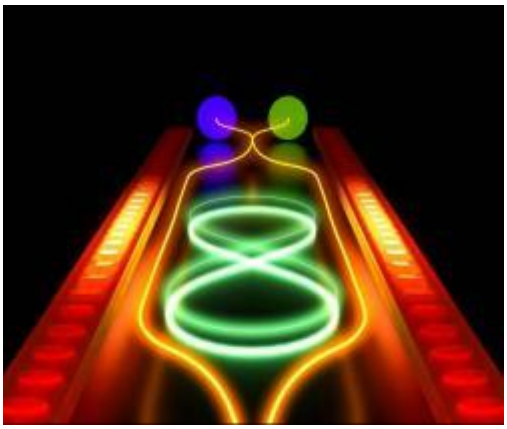
https://www.reflex.cz/clanek/kultura/86848/monstrum-jmenem-jakes-dokument-milda-ukazuje-ze-to-neni-jen-smesny-pan-a-ze-si-stale-musime-davat-pozor.html

http://www.osel.cz/9884-kvantova-mechanika-na-vlastni-oci-entanglement-objektu-o-sirce-vlasu.html

Kvantová mechanika na vlastní oči: Entanglement objektů o šířce vlasu! Šikovní nanoinženýři kvantově provázali mikrorezonátory, a také mikrobubny. V obou případech jde o objekty na hranici viditelnosti pouhým okem, které se skládají z mnoha miliard atomů.



Kvantově provázané mechanické mikrorezonátory. Kredit: Moritz Forsch. Kavli Institute of Nanoscience, Delft University of Technology.

Kdo slyšel o entanglementu, tak už nejspíš nikdy nebude úplně v klidu. Entanglement, čili kvantové provázání, je jedním z nejpodivnějších projevů kvantové mechaniky. Pokud jsou dva objekty kvantově provázané, tak jsou jejich stavy navzájem neoddělitelné. Když stav jednoho takového objektu změní, tak se změní i ten druhý. Jak praví kvantová mytologie, takové provázání trvá, i kdyby objekty dělily světelné roky.

Simon Gröblacher. Kredit: Delft University of Technology.

Vědci pozorují entanglement obvykle na elementárních částicích a podobných věcech nepatrných velikostí. Postupně se ale odvažují dál, směrem do makrosvěta. Britského fyzika Andrewa Armoura z Nottinghamské univerzity, a jistě i mnohé další, velmi dráždí otázka, kam až se s entanglementem asi můžeme dostat? U jak velkých objektů může ještě fungovat?

Příslušné odpovědi nás přivádějí k velmi zajímavým technologiím, jako jsou třeba ultrapřesná měření gravitace nebo nehacknutelný kvantový internet.

Albert Einstein entanglement zrovna dvakrát nemusel. Bylo to pro něj strašidlo, s nímž si není radno zahrávat. Během posledních desetiletí ale fyzici museli uznat, že tohle strašidlo skutečně existuje, a že působí minimálně na vzdálenost mezi Zemí a oběžnou dráhou. Entanglované částice bývají velmi malé, protože je snadnější chránit jejich křehké kvantové stavy před chaosem okolního světa. Teď se to ale mění.

Mika Sillanpää. Kredit: Aalto University.

Hned dva výzkumné týmy nedávno zapracovaly na tom, aby dostaly entanglement do makrosvěta. V obou případech museli badatelé experimenty zchladit na teplotu blízkou absolutní nule. Simon Gröblacher z nizozemské Technische Universiteit Delft a jeho spolupracovníci vykouzlili kvantové provázání křemíkových mikrorezonátorů (silicone beams) o velikosti bakterií na křemíkovém čipu. Povedlo se jim to sice jenom na zlomek sekundy, na publikaci v časopise Nature to ale stačilo. Jeden takový mikrorezonátor přitom obsahoval asi 8 miliard atomů.

Kvantově provázané mikrobubny na křemíkovém čipu. Kredit: Aalto University/Petja Hyttinen & Olli Hanhirova, ARKH Architects.

Finský fyzik Mika Sillanpää z univerzity Aalto-yliopisto s kolegy nato šli jinak. Použili miniaturní mechanické bubny z vibrující hliníkové membrány o šířce zhruba odpovídající hodně tenkému lidskému vlasu (15 mikrometrů). Na bubny působili mikrovlnami a sledovali kvantové stavy bubnů. Nakonec se jim povedlo prokázat kvantové provázání bubnů, které prý může trvat prakticky věčně, pokud budou mikrobubny skrápěné mikrovlnami. V prestižním Nature mají článek hned za Gröblacherovým týmem.

Kvantové provázání v makrosvětě by mohlo mít řadu možných aplikací. Gröblacherovy mikrorezonátory záměrně vibrují tak, aby byly kompatibilní s existujícími telekomunikačními systémy. Časem by se mohly stát základem uzlů kvantového internetu. Mikrobubny týmu, který vedl Sillanpää, jsou prý zase vhodné k přesným měřením. Mohly by z nich vzniknout kvantové senzory, které by byly skvělé na ultrapřesná měření chvění časoprostoru v souvislosti s detekcí gravitačních vln a v podobných aplikacích.

Podle Johna Teufela z institutu National Institute of Standards and Technology (NIST) v Boulderu, stát Colorado, mají oba experimenty svá pro a proti. Entanglement . Gröblacherových strun trval jenom velmi krátkou dobu, byl ale detekován s vysokou pravděpodobností. Sillanpääovy mikrobubny byly entanglovány na dobrou půlhodinu, ale prokazování úspěchu jim dalo hodně zabrat a vyžadovalo komplikované teoretické úvahy. Teufel naznačuje, že jen máloco bývá ideální. Je každopádně nadšený a zároveň zvědavý na další kroky v tomto směru. Kdo by nebyl?

Video: Mika Sillanpää: "The borderline between quantum physics and everyday world"

Literatura

Science News 25. 4. 2018, Nature 556: 473–477 a 478–482.

Autor: Stanislav Mihulka
Datum: 27.04.2018

Tisk článku

Související články:

Einsteinovo strašidelné působení ve kvantových sítích Autor: Stanislav Mihulka (24.01.2015)
Fyzici prověřili kvantový entanglement pomocí záře hvězd Autor: Stanislav Mihulka (07.02.2017)
Švýcarští vědci zvládli rekordní simulaci 45-qubitových kvantových výpočtů Autor: Stanislav Mihulka (06.07.2017)

Diskuze:

Z Z,2018-04-29 23:52:01

"hlavní výhoda nebo "killing feature" je, že výpočet je okamžitý tj. ve chvíli, kdy jsou nastaveny vstupní hodnoty máme výsledek."

Ale to bude asi platiť len pre jeden "takt" takéhoto počítača. Asi sa všetko nedá previesť na takéto "okamžité" vypočítanie výsledku. Niektoré výpočty sa vraj dajú vyrátať oveľa rýchlejšie, no nie okamžite, pretože je iná závislosť počtu iterácií ako pri "klasickom" počítači.

Odpovědět

matematický konstrukt

Pavel K2,2018-04-29 22:40:21

kvantové provázání je pouze matematický konstrukt, který složitě popisuje, že máte dvě "částice" (daleko od sebe) v přesně korelovaných stavech. Pokud roztočíte dva setrvačníky ve shodné ose (nebo protilehlé), zajistíte kompenzaci mechanických ztrát a vzdálíte je od sebe, dosáhnete téhož. V žádném případě se kouknutím na jeden z těchto setrvačníků nepřenese žádná informace na ten druhý :-)

Odpovědět

Re: matematický konstrukt

Z Z,2018-04-29 23:32:17

Obávam sa, že toto prirovnanie značne "kríva".
"Kouknutie" v kvantovej m. znamená zároveň aj ovplyvnenie stavu.
Pri zotrvačníku nespôsobí "kouknutie" to, že sa bude otáčať v náhodnom smere.
Vlastnosťou toho kvantového previazania je aj to, že veličina bude mať "jasnú" hodnotu až po meraní a nie vopred ešte pred meraním - ako pri zotrvačníkoch.
Je to popísané napríklad aj v http://www.osel.cz/5110-podivnosti-kvantoveho-sveta.html (Bellove nerovnosti).

Odpovědět

Re: matematický konstrukt

Pavel Brož,2018-04-30 00:06:09

Je vidět, že o kvantové teorie nevíte prakticky nic. Dva klasické setrvačníky lze popsat faktorizovaným stavem, kdy se prostě popíše každý setrvačník jedním stavem (například vektorem jeho impulsmomentu). Dvě entanglované částice faktorizovaným stavem popsat nelze - entanglované stavy jsou tak totiž definovány, tak např. dva entanglované elektrony s nulovým celkovým spinem jsou popsány stavovým vektorem:

(1/odm(2))*[|1/2> |-1/2> - |-1/2> |1/2>]

Rozdílů mezi dvěma roztočenými klasickými setrvačníky a dvěma entanglovanými elektrony je ale více. Tak např. u setrvačníku jakožto klasického systému je možné současně změřit všechny tři složky jeho impulsmomentu (tj. všechny průměty jeho vektoru impulsmomentu na všechny tři osy). U kvantového systému to není možné, protože průměty spinu elektronu na vzájemně kolmé osy jsou tzv. nekompatibilní pozorovatelné, kdy změřením průmětu do jedné osy učiníte výsledek měření průmětu do kolmé osy naprosto náhodným - jakmile je změřen např. průmět spinu do osy x, tak při následném měření průmětu spinu do osy y nebo z se získá se stejnou pravděpodobností výsledek -1/2 i 1/2, a to bez ohledu na počáteční stav elektronu před měřením průmětu spinu do osy x. Nic takového se u měření impulsmomentu klasického setrvačníku neděje.

Odpovědět

Re: Re: matematický konstrukt

Pavel Brož,2018-04-30 00:07:40

tato poznámka byla na pana Pavla K2.

Odpovědět

Kvantový internet

Václav Dvořák,2018-04-27 16:57:55

Znamenalo by to, že by bylo možné komunikovat mezi planetami, typicky na Mars bez zpoždění?

Odpovědět

Neznamenalo

Pavel Brož,2018-04-27 17:46:40

Při komunikaci s využitím kvantového provázání získá příjemce řetězec symbolů, který je sice korelovaný s řetězcem odesilatele, ale který je přesto sám o sobě náhodný. Aby se z tohoto řetězce dala demodulovat informace, potřebuje příjemce získat dodatečnou informaci o nastavování odesilovatelova zařízení, a tuto informaci nelze předat jinak, než klasickou cestou.

Přínos kvantové komunikace (ve smyslu komunikace s využitím entanglovaných stavů) není v dosažení nadsvětelné rychlosti komunikace, ale v její bezpečnosti. Při jakémkoliv pokusu o odposlech totiž dojde nevyhnutelně ke ztrátě korelace mezi kvantovými stavy odesilatele a příjemce, díky čemuž příjemce dostane po demodulaci opět jen náhodný řetězec symbolů - díky tomu pozná, že byl odposloucháván. Byla samozřejmě vymyšlena spousta protokolů, které umožňují v co nejefektivnější míře ochránit přenášenou informaci a co nejdříve odhalit případný odposlech, podstata se ale skrývá právě v té ztrátě korelace mezi kvantovými stavy odesilatele a příjemce při jakémkoliv pokusu o odposlech.

Odpovědět

Re: Neznamenalo

Jirka Niklík,2018-04-27 18:29:17

A je tam nutný ten entanglement? Snažil jsem se pochopit, jak funguje konkrétní zařízení (http://optics.org/news/1/7/21) a přišlo mi, že to funguje i bez toho bájného entanglementu. A navíc, že o kvantovosti mluví jen proto, že je to v módě. Prostě vysílají strašně slabý signál (ten se samozřejmě odposlouchává těžko) a použitý protokol umožňuje data z toho šumu zase vylovit. Většina článků o kvantové technice je stejně nekonkrétní, jako tenhle článek, takže zatím nevím, jestli se tomu dá vůbec věřit, nebo jestli je celý entanglement jen myšlenková konstrukce, kterou se ještě nepodařilo experimentálně dokázat, natož využít...?

Odpovědět

Re: Re: Neznamenalo

Pavel Brož,2018-04-27 22:14:10

Ten článek, který odkazujete, opravdu nic konkrétního neříká, z toho ale nemůžete dovozovat, že většina článků o kvantové technice je nekonkrétní. Existuje spousta seriózních zdrojů o kvantové optice, kde jsou referovány i přístroje konstruované na realizaci entanglovaných párů a jejich měření. V České Republice se tomuto tématu věnovala např. společná laboratoř optiky Univerzity Palackého a Fyzikálního ústavu Akademie věd ČR, zejména jméno prof. Jana Peřiny má ve světě obrovské renomé (mám jeho už letitější knížku Quantum Statistics of Linear and Nonlinear Optical Phenomena, kterou mohu vřele doporučit). Experimenty týkající se entanglementu můžete najít v přístupné formě např. v knížce Koncepční otázky kvantové teorie od Miloslava Duška, což je další z vynikajících českých specialistů na tento obor.

Každopádně entanglement není žádný podvod, je to seriózní fenomén studovaný už desítky let v mnoha špičkových optických laboratořích, a vlastnosti, které pro něj předpovídá kvantová teorie, byly už nesčíslněkrát ověřeny. V dnešní době není problém nejen pro špičkovou, ale i pro běžnou optickou laboratoř vytvořit jednotlivé entanglované páry fotonů přenášené na kilometrové vzdálenosti - toto už bylo možné realizovat před více než deseti lety. Většina dnes řešených problémů je technických - samozřejmě nestačí přenést jen jeden nebo několik párů fotonů, to stačí na demonstraci jevu, ale ne na reálné použití v praxi, kde vyžadujete aspoň stovky kilobitů za vteřinu. Potřebujete také spolehlivou funkčnost, pro úspěšné komerční využití si nevystačíte s tím, že statisticky dokážete, že vaše metoda funguje na hladině významnosti n-sigma - to sice stačí pro publikování ve vědeckém časopise, ale ne v byznysu. Nicméně překotný vývoj v tomto oboru (ve kterém bohužel Evropa prvenství dobrovolně přenechala Číně, která na rozdíl od ní rychle pochopila vojenskou i průmyslovou strategičnost tohoto výzkumu a patřičně ho subvencovala) nenechává nikoho na pochybách, že během deseti let bude kvantová kryptografie rutinně využívána ve velkých firmách typu banky atd., a během dalších deseti let i v těch menších.

Mimochodem, entanglement jako takový není ve skutečnosti vůbec nic vzácného. Entanglovaný stav systému definujeme jako stav, který nejde faktorizovat na direktní součin stavů jeho komponent. Z pohledu této definice jsou entanglovány např. i elektrony v molekule

vodíku, a obecně úplně každý vázaný stav je stavem entanglovaným. Jinými slovy, všechno, co kolem sebe momentálně vidíte, dokonce včetně Vás samotného, je tvořeno částicemi nacházejícími se v entanglovaném stavu. Takovýto entanglement akorát není využitelný pro tu kvantovou kryptografii (k ní potřebujete daleko od sebe oddělené a přitom stále entanglované částice), nicméně z hlediska definice je to také entanglement. To jen k Vaší úvaze, zda entanglement není jen nějaká myšlenková konstrukce, která se ve skutečnosti nerealizuje.

Odpovědět

Re: Re: Re: Neznamenalo

Milan Krnic,2018-04-27 22:25:21

Děkuji za Váš komentář. Já si počkám, co uchopitelného nakonec z těch statistických metod vyleze. Na pochybách jsem.

Odpovědět

Re: Neznamenalo

Václav Dvořák,2018-04-28 08:46:12

Viděl jsem před nějakým časem na TEDx prezentaci právě z Univerzity v Delft, kde ukazovali, že entanglované částice je možné obarvit a tím přenést dodatečnou informaci i bez potřeby mít k dispozici obě strany komunikace. Právě proto jsem se takhle ptal... Zkuste si to najít třeba někde na youtube. Co se týká ostatních tvrzení, tak 100% souhlas, to je známá (a v případě širšího nástupu kvantových počítačů nutná) věc.

Odpovědět

Re: Re: Neznamenalo

Pavel Brož,2018-04-28 12:04:29

To se mi nějak nezdá, "přenést dodatečnou informaci i bez potřeby mít k dispozici obě strany komunikace", tak to se přiznám, že naprosto netuším, co si pod tím představit. Hledal jsem na youtube i jinde ale nenašel jsem, máte prosím odkaz?

Odpovědět

Re: Re: Re: Neznamenalo

Václav Dvořák,2018-04-29 23:22:22

Našel jsem, je to už jedno ze starších videí - https://youtu.be/wZzHnZzm_58.

Odpovědět

Re: Re: Re: Re: Neznamenalo

Pavel Brož,2018-04-30 01:01:35

Ne, tak to na tom video nebyl přenos informace bez nutnosti mít k dispozici obě strany komunikace, to co tam bylo ukázáno, byl tzv. přenos entanglementu, který se používá v kvantové teleportaci. Ty barvy tam ve skutečnosti substituovaly libovolnou přenášenou kvantovou vlastnost, kterou může být třeba spin částice, ten se v těchto pokusech používá nejčastěji, protože se jeho měření nejlépe realizuje. Ani u přenosu entanglementu, ani u kvantové teleportace ale nejde přenést informaci rychleji než světlo - to, co se přenese, je entanglovaný stav, ze kterého lze následným měřením zrekonstruovat původní vzdálený stav. Tuto rekonstrukci lze ale provést až poté, co je na vzdálené místo klasickou cestou přenesena informace o tom, jakým způsobem byl původní stav provázán se stavem, který slouží pro přenos entanglementu. Tato informace bohužel v tom videu chybí.

Kvantová teleportace funguje tak, že máte stav, který chcete přenést. Na tom videu by to byla ta zelená kulička vlevo např. v čase 9:21. Tento stav provážete pomocí entanglovaného páru, tím entanglovaným párem je na tom videu ta dvojice kuliček neurčité bílo-červené barvy. Provázání původního stavu s entanglovaným párem se provede pomocí měření tzv. Bellových stavů, to na tom videu chybí, a teprve po této detekci se vzdálená částice prováže s původním stavem, což je znázorněno na tom videu v čase 9:22. Při měření Bellových stavů dvojice částic vlevo zkolabuje do jednoho ze čtyř možných Bellových stavů, a tahleta informace je nezbytná pro správnou rekonstrukci vzdáleného stavu vpravo. Tuto informaci, do kterého z Bellových stavů při provázání původního stavu s entanglovaným párem subsystém vlevo zkolaboval, je nutné klasickou cestou přenést do té vzdálené destinace (na videu prezentované částicí vpravo), a teprve s využitím této informace je možné příslušným měřením na vzdáleném místě rekonstruovat původní stav (na videu v čase 9:42, kdy vzdálená částice vpravo získala stav, který měla původní blízká částice v tom čase 9:21).

To video je bohužel popularizační a spousta klíčových informací v něm chybí - tyto informace je možné nalézt např. zde https://en.wikipedia.org/wiki/Quantum_teleportation, anebo česky opět v knížce Koncepční otázky kvantové teorie od Miloslava Duška na straně 188 (kapitola 12 - Kvantová teleportace a husté kvantové kódování).

Odpovědět

Re: Re: Re: Re: Re: Neznamenalo

Václav Dvořák,2018-04-30 03:14:24

Ok, díky za kritické posouzení, promyslím to všechno v souvislostech, přeci jen od té doby se stav vědění všeobecně posunul a budu si muset dostudovat celou tu víceletou mezeru. Váš příspěvek beru jako důležitý korektiv, díky. A určitě se tady nebo v nějakém navazujícím článku ještě ozvu.

Odpovědět

Re: Neznamenalo

Jakub Fiala,2018-04-28 18:48:18

Nadpis příspěvku
Re: Neznamenalo
Jméno autora
Jakub Fiala
Text původního příspěvku
Při komunikaci s využitím kvantového provázání získá příjemce řetězec symbolů, který je sice korelovaný s řetězcem odesilatele, ale který je přesto sám o sobě náhodný. Aby se z tohoto řetězce dala demodulovat informace, potřebuje příjemce získat dodatečnou informaci o nastavování odesilovatelova zařízení, a tuto informaci nelze předat jinak, než klasickou cestou.

Takže stačí poslat poslat klasicky počáteční nastavení a komunikace pomocí kvantového provázání pojede dále v reálném čase bez zpoždění? Nebo dostane řetězec informací a při dalším je nutné opět poslat nastavení? Je použitelná analogie sledovaní streamu informací když pošlu protistraně info o tom jak např. video dekódovat?

Asi se ptám blbě.

Odpovědět

Re: Re: Neznamenalo

Pavel Brož,2018-04-28 23:11:16

Neptáte se blbě, ptáte se naprosto správně, ona ta problematika totiž není úplně triviální.

Nevyhnutelným základem kvantové kryptografie tvoří entanglované páry částic, nicméně kvantová kryptografie se nedá zúžit pouze na měření prováděná na těchto párech, je zapotřebí něco více, pokusím se to tady popsat.

Nejprve si řekněme, co vlastně ty entanglované páry mají za tu klíčovou vlastnost, kterou klasické stavy hmoty nemají - touto vlastností je úplná korelace či antikorelace výsledků vzdálených měření (jestli jde o korelaci či antikorelaci závisí na druhu měření a také např. na tom, jestli entaglovaným párem je pár bozonů nebo naopak fermionů). Nejčastější měřenou vlastností u entanglovaných párů je spin (přesněji jeho průmět do vybrané osy), ten se měří jednoduše. U fotonů navíc spin odpovídá polarizaci fotonu, s pomocí polarizačních hranolů se dá tedy snadno měřit. Natočení polarizačního hranolu odpovídá výběru osy, která určuje průmět spinu, který měříme - jinými slovy, pokaždé, když změníme směr té osy, tak vlastně měříme jiný průmět spinu. Kvantová mechanika díky Heisenbergovu principu neurčitosti garantuje, že pokud měříme průmět spinu do nějaké osy, tak průmět spinu do jiného směru je neurčitý. V případě fermionů, pokud určíme průmět spinu do jedné osy, tak měření průmětu spinu do osy kolmé je už náhodné vzhledem k prvnímu měření (jinými slovy, u fermionů je mezi měřeními průmětu spinu do kolmých os vždy nulová korelace). U bozonů, jako jsou třeba fotony atd., dostaneme nulovou korelaci ne pro kolmé osy, ale pro osy pootočené o 45 stupňů.

Pro entanglované páry se dá ukázat, že ať už vybereme osu pro průmět spinu (tzv. polarizační bázi) jakkoliv, výsledek měření na jedné částici je naprosto náhodný. To také garantuje kvantová mechanika. Bez ohledu na to, jakou polarizační bázi zvolí odesilatel (tj. bez ohledu na to, jak natočí polarizační hranoly), tak se stejnou pravděpodobností (tj. s pravděpodobností

přesně jedna polovina) naměří jednu ze dvou možných hodnot průmětu spinu. Pro zjednodušení jedné hodnotě průmětu spinu přiřaďme nulu, druhé jedničku - odesilatel tedy nemůže ovlivnit, jestli při jakémkoliv měření dostane nulu nebo jedničku. On si pouze může být jistý tím, že vzdálený příjemce provádějící měření na druhé částici toho entanglovaného páru dostane - pakliže-li používá stejné natočení polarizačního hranolu, tedy stejnou bázi - naprosto tutéž hodnotu. Takže pokud odesilatel dostane nulu, ví, že nulu dostane při současném vzdáleném měření i příjemce, pokud dostane jedničku, ví, že ji dostane i příjemce (přesněji toto platí pro fotony a obecně pro bozony, pokud by místo nich byly použity entanglované fermiony, tak pokud by odesilatel dostal nulu, tak příjemce dostane jedničku a naopak).

Jinými slovy, to, co měření na entanglovaných párech poskytuje, není zpráva, ale je to generování náhodného klíče. Odesilatel svými měřeními naprosto neovlivní, jaký klíč vygeneruje, on vygeneruje náhodnou posloupnost bitů, ale může si být jistý, že příjemce - pokud používá stejnou bázi - získá přesně stejnou náhodnou posloupnost bitů. A získá ji okamžitě, na až když od odesilatele k příjemci dorazí rychlostí světla jakákoliv zpráva.

Právě tato náhodnost zachraňuje zadek speciální teorii relativity, která nepřipouští okamžitý přenos informace. Klíč je sice přenesen nadsvětelnou rychlostí (ve skutečnosti ale nedává smysl mluvit o nějakém přenosu, protože měření mohou být prováděna v identický čas, stejně dobře by tedy příjemce mohl tvrdit, že přenesl klíč k odesilateli), ale to, co je "přeneseno", není žádná informace, je to pouze náhodná sekvence bitů. Proto je také přesnější nenazývat to přenosem, ale korelací - prostě bez ohledu na to, kdo měřil dříve a kdo později, pro entanglované páry budou výsledky vzdálených měření při použití stejných polarizačních bází vždycky dokonale lícovat.

K čemu je dobrý náhodný klíč? Ke kryptování zpráv, které jsou pak přenášeny klasicky. Takhle to funguje i v dnešní klasické kryptografii, jedna strana komunikace vygeneruje náhodný klíč, sdělí ho druhé straně, a od té doby si vyměňují kryptované zprávy zašifrované právě tímto klíčem. Bohužel to je zároveň nejzranitelnější místo klasické kryptografie, to posílání vygenerovaného klíče protistraně, protože to v principu může být odposlechnuto. Kvantová kryptografie se od klasické liší právě v tom, že za pomocí entanglovaných stavů umí toto slabé místo odstranit. Nicméně výše popsaná procedura vygenerování klíče pomocí entanglovaných párů na to sama o sobě nestačí, protože je průstřelná klasickým odposlouchávacím trikem, který se nazývá „man in the middle“ - čili prostředník, který potají rozetne komunikační kanál mezi odesilatelem a příjemcem a sám se postaví mezi ně, přičemž vůči odesilateli se tváří, že je příjemce, a vůči příjemci, že je odesilatel. Nic netušící odesilatel mu pošle klíč, on si ho přečte a přepošle příjemci, a od té doby pohodlně dešifruje veškerou jejich komunikaci zašifrovanou právě tímto klíčem. Primitivní, ale účinné, jak by řekl zloduch Kopecký ve filmu Adéla ještě nevečeřela.

Jakým způsobem se tomu dá při měření entanglovaných párů zabránit? Aplikací následujících opatření:

- odesilatel i příjemce při měření na entanglovaných částicích používají navzájem na sobě nezávisle náhodně volené báze. Jinými slovy, odesilatel náhodně volí natočení polarizačního hranolu mezi dvěma orientacemi, které jsou vůči sobě natočeny o 45 stupňů (předpokládejme, že entanglovanými částicemi jsou fotony), a příjemce taktéž náhodně, nezávisle na odesilateli, mění natočení polarizačního hranolu mezi dvěma těmito možnostmi

- po skončení měření na veřejném kanále zveřejní natočení svých hranolů (nezveřejní ale výsledky svých měření, tedy zda pro to které natočení naměřili nulu nebo jedničku – připomeňme, že pro JAKÉKOLIV natočení hranolů jde získat se stejnou pravděpodobností nulu i jedničku)

- obětují část bitů na odhalení případného odposlechu

K čemu tato opatření budou? Připomeňme, že vzdálená měření budou korelovaná jenom tehdy, když se polarizační báze, tedy natočení hranolů u odesilatele a příjemce shodují, zatímco pokud budou báze vůči sobě pootočeny o 45 stupňů, bude mezi měřeními odesilatele a příjemce nulová korelace. Protože ale odesilatel i příjemce volí báze náhodně, shodnou se pouze v zhruba polovině případů. To, ve kterých případech se shodnou, se dozví právě dodatečným zveřejněním svých bází na veřejném kanále. Tak např. dejme tomu, že odesilatel i příjemce provádí měření na dvou tisících entanglovaných párech. Měřením tedy každý z nich získá náhodnou sekvenci dvou tisíc bitů – protože ale oba volili báze náhodně, pouze zhruba tisíc bitů bude korelovaných, zatímco pro těch zbylých zhruba tisíc bitů bude mezi odesilatelem a příjemcem nulová korelace. Kterých tisíc bitů je korelovaných se oba dozví po zveřejnění svých bází na veřejném kanále. Veřejný kanál je sice veřejný a proto si tam úplně každý může přečíst, které z těch bitů mají odesilatel a příjemce stejné – nicméně nedozví se, jestli ten který bit je nula nebo jednička, to ví jenom odesilatel a příjemce, a tuto informaci samozřejmě nezveřejňují, protože právě tato informace je tím vygenerovaným klíčem, který nadále budou používat ke komunikaci - přesněji ale jenom jeho část po obětování části bitů.

A to je ta poslední část, a to odhalení případného odposlechu obětováním části bitů. Tady se opět využije vlastnost kvantové mechaniky, která garantuje, že jakékoliv měření zruší korelaci následných měření na stejném páru. Takže pokud někdo využije onu odposlechovou strategii „man in the middle“, tak se sice dozví ten klíč, ale dozví se to i příjemce, že byl odposloucháván, a to proto, že jeho bity nebudou korelovány ani v případech, kdy zvolil stejné báze jako odesilatel. Dozví se to ale tak, že část z těch měřených bitů se přece jen musí zveřejnit a tudíž obětovat (zveřejněné bity samozřejmě nemá smysl používat jako část klíče). Dejme tomu, že odesilatel se s příjemcem dohodne, že zveřejní každý desátý bit, ve kterém se měli shodnout. Už víme, že se shodli zhruba v tisícovce bitů a oba ví, které bity by to měli být, nyní už zbývá ověřit, že je nikdo neodposlouchával. Odesilatel kromě nastavení bází zveřejní i každý desátý bit, ve kterým měli oba shodné báze, souhrnně je to tedy zhruba sto zveřejněných (a tedy obětovaných) bitů. Příjemce zkontroluje, jestli opravdu naměřil ve všech těchto bitech tutéž hodnotu (tedy nulu nebo jedničku). Pokud je nikdo neodposlouchával, tak se korelace zachovala, a příjemce zjistí, že jeho hodnoty pro těchto sto bitů jsou identické s odesilatelovými – zbylých cca 900 nezveřejněných bitů pak mohou použít jako tajný klíč pro šifrování následujících zpráv. Pokud ale příjemce zjistí, že jenom cca polovina z obětovaných bitů je stejná, tak ví, že byli odposloucháváni, a oznámí to na veřejném kanále odesilateli – tím pádem vygenerovaný klíč nepoužijí, a pokusí se vygenerovat si klíč někdy později, po provedení nějakých protiopatření proti potenciálnímu odposlouchávajícímu prostředníkovi.

A to je celé :-)

Odpovědět

Re: Re: Re: Neznamenalo

Vladimír Lieberzeit,2018-04-29 09:32:04

Pro pochopení té ochrany proti odposlechu mi chybí ještě jedna informace: Útočník by mohl teoreticky zachytit přenášenou částici, změřit ji v obou bázích, a poslat dál (samozřejmě v kolabovaném stavu). Cílový adresát ji také změří, ve své náhodně vybrané bázi -- ale protože útočník zná hodnoty v obou bázích, je mu to jedno.

Předpokládám, že toto nejde, ale chybí mi informace, proč. Změřením v druhé bázi se zároveň zruší výsledek měření v první bázi (tj. opakovaným měřením v první bázi vyjde jiná hodnota)? Nebo je to jinak?

Odpovědět

Re: Re: Re: Re: Neznamenalo

Pavel Brož,2018-04-29 13:41:44

To je naprosto správná připomínka, už po odeslání příspěvku jsem si uvědomil, že jsem to tam měl rozvést, ale měl jsem za to, že se nad tím stejně nikdo nebude pozastavovat – těší mě, že někdo čte mé příspěvky tak důkladně :-)

Útočník může rozetnout kanál a mít k dispozici naprosto identické přijímací vybavení jako legitimní příjemce, může dělat naprosto totéž, co by dělal příjemce, a proto získá svými měřeními v těch případech, kdy se shodne v bázích s odesilatelem, naprosto tutéž sekvenci bitů. Útočník se tedy tuto sekvenci dozví tak jako tak, jde jenom o to, aby tato sekvence poté nebyla použita jako klíč pro následnou komunikaci - tedy jde jenom o to, aby legitimní příjemce spolehlivě poznal, že k odposlechu došlo.

Odposlech jde spolehlivě poznat díky ztrátě korelace mezi měřeními odesilatele a legitimního příjemce. Korelace je při odposlechu zachována mezi odesilatelem a útočníkem, a útočník opravdu může po měření poslat po měření částici dál příjemci, event. vygenerovat novou (v případě fotonů to ani jinak nejde, protože foton po detekci zaniká). Pravidla kvantové mechaniky ale garantují, že takto přeposlaná či znovu vygenerovaná částice už nebude entanglovaná s částicí odesilatele - a pouze entanglované částice mají tu magickou vlastnost, že měření na nich prováděná jsou korelovaná.

Pravidla kvantové mechaniky navíc garantují to, že nemůžete vytvořit v jednom místě částici entanglovanou s jinou vzdálenou částicí, aniž byste vytvořil interakční řetězec mezi oběma místy. Existuje sice fenomén známý jako tzv. přenos entanglementu, který se dá využít k tzv. kvantové teleportaci, kdy přenesete lokální kvantový stav z jednoho místa do jiného vzdáleného místa - nicméně v tomto případě potřebujete obě místa propojit jiným entanglovaným párem, který umožní ten entanglement přenést. Pokud by tedy útočník chtěl vytvořit entanglovanou částici s částicí odesilatele, musel by spolupracovat s odesilatelem, aby se mu to podařilo. Ani potom by neměl vyhráno, kvantová teorie totiž přináší další omezení v podobě tzv. "No-cloning" teorému (https://en.wikipedia.org/wiki/No-cloning_theorem), který výrazně omezuje možnost vytvořit kopii kvantového stavu (striktně řečeno, "kopírováním" kvantového stavu se zničí originál, takže např. při kvantové teleportaci není možno vytvářet klony originálu - v kvantové kryptografii se tomuto teorému a jeho případnému obejití logicky věnovala velká pozornost, a díky tomu se podařilo získat i spoustu výsledků, které umožňují tu striktnost toho zákazu "změkčit" a vytvořit nedokonalou kopii).

Co se týče toho změření částice v obou bázích, tak tam opět úřaduje kvantová mechanika a jí

předpovídaná ztráta korelace. Měření ve dvou bázích pootočených vůči sobě o 45 stupňů (bavíme-li se o fotonech) jsou totiž vzájemně nekompatibilní, podobně, jako je v kvantové mechanice vzájemně nekompatibilní měření polohy a hybnosti. Heisenbergův princip neurčitosti říká, že když naprosto přesně změříte jedno, tak máte maximální neurčitost pro měření druhého. V případě měření spinu samozřejmě můžeme dostat jenom dvě možné hodnoty, ta maximální neurčitost se v tomto případě tedy neodrazí v množství hodnot, které lze na druhé ose naměřit, ale v tom, že mezi těmi měřeními bude nulová korelace. Pokud tedy útočník změří průmět spinu částice v jedné bázi, a pokud zrovna náhodou použil stejnou bázi jako odesilatel, bude mít absolutní korelaci měřených hodnot s odesilatelem. Pokud následně bude měřit v druhé bázi, toto měření už bude mít nulovou korelaci s měřením předchozím (a tím pádem i s měřením odesilatele) – a to právě díky principu neurčitosti, zde aplikovanému na měření v různých polarizačních bázích.

Odpovědět

Re: Re: Re: Neznamenalo

Richard Palkovac,2018-04-29 10:03:54

Dokladne vysvetlene, len by som poopravil jednu malickost netykajucu sa entaglementu. Sucasna klasicka kryptografia pouzivana na internete nie je o "jedna strana komunikace vygeneruje náhodný klíč, sdělí ho druhé straně, a od té doby si vyměňují kryptované zprávy zašifrované právě tímto klíčem". To by sa jednalo pouzitie symetrickej sifry (klucom ktorym zasifrujem aj odsifrujem) a ta je na internete nepouzitelna.

Pouziva sa asymetricke sifrovanie, ked jedna strana si vygeneruje svoj privatny aj verejny kluc. Privatny kluc je tajny, nikam sa neposiela a sluzi na odsifrovanie stravy. Verejny kluc sa vystavi verejne na internete, moze si ho hocikto skopirovat, ten totiz sluzi len na zasifrovanie spravy. Z verejneho kluca nie je mozne zistit privatny kluc (v rozumnom case) a tak ak niekto zasifruje verejnym klucom spravu, ktoru chce odoslat a nezachova si original, uz sa k originalu nedostane, totiz zasifrovana sprava a verejny kluc ho k orginalu uz nevrati.

Takto funguje (aspon dufam) komunikacia s bankami a vsetkymi internetovymi strankami ktore idu cez "https://" , to "s" je tam dolezite.

Kvantove pocitae nas strasia tym, ze asymetricka sifra bude prelomitelna hrubou silou, kedze budu mat na taketo ulohy velky vykon. Zatial je to ale len strasenie.

Odpovědět

Re: Re: Re: Re: Neznamenalo

Vladimír Lieberzeit,2018-04-29 10:27:25

V reálu se asymetrická šifra nepoužívá pro šifrování celé zprávy, protože je příliš pomalá a výpočetně náročná. Místo toho se zpráva šifruje symetrickou šifrou s náhodně vygenerovaným dočasným klíčem. Pouze tento dočasný klíč se chrání pomocí asymetrické šifry. Kvantová kryptografie tedy v tomto schématu nahrazuje tu asymetrickou šifru (přesněji key agreement - postup pro shodu obou stran na dočasném klíči), dál už je to stejné.

Odpovědět

Re: Re: Re: Re: Re: Neznamenalo

Richard Palkovac,2018-04-29 17:23:03

Diky za upresnenie.

Odpovědět

Re: Re: Re: Neznamenalo

Jakub Fiala,2018-04-29 22:34:07

Ok. Děkuji už je mi to jasné.

Odpovědět

Re: Neznamenalo

Zdeněk Smutný,2018-04-29 01:44:44

Mám tu čest s vámi nesouhlasit. Kvantová provázanost objektu je sama o sobě informace, vrsvením provázanosti objektů lze dosáhnout zprávy (toku informací) stejné jako má bit v našich počítačích, jen s tím rozdílem, že možností stavů objektu je nezměrně více než 0-1. Kdyby to tak nebylo nesnažili by se vědci a další organizace sestavit kvantové počítače které budou o řády výkonější než dnešní klasické počítače. Nemyslím si dokonce ani to, že by adresát musel vědět stav objektu u odesílatele, protože při zjištění tohoto stavu u odesílatele by okamžitě došlo ke změně stavu provázanosti objektu, což by mělo za následek nekonečnou smyčku chybných informací (změny stavů objektu).

Odpovědět

Re: Re: Neznamenalo

Pavel Brož,2018-04-29 14:11:12

Takhle, jestli kvantovou provázanost neboli entanglement a jeho přenos nazveme informací nebo ne, to je opravdu maximálně tak etymologický problém, který nemá žádný dopad na to, že ani s využitím entanglementu nelze informaci přenést rychleji než světlo. Bez využití dodatečných klasicky přenášených informací o nastavení bází apod. je výsledek finálního měření na stavech získaných přenášením entanglementu naprosto náhodný. Platí to i pro oblast kvantového počítání.

Toto omezení samozřejmě neznamená, že s využitím tzv. kvantových bitů alias qubitů, které opravdu obsahují více informace, než klasická nula a jednička, nelze získat rapidní nárůst výkonu počítačů - přesně proto je samozřejmě jak píšete této oblasti věnována tak velká pozornost.

Vaše poslední věta týkající se oné údajné nekonečné smyčky chybných informací nedává

bohužel smysl - žádná nekonečná smyčka chybných informací nenastává, korelace je ztracena už po prvních měření, od toho okamžiku jsou částice nadále neprovázané a chovají se vůči sobě nezávisle, žádná nekonečná smyčka změn stavů objektu tedy nehrozí.

Tak jako tak, nemožnost přenést informaci s využitím entanglementu, pokud se zároveň nepřenese klasickou cestou (tedy maximálně světelnou rychlostí) i informace např. o nastavování bází odesilatele, jde v kvantové mechanice matematicky exaktně dokázat, jeden takový důkaz je popsán např. v kníže Koncepční otázky kvantové teorie od Miloslava Duška na straně 151 - důkaz zabírá sice pouze jednu stránku, nicméně je nutné znát i značné množství prerekvizit z kvantové mechaniky, proto nemá smysl, abych jej zde přepisoval. Tento matematický důkaz tedy implikuje, že buď je kvantová teorie správně a nejde přenést informaci nadsvětelnou rychlostí, anebo jde přenést informaci nadsvětelnou rychlostí, a kvantová teorie je špatně - jinou možnost logika nepřipouští. Vyberte si.

Odpovědět

Re: Re: Re: Neznamenalo

Z Z,2018-04-29 21:39:14

využitím tzv. kvantových bitů alias qubitů, které opravdu obsahují více informace, ... rapidní nárůst výkonu počítačů

Nie je jednou z podstát nárastu výkonu takýchto počítačov to, že sa vlastne jedná o analógové počítače? Len sú veličiny na oveľa menších objektoch než analógové počítače, ktoré sa používali kedysi dávno. A kvantová previazanosť je ďalšia využiteľná charakteristika takých počítačov.

Odpovědět

Re: Re: Re: Re: Neznamenalo

Václav Dvořák,2018-04-29 23:30:14

Myslím, že v podstatě máte pravdu v tom, že jde určitým způsobem o analogové počítače (v tom smyslu že se pracuje s float hodnotami namísto integerů), ale hlavní výhoda nebo "killing feature" je, že výpočet je okamžitý tj. ve chvíli, kdy jsou nastaveny vstupní hodnoty máme výsledek. Proč to tak je by vedlo k opravdu divokým hypotézám, které souvisí s mnoha dalšími kvantovými fenomény a nejen s nimi a raději to tady nebudu rozvádět, protože chci zůstat na bezpečném poli technologií :)

Odpovědět

Re: Re: Re: Re: Neznamenalo

Pavel Brož,2018-04-29 23:48:30

Kdepak, kvantové počítače sice částečně lze chápat jakožto analogové počítače pracující s pravděpodobnostními algoritmy, které využívají jevy jako je linearita evoluce, superpozice atd. (které ale nejsou výsadou jenom kvantové teorie, uplatňují se totiž i v klasické

elektrodynamice, včetně jejích technických aplikací, jako je elektrotechnika atd.), jejich hlavní přednost ale vězí v něčem jiném, a to je exponenciální růst dimenze stavového prostoru v závislosti na počtu jeho komponent. Takhle napsáno to zní jako nicneříkající blábol, proto to blíže rozvedu.

Pokud máme nějakou kvantovou charakteristiku, jako je třeba spin částice, tak tu popisujeme stavovým vektorem v komplexním vektorovém prostoru, který má takovou komplexní dimenzi, kolik hodnot průmětu spinu můžeme dostat. Třeba u elektronu nebo fotonu můžeme dostat pouze dvě hodnoty, proto stavovým prostorem jejich spinu je dvoudimenzionální komplexní prostor (ten je mimochodem ekvivalentní čtyřdimenzionálnímu reálnému prostoru, ale to v našich úvahách nebude hrát roli). Ve skutečnosti ale musí být stavový vektor normovaný, takže jednu komplexní dimenzi ubereme (jednu reálnou dimenzi ubereme podmínkou, že norma vektoru je rovna jedné, další reálnou ubereme ignorováním fyzikálně nepodstatného fázového faktoru, takže ubereme dvě reálné = jednu komplexní dimenzi). Spin částice se používá nejčastěji, vektor v odpovídajícím stavovém prostoru se pak nazývá qubit, a je popsán právě jedním komplexním číslem (nenabývá tedy jenom hodnot 0 nebo 1 jako klasický bit, ale může být popsán libovolným komplexním číslem).

Zatím jsme nijak nevybočili z možností, které lze realizovat i klasickými nekvantovými způsoby. Tak např. střídavý elektrický proud v obvodu také můžeme popsat komplexním číslem, jehož absolutní hodnota odpovídá amplitudě proudu a jehož argument určuje fázi proudu. To, čím se ale kvantová teorie od klasických analogových systémů liší, je jakým způsobem roste dimenze systému s počtem komponent.

V kvantové teorii se totiž systém složený z n subsystémů popisuje komplexním vektorovým prostorem, jehož dimenze je rovna součinu dimenzí stavových prostorů komponent. Oproti tomu pro klasické nekvantové systémy platí, že dimenze stavového prostoru celkového systému je rovna součtu dimenzí stavových prostorů komponent. Pokud bychom se pokusili jeden qubit realizovat např. proudem či napětím v nějakém obvodu, mohli bychom s ním dělat srovnatelné věci, co s kvantovým qubitem realizovaným pomocí spinu např. elektronu. Rozdíl by nastal, pokud těch qubitů začneme dávat dohromady více a více.

Pro systém složený ze dvou „elektrických qubitů“ (tedy např. ze dvou nezávislých obvodů) dostaneme dvě komplexní dimenze (jedna pro každý obvod), pro systém složený ze tří „elektrických qubitů“ dostaneme tři komplexní dimenze, pro čtyři obvody dostaneme čtyři komplexní dimenze, atd.. Oproti tomu pro systém složený ze dvou KVANTOVÝCH qubitů dostaneme tři komplexní dimenze (dva krát dva a nakonec minus jedna komplexní dimenze na normu a společný irelevantní fázový faktor), pro tři qubity dostaneme sedm komplexních dimenzí (dva krát dva krát dva a nakonec minus jedna na normu a společnou fázi), pro čtyři qubity dostaneme patnáct komplexních dimenzí (dvě na čtvrtou minus jedna), atd..

V čem je rozdíl kvantových systémů vůči nekvantovým, že pro ty kvantové roste dimenze jejich stavového prostoru tak rychle? To navíc dělají entanglované stavy. Entanglované stavy jsou stavy systému, ve kterých jej nejde popsat jako direktní součin stavů jejich komponent – takhle to zní příliš učeně, laickým jazykem bychom řekli, že systém nejde popsat tak, že popíšeme stavy jeho komponent, ale že ho místo toho musíme popsat jako celek. Stavy systému, které se dají redukovat na popis stavů jednotlivých komponent, jsou neentanglované stavy (také jim říkáme faktorizovatelné stavy, protože stav celkového systému lze napsat jako direktní součin stavů komponent). Pokud bychom se omezili na neentanglované (tedy faktorizovatelné) stavy, tak by dimenze stavového prostoru systému rostla úplně stejně, jako u

klasických systémů, tedy dimenze prostoru pro popis celého systému by byla pouze součtem dimenzí prostorů pro popis jeho komponent. Ty dimenze navíc mají na svědomí právě ty stavy, které faktorizovatelné nejsou, a to jsou entanglované stavy.

Vidíme tedy, že už od tří qubitů včetně je entanglovaných stavů více, než těch neentanglovaných, a tento rozdíl exponenciálně narůstá s počtem qubitů. Obrovský teoretický výpočetní výkon kvantových počítačů tedy mají na svědomí entanglované stavy, protože jenom díky nim narůstá dimenze stavového prostoru systému exponenciálně. Díky tomuto exponenciálnímu nárůstu stavového prostoru je potom možné pomocí fenoménů, jako je superpozice kvantových stavů a linearita evoluce kvantového systému, provést nesrovnatelně více paralelních „výpočetních podprocesů“, ze kterých se finálně získá konečný výsledek.

Když bychom udělali jakousi rekapitulaci toho, jak kvantová teorie měnila naše chápání světa, tak bychom logicky začali u jednočásticových systémů popisovaných vlnovou funkcí podobnou, která je formálně podobná popisu třeba potenciálu elektrického pole. Kvantová teorie nám už u těchto primitivních systémů ukázala prapodivné fenomény, jako je dualita vlna-částice či Heisenbergův princip neurčitosti, který zamezuje současné přesné měření polohy a hybnosti částice. Pokud už máme pocit, že jsme tyto podivnosti vstřebali, tak kvantová teorie výrazně přitvrdí ukázáním dalších prapodivností, jakými jsou entanglované stavy dvou a více částic a s nimi spojené nelokální korelace (existence těchto nelokálních korelací je dnes už opravdu nade všechnu pochybnost experimentálně prokázána). S dalším růstem počtu částic pak kvantová teorie nabízí nebývalý nárůst výkonu kvantových počítačů, který je právě garantován tím, že počet entanglovaných stavů roste s počtem qubitů exponenciálně, zatímco počet neentanglovaných stavů pouze lineárně.

Samozřejmě není to až tak jednoduché ty kvantové počítače sestrojit, protože entanglované stavy jsou extrémně křehké, a při sebemenším narušení kolabují do stavů neentanglovaných – což je také důvod, proč svět kolem nás vypadá na makroskopických měřítkách klasicky a ne kvantově, a proč makroskopické entanglované stavy typu Schrodingerova kočka kolem sebe nevídáme.

Odpovědět

Re: Re: Re: Re: Re: Neznamenalo

Václav Dvořák,2018-04-30 03:22:19

Kvantový počítač lze realizovat i chemicky. Jste si jist, že i v tomto případě bude výsledek reakce záviset na entaglementu? A není v tom případě entaglement projevem nějakého vyššího principu resp. obecné teorie?

Apropos rozvedl jste to doširoka, ale jste si opravdu jist, že stavy typu Schrodingerova kočka kolem sebe nevídáme? Myslím tím hlavně interní stav mozku nebo vědomí, nikoli (jen) realitu zprostředkovanou smysly...

Odpovědět

Re: Re: Re: Re: Re: Re: Neznamenalo

Pavel Brož,2018-04-30 11:07:45

Tam se jedná o to, co nazvete kvantovým počítačem. Dejme tomu, že vyrobíte řadu qubitů jakožto základ pro kvantový počítač, ale nebudete umět entanglovat jejich stavy (v takovém případě můžete ty qubity realizovat i klasicky). I na takovém počítači můžete provádět množství různých výpočetních operací, které využívají superpozici a interferenci, ale nikdy nevyužijete skutečný potenciál, který poskytují právě ty entanglované stavy. Počítač postavený na řadě qubitů bez možnosti entanglementu bude rovnocenný analogovému počítači s patřičným počtem paralelně pracujících obvodů, které budou uchovávat ty analogové stavy mezi nulou a jedničkou. Jestli se rozhodneme takový počítač nazvat kvantovým, to je otázka terminologie, nemění se tím nic na tom, že takovýto zjednodušený počítač by neměl šanci louskat v polynomiálním čase klasicky exponenciální úlohy, např. prolamovat dnes neprolomitelné šifry. A právě příslib, že kvantové počítače by mohly umožnit řešit exponenciální úlohy v polynomiálním čase je přesně ten důvod, proč se jim věnuje taková pozornost.

Co se týče toho, jestli makroskopické entanglementy typu Schrodingerova kočka lze či nelze vidět interně ve stavu mozku, tak k tomu mohu říct jen tolik, že do cizích mozků nevidím, maximálně tak do svého a to ještě s velkými výhradami, a pokud mohu soudit, tak Schrodingerovy kočky ani jiné entanglované příšery nevidím ani v těch nejdivočejších snech, a to si myslím, že obecně umí být sny opravdu hodně ujeté.

Odpovědět