana uvezana stanja od 3 do 13 qubita

Prilikom posmatranja zavisnosti disperzija od broja qubita, eksperimentalne tačke za mali broj qubita su izostavljane s obzirom da se karakteristike stanja ispoljavaju tek pri većem broju qubita, pa samim tim nema smisla posmatrati njihove disperzije.

Separabilna stanja (slika 2). Očekivana vrednost merenja nije 0 što se objašnjava konfiguracijom POVM elemenata. Takođe, ovaj grafik oslikava i centralnu graničnu teoremu na osnovu koje zbir nezavisnih slučajnih promenljivih teži normalnoj raspodeli (Dimić i Dakić 2016). Pri povećanju broja qubita raspodela bi sve više težila normalnoj.

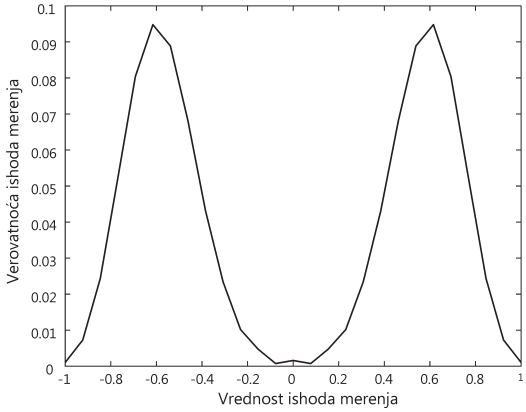
Disperzije raspodele X (slika 3) se skaliraju sa $\frac{A}{\sqrt{N}} + B$ ($A = 0.3129$, $B = -0.02207$).

GHZ uvezana stanja. Samo dva izraza $(|0\rangle^{\otimes N} + |1\rangle^{\otimes N})$ koji se nalaze u zapisu GHZ stanja se na grafiku oslikavaju izraženim pikovima sa leve i desne strane. Takođe, zbog simetričnosti



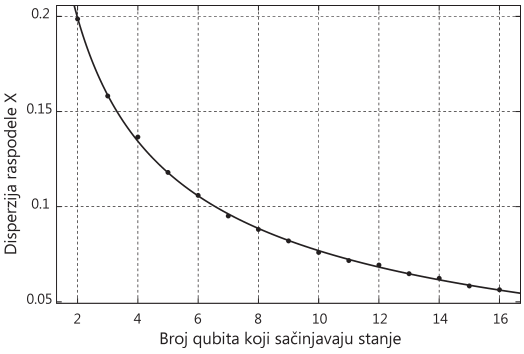
Slika 2. Raspodela X za slučajno generisano stanje od 16 qubita

Figure 2. Distribution X for randomly generated state of 16 qubits



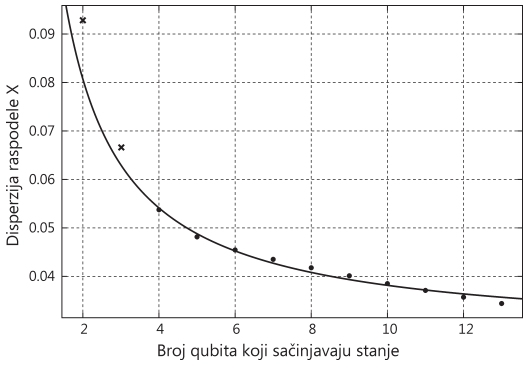
Slika 4. Raspodela X za GHZ uvezano stanje od 13 qubita

Figure 4. Distribution X for GHZ entangled state of 13 qubits



Slika 3. Zavisnost disperzije raspodele X od broja qubita u slučajno generisanom separabilnom stanju

Figure 3. Dispersion of X vs number of qubits in randomly generated separable state



Slika 5. Zavisnost disperzije raspodele X od broja qubita u GHZ stanju

Figure 5. Dispersion of X vs number of qubits in GHZ state

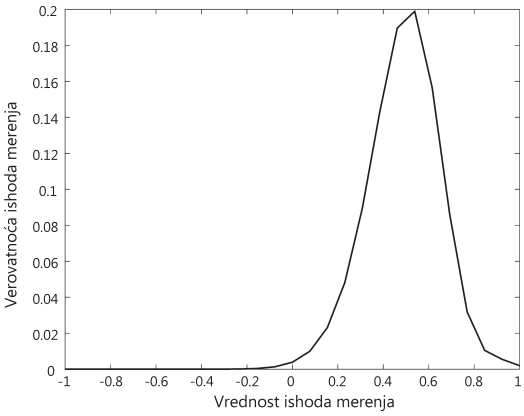
stanja je i njegova gustina raspodele simetrična u odnosu na nulu (slika 4).

Disperzije raspodele X (slika 5) se skaliraju sa $\frac{A}{N}+B$ ($A = 0.1064$, $B = 0.02751$).

W uvezana stanja (slika 6). Disperzije raspodele X se skaliraju sa $\frac{A}{N}+B$ ($A = 0.4754$, $B = 0.02822$, slika 7).

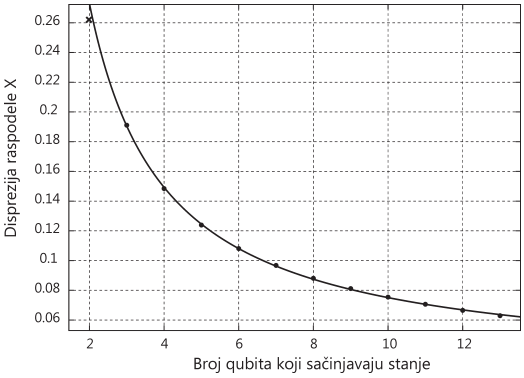
Dicke uvezana stanja (slike 8 i 9). Na grafiku 8a prikazana raspodela X za Dicke stanje od 13 qubita sa dve ekscitacije, a na grafiku 8b sa tri ekscitacije. Raspodele za Dicke stanja od 8 qubita sa tri, pet i četiri ekscitacije prikazani su na graficima 9a, 9b i 9c respektivno.

Primećeno je da se izgled raspodele X za Dicke stanje menja u zavisnosti od broja ekscitacija (E) u stanju od N qubita na sledeći način:



Slika 6. Raspodela X za W stanje od 13 qubita

Figure 6. Distribution X for W state of 13 qubits

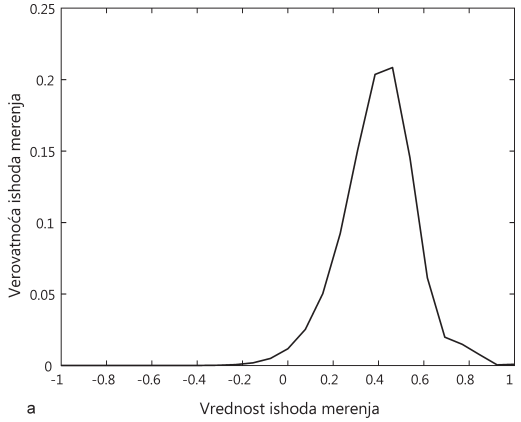


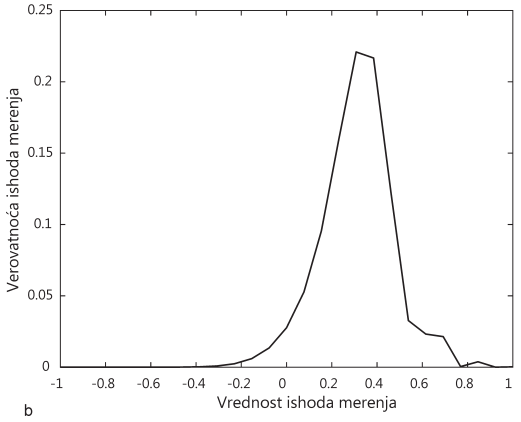
Slika 7. Zavisnost disperzije raspodele X od broja qubita u W stanju

Figure 7. Dispersion of X vs number of qubits in W state

– $E < N/2$, na grafiku se dobija dodatni pik sa desne strane (slika 9a)
– $E > N/2$, na grafiku se dobija dodatni pik sa leve strane (slika 9b)
– $E = N/2$, na grafiku se dobija izraženi centralni pik i raspodela koja je simetrična (slika 9c)

Zavisnost disperzije raspodele X od broja qubita u Dicke stanju sa dve ekscitacije i tri ekscitacije data je na graficima 10 i 10b respektivno.





Slika 8. Raspodela X za Dicke stanje od 13 qubita sa 2 ekscitacije (a) i 3 ekscitacije (b)

Figure 8. Distribution X for Dicke state of 13 qubits with 2 excitations (a), and with 3 excitations (b)

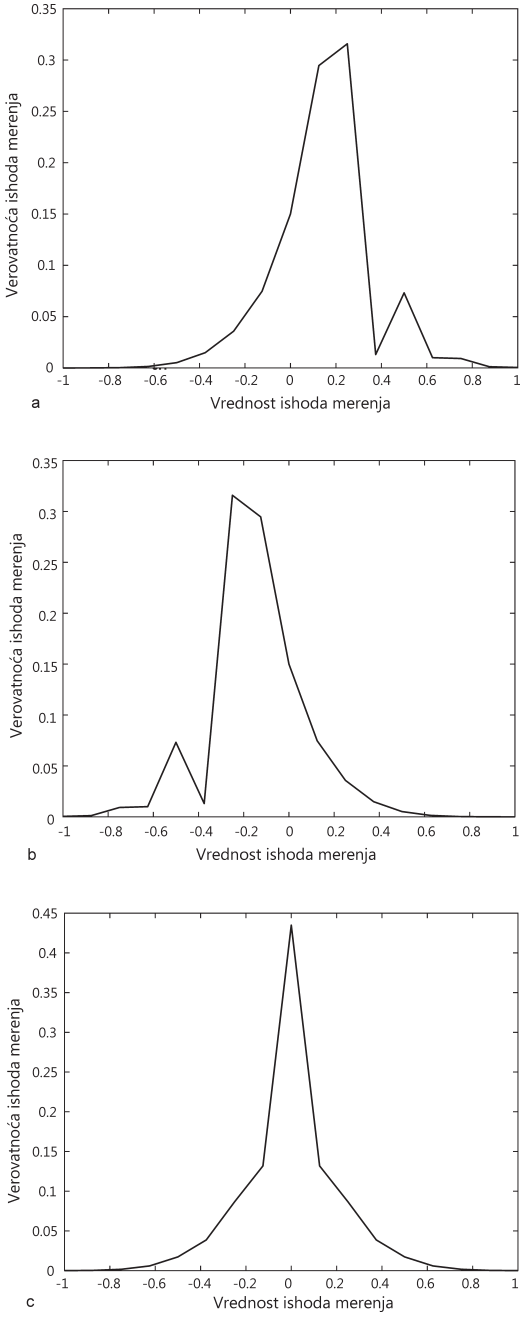
Disperzije raspodele X se skalirju sa

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

($A = 0.6204$, $B = 0.01624$ za dve ekscitacije i $A = 0.7274$, $B = 0.009791$ za tri ekscitacije).

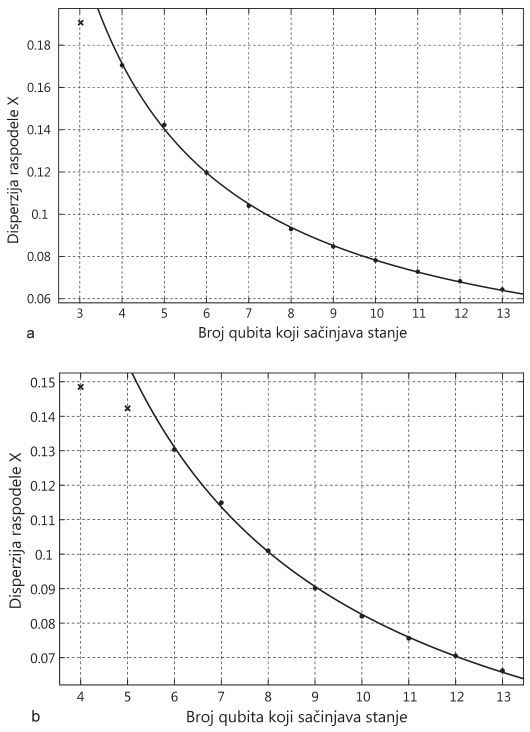
Slučajno generisana uvezana stanja. Raspodela X za slučajno generisano uvezano stanje od 13 qubita data je na slici 11. Zavisnost disperzije raspodele X od broja qubita u slučajno generisanom uvezanom stanju data je na slici 12.

Disperzije raspodele X se skalirju sa $\frac{A}{N} + B$ ($A = 0.3182$, $B = 0.02357$).



Slika 9. Raspodela X za Dicke stanje od 8 qubita sa 3 ekscitacije (a), 5 ekscitacija (b) i 4 ekscitacije (c)

Figure 9. Distribution X for Dicke state of 8 qubits with 3 excitations (a), 5 excitations (b), and 4 excitations (c).

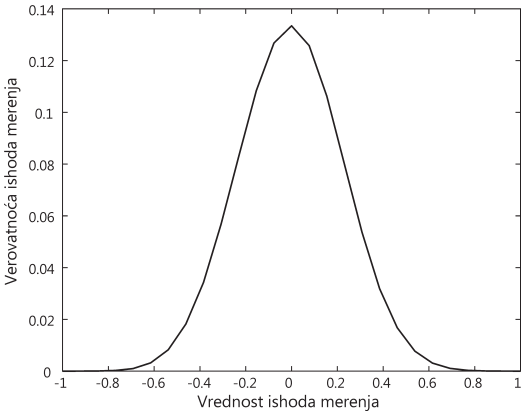


Slika 10. Zavisnost disperzije raspodele X od broja qubita u Dicke stanju sa dve ekscitacije (a) i tri ekscitacije (b)

Figure 10. Dispersion of X vs number of qubits in Dicke state with 2 excitations (a), and with 3 excitations (b)

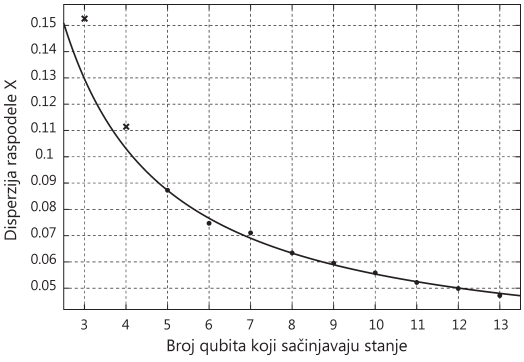
Generalno, zaključujemo da ukoliko se posmatra disperzija raspodele X, za separabilna stanja ona će se skalirati sa $\frac{1}{\sqrt{N}}$, dok će za uvezana stanja to biti izraz $\frac{1}{N}$.

Primena u komunikacionim protokolima. 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.



Slika 11. Raspodela X za slučajno generisano uvezano stanje od 13 qubita

Figure 11. Distribution X for randomly generated entangled state of 13 qubits



Slika 12. Zavisnost disperzije raspodele X od broja qubita u slučajno generisanom uvezanom stanju

Figure 12. Dispersion of X vs number of qubits in randomly generated entangled state

Bitno je napomenuti da su sve predstavljene metode hipotetičke jer još uvek ne postoji način za fizičku implementaciju zadatih stanja sa proizvoljnim brojem qubita. Trenutno je moguće implementirati W stanja do 11 qubita, dok se radi na implementaciji GHZ stanja od 6 qubita na Institutu za kvantnu optiku i kvantnu informatiku u Beču. Takođe, fizikčka implementacija podrazumevala bi optičku realizaciju qubita u vidu fotona sa primenom lasera, s obzirom da su sve ostale varijante kratkog životnog veka i nepogodne za prenos (McCutcheon *et al*. 2016).

Pretpostavimo da Alice i Bob imaju prethodni dogovor oko stanja koje će biti poslato, kao i broj qubita koje će stanje sadržati. Primer prethodnog dogovora mogao bi da podrazumeva da se na osnovu trenutnog datuma i vremena, šife, određenih matematičkih operacija (modulo), kao i heš-funkcije odredi stanje koje će biti poslato. Na osnovu toga, nakon što Alice bilo kojim kanalom komunikacije Bobu dostavi potrebne informacije, on zaključuje koja stanja je potrebno da prima.

Predstavljamo dva načina za verifikaciju sigurnosti kvantnog kanala (slika 13):

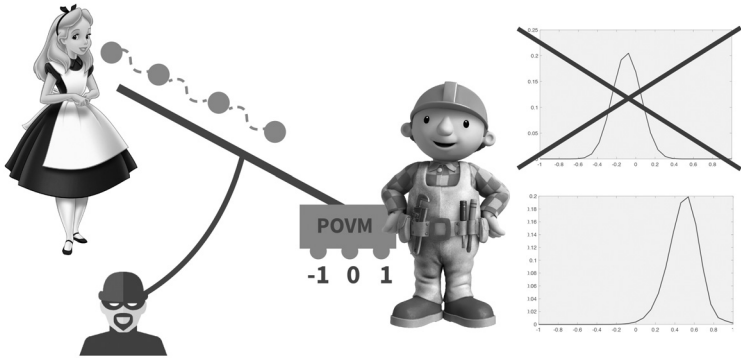
1. Verifikacija jednim stanjem

Ideja je da Alice šalje Bobu W, GHZ ili Dicke uvezano stanje od N qubita na osnovu prethodnog 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, izvršilo merenje, a samim tim i narušilo uvezanost u sistemu.

2. Verifikacija serijama stanja

Ideja je da Alice šalje Bobu W, GHZ ili Dicke uvezana stanja od $N_1, N_2, \ldots, N_k$ qubita na osnovu prethodnog 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 $\frac{A}{\sqrt{N}} + B$ ili sa $\frac{A}{N} + B$, 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.

Na osnovu No-cloning teoreme, imamo garanciju da Eva ne može kopirati stanje pre merenja, a zatim ga proslediti. Jedini način da Eva prevari Alisu i Boba jeste da odredi o kom stanju je reč, a zatim stvara takva stanja. Međutim, kako bi to učinila, Eva mora vršiti pravu vrstu merenja (projektivna, POVM) i imati istu POVM postavku kao i Bob. Ukoliko Eva izvrši projektivno merenje, Bob bi dobio separabilno stanje. Sa druge strane, POVM merenja će dovesti do promene stanja pri kojima može ostati uvezanost.



Slika 13. Uprošćeni prikaz verifikacije kvantnog kanala

Figure 13. Simplified representation of quantum channel verification

Međutim, kako se radi o potpuno drugom stanju, Bob će detektovati izvršeno merenje na osnovu drugačije srednje vrednosti i disperzije. S obzirom da bi red veličine trajanja prenosa svih 10 000 stanja iznosio 1 sekund, ne postoji mogućnost da Eva za to vreme odredi stanje o kom je reč, spremi aparaturu, a zatim i proizvede ta stanja: Bob će primetiti kašnjenje.

Bitno je napomenuti da se prilikom upoređivanja izmerenih vrednosti sa eksperimentalnim rezultatima mora dozvoliti određeni prag greške pre svega zbog šuma koji postoji u kanalu. Nažalost, u ovom radu nije određen optimalan prag greške koji je potrebno koristiti. Međutim, izvršena je mala simulacija koja oslikava pouzdanost prepoznavanja stanja na osnovu eksperimentalnih rezultata (koeficijenta A i B, kao i disperzija). Pošto se stanje nakon POVM merenja ne može odrediti, i može postojati beskonačno mogućnosti za dobijena stanja, možemo pretpostaviti da je stanje koje Eva prosleđuje nakon merenja slučano generisano uvezano stanje. Za $N = 4$ dobijena je pozdanost prepoznavnja od 83%, od čega je u 85% slučajeva pogrešne klasifikacije slučajno generisano uvezano stanje pomešano sa GHZ stanjem. Ni jednom nije došlo do mešanja sa Dicke stanjem sa dve ekscitacije sa slučano generisanim stanjem iz čega možemo zaključiti da je za mali broj qubita najpouzdanije raditi sa Dicke stanjima. Za $N = 5$ dobijena je pouzdanost od 94%, od čega je u 100% slučajeva pogrešne klasifikacije slučajno generisano uvezano stanje pomešano sa GHZ stanjem. Za $N > 5$ klasifikacija je bila tačna u 100% slučajeva. Iz datih rezultata se može zaključiti da pouzdanost protokola raste sa porastom broja qubita koji predstavljaju verifikacioni ključ, kao i da je preporučljivo koristiti stanja sa brojem qubita većim od 5.

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 $\frac{A}{\sqrt{N}} + B$, dok se disperzije uvezanih stanja skaliraju sa $\frac{A}{N} + B$. Ovi zaključci su u skladu sa referentnim radovima (Dimić i Dakić 2016). Prethodno pomenuti rezultati i zaključci iskorišćeni su za predlog implementacije verifikacionog protokola prilikom komunikacije.

Literatura

Brandt H. E. 2003. Quantum measurement with a positive operator-valued measure. *Journal of Optics B: Quantum and Semiclassical Optics*, **5** (3): S266.

Dimić A., Dakić B. 2016. On the central limit theorem for unsharp quantum random variables. arXiv:1609.01680.

Dür W., Vidal G., Cirac J. I. 2000. Three qubits can be entangled in two inequivalent ways. arXiv:quant-ph/0005115.

Greenberger D. M., Horne M. A., Zeilinger A. 2007. Going beyond Bell's theorem. arXiv:0712.0921.

McCutcheon W., Pappa A., Bell B. A., McMillan A., Chailloux A., Lawson T., Rarity J. G. 2016. Experimental verification of multipartite entanglement in quantum networks. *Nature communications*, **7**: 13251.

Nielsen M. A., Chuang I. L. 2010. *Quantum Computation and Quantum Information*: 10th Anniversary Edition. Cambridge University Press

Toth G. 2005. Detection of multipartite entanglement in the vicinity of symmetric Dicke states. arXiv:quant-ph/0511237.

Vuk Vuković and Mia Mijović

Quantum Entanglement Detection Using POVM Measurements with the Application in Communication Protocols

The purpose of this project is the analysis of some POVM measurements' distributions in order to faster detect entanglement in a quantum system, as well as propose a model for verification in communication protocol based on the obtained results. Separable and entangled states with different number of qubits (up to 13) were examined. By performing a simulation, we determined measurements' distributions for randomly generated separable states, as well as for generally known and randomly generated entangled states. Based on the results, it can be concluded that the dispersions of separable and entangled states are differently proportional to the number of qubits that the system consists of. The potential application of the obtained results includes the use of entangled states as a verification key transfer protocol in communication. After performing POVM measurements and determining the dispersion, the receiver can probabilistically conclude whether there was a third-party present who was listening in the protocol. The advantage of this method is the verification of security based on a small number of quantum state copies, as well as a system of medium size.