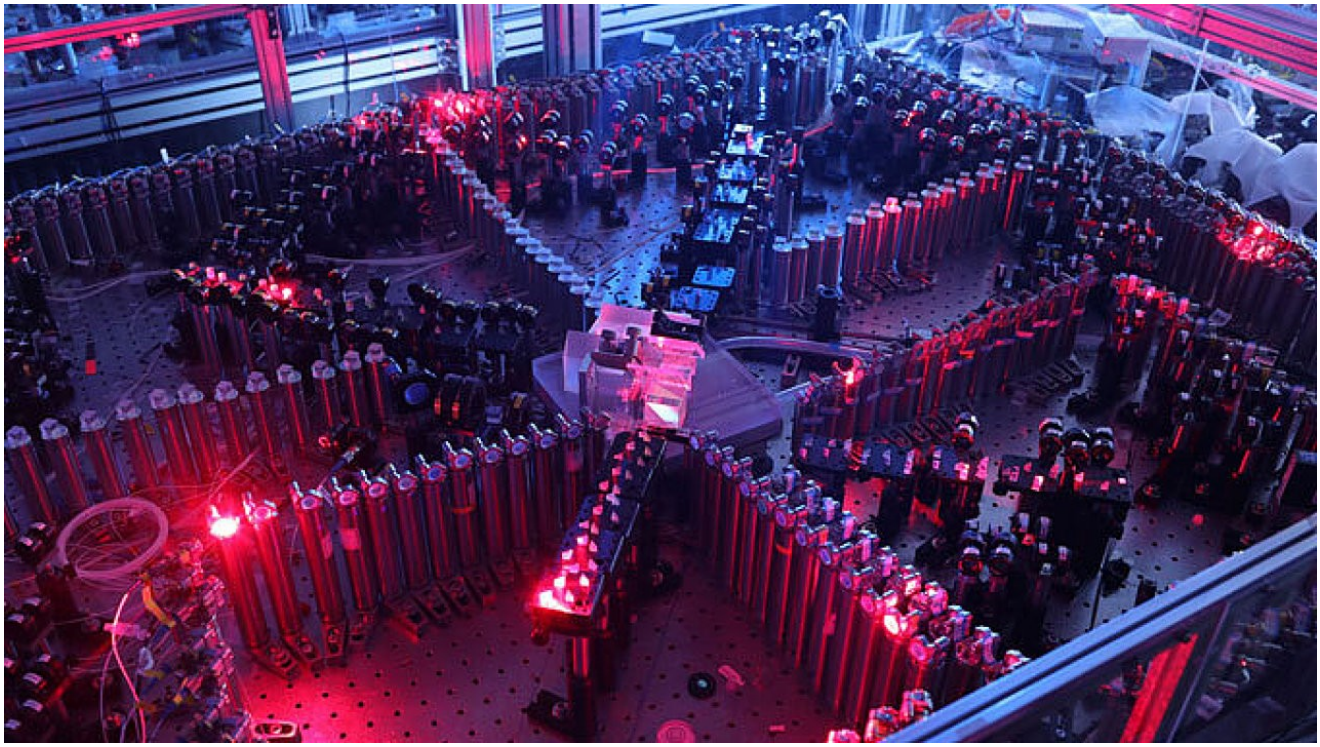
Vědci zkrotili jev umožňující teleportaci informací, pokládají základy kvantového internetu

https://zahranicni.ihned.cz/c1-66875080-vedci-zkrotili-jev-umoznujici-teleportaci-informaci-pokladaji-zaklady-kvantoveho-internetu



Kvantový počítač Jiuzhang dosáhl kvantové nadřazenosti díky algoritmu vyvinutému českými vědci. autor: Han-Sen Zhong, University of Science & Technology of China

- David Busta, editor

1. 2. 2021 07:33 / 17 minut čtení

Velké čtení fyzika informatika bezpečnost šifrování počítač

Einstein by šel asi do mdlob, kdyby viděl, že kvantová teleportace informací je nejen možná, ale dokonce na ní půjde jednou vystavět kvantový internet. To, co velký vědec pokládal za důsledek neúplnosti kvantové teorie, popisující chování mikrosvěta, nyní odborníci z Caltechu, NASA, Fermilabu, Harvardu, Calgarské univerzity a AT&T využili k demonstraci stabilní teleportace informací na vzdálenost 44 kilometrů. Čína zároveň zprovoznila první kvantovou síť. V prosinci přišla navíc zpráva, že země dosáhla kvantové nadřazenosti - vlastní počítač schopný provést takový výpočet, který nezvládne žádný současný superpočítač ani za prakticky neomezeně dlouhou dobu. Povedlo se jí to díky algoritmu, který vyvinuli čeští vědci.

Lidstvo je svědkem druhé kvantové revoluce, i když si to pro těžkou uchopitelnost kvantové fyziky dost možná neuvědomuje a přehlíží její dalekosáhlé důsledky. Podobně jako v 60. letech většina lidí netušila, čeho předzvěstí je spuštění Arpanetu, tedy předchůdce dnešní podoby internetu. Sledovat vývoj na poli kvantových technologií je nezbytné už proto, že revoluce tentokrát přichází především z Východu. Proto jsme se rozhodli ve spolupráci s kvantovými fyziky z ČVUT v Praze našim

čtenářům přiblížit, jak kvantové technologie fungují a jak zásadně dopadnou na život nás všech v blízké budoucnosti.

Pro zorientování se ve světě kvantových technologií je třeba se nejdříve ponořit do zákonitostí mikrosvěta a principu kvantových výpočtů. V klasické výpočetní technice je jednotkou informace bit, který může nabývat hodnoty 0 nebo 1. V kvantovém světě je ale jednotkou informace kvantový bit neboli qubit, který se dle zákonů kvantové mechaniky může nacházet v takzvané superpozici stavů 0 a 1 zároveň. V praxi to znamená, že měříme-li stav qubitů připravených ve stejné superpozici, je možné s určitými pravděpodobnostmi dostat oba výsledky 0 a 1.

U klasického počítače je 0 nebo 1 reprezentována fyzicky tranzistorem, který je buď pod napětím, nebo není. U kvantového počítače může být qubit fyzicky reprezentovaný například polarizací fotonů nebo spinem elektronů. Spin je vlastnost částic mikrosvěta, kterou je obtížné si vizuálně představit, neboť neodpovídá ničemu, co existuje v našem světě velkých rozměrů.[1] U částic je zodpovědná za generování magnetického pole, a co je důležité, spin může být orientován dvěma směry. Pro zjednodušení může jít o směr nahoru a dolů. Zároveň platí princip superpozice, tedy že částice má s nějakou pravděpodobností jak spin nahoru, tak spin dolů. Přirozeně se proto částice nachází v superpozici obou stavů, kdy má spin nahoru i dolů zároveň. Qubit je v superpozici 0 a 1.

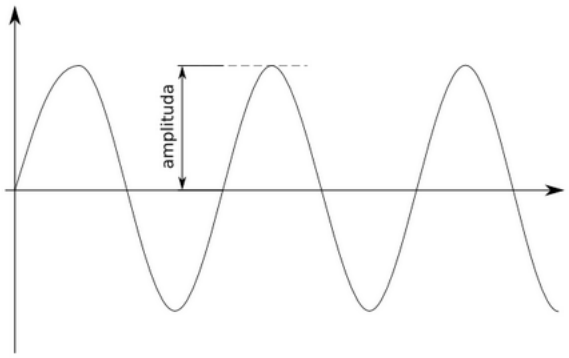
Celé to lze zapsat matematicky. Například spin směrem nahoru lze označit znakem $|0\rangle$ a spin směrem dolů takto $|1\rangle$. Toto je kvantový zápis pro 0 a 1. Superpozici jednoho qubitu pak lze zapsat matematicky jako:

$$\alpha|0\rangle + \beta|1\rangle$$

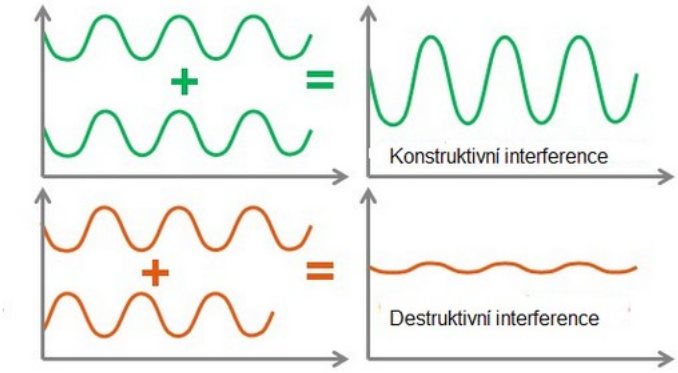
Písmena α a β jsou důležité koeficienty, takzvané amplitudy *(viz box)*. Jejich umocněním lze následně získat pravděpodobnost, s jakou se qubit nachází ve stavu $|0\rangle$ nebo $|1\rangle$.* Když bude α rovna nule a β rovna jedné, znamená to, že po změření částice vědec s naprostou jistotou zjistí, že spin míří směrem dolů, tedy že hodnota qubitu je 1. Když bude α rovna 0,6 a β rovna 0,8, pak pravděpodobnost, že po změření bude qubit ve stavu $|0\rangle$ je rovna $0{,}6^2$, což je 0,36. Pravděpodobnost, že bude ve stavu $|1\rangle$ pak odpovídá $0{,}8^2$, což je 0,64. Součet obou pravděpodobností 0,36 a 0,64 musí být roven jedné, protože pravděpodobnost nemůže být vyšší než jedna neboli sto procent. A tímto se qubity liší od bitů. Zatímco bit nabývá přirozeně pouze hodnoty 0, nebo 1, qubit je v superpozici 0 i 1, dokud není změřen. V okamžiku změření si musí qubit vybrat jednu z hodnot 0 a 1.

Amplituda

Amplituda je rozkmit vlny. Jde o výšku vlny vyznačenou v obrázku níže.



Částice mikrosvěta se chovají i jako vlny. Když vědci kvantový počítač programují, manipulují právě s jejich amplitudami, tedy koeficienty α a β. Dělají to s využitím laserového pulzu nebo magnetického pole. Operace se provádí u všech koeficientů naráz. Takto zadají počítači výpočetní úlohu. Vlny jsou charakteristické tím, že se vzájemně ovlivňují. Když se hodí do vody dva kameny, vyvolají na hladině vody vlny, které se vzájemně ovlivňují, posilují se nebo se oslabují. Říká se, že interferují. A tak se to děje i s částicemi mikrosvěta. Po spuštění programu dochází ke kvantové interferenci, čímž dojde k zesílení amplitud některých vln. Jinak řečeno soustava qubitů vytvoří preferovaný stav a jeho přečtením se získá řešení zadaného výpočetního úkolu.



Když se potkají dvě vlny vzniklé například dopadem dvou kamenů do rybníka, interferují spolu. Mohou se vzájemně posílit, pak výsledná složená vlna má vyšší amplitudu než původní vlny. Jde o konstruktivní interferenci. Může ale dojít i k destruktivní interferenci, kdy je amplituda složené vlny nižší, jak ukazuje spodní obrázek. Jde o destruktivní interferenci. Podobně spolu interferují i částice mikrosvěta.

Obrázky: Wikimedia/Krmo

K postavení kvantového počítače je zapotřebí ještě další podivné vlastnost mikrosvěta, tou je kvantové provázání. Odborně jde o kvantově korelovaný stav systému dvou a více částic. A do tohoto stavu je potřeba dostat qubity. Co to znamená? Jeden qubit je přirozeně v superpozici dvou stavů, jak bylo zmíněno výše. Při aktu měření pak u něj s určitou pravděpodobností vědec naměří 0, nebo 1. Dva qubity mohou být ve vzájemné superpozici až čtyř možných stavů 00, 11, 01 i 10, které mají každý svůj koeficient α, β, γ, δ.

Matematický obecný zápis stavu dvou qubitů proto vypadá takto:

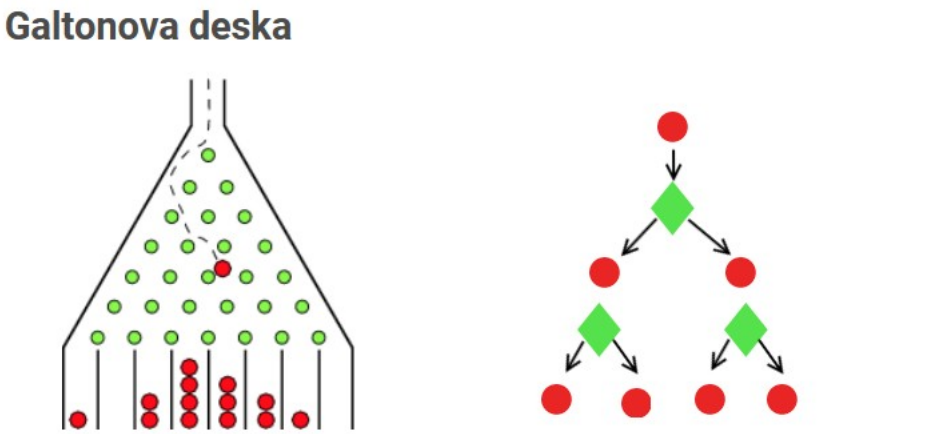
$$\alpha|00\rangle + \beta|11\rangle + \gamma|01\rangle + \delta|10\rangle$$

První číslo v závorce odpovídá prvnímu qubitu a druhé druhému qubitu. Pokud dojde k měření, vědec s danými pravděpodobnostmi změří, že buď první qubit je 0 a druhý 0, nebo první je 1 a druhý 1, nebo první 0 a druhý 1, nebo první 1 a druhý 0. Kvantově provázané stavy jsou pak speciální superpozice stavů, jako je například stav $\gamma|01\rangle + \gamma|10\rangle$, kdy α a β jsou nulové a γ=δ.[2] Jejich zvláštní vlastností je, že měření na jednotlivých qubitech jsou navzájem korelovaná. Na příkladu výše uvedeného provázaného stavu: změříme-li první qubit, zdali je ve stavu 0, nebo 1, je výsledek měření na druhém qubitu pak již daný a rovný opačné hodnotě naměřené na prvním qubitu. Pokud je výsledek na prvním qubitu 1, pak je na druhém 0 a naopak.

Čím více qubitů se podaří takto provázat, tím může být kvantové zpracování informace efektivnější.[3] Známý kvantový počítač od Googlu Sycamore disponuje 53 qubity, to znamená, že je schopný být v superpozici stavů, které zahrnují více než devět biliard možností. Tedy stav jednoho qubitu popisují dva koeficienty *(α a β)* , u dvou provázaných qubitů jsou čtyři *(α, β, γ, δ)*, u 53 provázaných qubitů jich je už přes devět biliard (!), což je devítka následovaná patnácti nulami. Společnost IBM očekává do roku 2023 představení kvantového počítače s 1000 qubity.

Díky tomu může kvantový počítač pracovat při řešení řady úloh mnohem rychleji než běžné počítače – dovede zkoumat všechna potenciální řešení zadané úlohy najednou. Zatím se tím žádný kvantový počítač nezabýval, ale principiálně si to lze představit u šachové partie. Když klasický počítač hraje šachy, prochází všechny možné kombinace postupně. Pokud tak chce vidět pouhé tři tahy dopředu, musí projít devět milionů možných šachových partií. Kvantový počítač ale prochází všechny partie v jednotlivých tazích najednou. Tedy místo devíti milionů úkonů mu stačí udělat tři. To je příčina toho, proč dokáže podobné úlohy řešit dokonce i v porovnání se superpočítačem v tak extrémně krátkém čase a proč i s 53qubitovým kvantovým počítačem dokázal Google loni dosáhnout kvantové nadřazenosti, tedy provést výpočet, který by superpočítači trval neúnosně dlouho.

Je pravda, že dnešní algoritmy jsou kvantovým počítačům psané doslova na tělo a pořád jde o úlohy, které nejsou zrovna praktické. Podobně těžko v praxi využitelnou úlohu jako Google řešili i čínští vědci se svým kvantovým počítačem Jiuzhang, jenž je zároveň druhým kvantovým počítačem, který dosáhl kvantové nadřazenosti. Byl na něm spuštěn algoritmus řešící takzvané Gaussovo vzorkování bosonů. Za algoritmem stojí vědecký tým v čele s profesorem Igorem Jexem z Fakulty jaderné a fyzikálně inženýrské Českého vysokého učení technického v Praze. Princip fungování algoritmu Jex ilustruje na takzvané Galtonově desce, do níž se shora vloží kulička, která pak na základě náhodných nárazů do překážek skončí v jednom z kastlíků níže. Když se to opakuje s velkým množstvím kuliček, tak většina jich skončí v prostředním kastlíku a v těch prostřednímu nejbližších. Čím blíž je kastlík okraji, tím méně se do něj zatoulá kuliček.



Vlevo je standardní Galtonova deska. Když se do ní vhodí kulička, ta se náhodně odráží od překážek, až skončí v některém z kastlíků níže. Vpravo je kvantová obdoba. Kuličkou je foton a překážky jsou paprskové rozdělovače. Foton naráží na všechny rozdělovače zároveň. Když se navíc pošle do zařízení více fotonů najednou, interferují spolu. Proto obtížnost simulace takové úlohy klasickým počítačem velmi rychle narůstá. Animovanou verzi lze nalézt na stránkách německé Paderbornské univerzity: https://cutt.ly/QjUXSqD

Obrázky: Shutterstock

Čínští vědci pak provedli něco podobného. Místo kuliček ale použili fotony a místo překážek děliče paprsků. Když do takovéto kvantové verze desky vletí foton, tak při nárazu na první dělič se rozdělí a vydá se doprava i doleva zároveň. To je onen princip superpozice. Když se do desky pošle více kuliček najednou, může se stát, že některé do sebe vzájemně narazí a to je vychýlí z původního směru. Fotony v desce s děliči paprsků se také ovlivňují, říká se, že interferují. A čínští vědci udělali to, že do desky vyslali velké množství fotonů a udělali to několikrát za sebou. Po projití fotonů spletitými cestami počítače pak na jeho výstupech změřili, kolik jich každým výstupem prošlo, kolik jich skončilo ve kterém kastlíku. Výsledkem je rozložení fotonů, tedy pravděpodobnosti, na kterém výstupu kolik fotonů skončí. S rostoucím počtem fotonů prudce narůstá složitost problému. Klasický počítač by simulaci takovéto úlohy prováděl tisíce let.

Popsaný algoritmus a jeho způsob realizace kvantovým počítačem trochu připomíná staré analogové počítače. Před nástupem dnešních digitálních počítačů se k řešení rovnice vytvořil speciální algoritmus a k němu byl postaven počítač. Rovnice byla doslova modelována počítačem. Čínský kvantový počítač také nelze využít pro řešení žádné jiné úlohy. Jiuzhang demonstroval svou kvantovou nadřazenost mnohem důrazněji než Sycamore od Googlu. Na druhou stranu kvantový počítač Googlu je programovatelný, použitelný i k jiným výpočtům. Ukázal to minulý rok, kdy se na něm podařilo provést první simulaci chemické reakce. Vystupoval v ní sice primitivní diazen, což je sloučenina dvou atomů dusíku a dvou atomů vodíku, jde ale už o posun směrem k využitelnosti.

Rozvoj kvantových počítačů tak nestojí pouze na jejich technické konstrukci, ale i na jejich programování a vývoji algoritmů. Na vysokých školách už se s programováním kvantových počítačů studenti seznamují a svůj algoritmus mohou otestovat v praxi například na kvantových počítačích Googlu, IBM nebo Amazonu. Jednou by tak kvantové počítače mohly například umožnit efektivnější přístup k nelineárním dynamickým systémům. To laicky znamená lepší možnosti řešení úloh stojících na teorii chaosu, patří sem například předpověď počasí, obtékání vzduchu kolem karoserie automobilu nebo simulace chování plazmatu ve fúzních reaktorech. Nicméně špičku mezi

algoritmy zatím představuje Shorův algoritmus, jenž by mohl umožnit rozkládat velká čísla na prvočísla v reálném čase.

Dnešní šifrování například bankovních transakcí se nespoléhá na to, že by jej principiálně nebylo možné prolomit, ale na to, že by to trvalo prohibitivně (neúnosně) dlouho. Zjednodušeně řečeno, šifrování využívá soukromý klíč, který představuje dvojice velice vysokých prvočísel, a veřejný klíč, tvořený součinem těchto prvočísel. Veřejným klíčem může kdokoli zašifrovat zprávu. Přečíst ji je ale možné pouze pomocí soukromého klíče. Najít z veřejného klíče soukromý klíč je sice možné, ale velmi složité, neboť je těžké součin prvočísel rozložit zpět na prvočísla. Běžnému počítači může trvat nalezení původních prvočísel stovky let. Pokud tedy hacker zná jen součin, nemá moc naději, že zabezpečení prolomí.

Pokud by ale disponoval dostatečně výkonným kvantovým počítačem a spustil na něm Shorův algoritmus, mohlo by mu k prolomení jakékoliv šifry stojící na tomto principu stačit pár sekund. Představa, že někdo takovou výpočetní silou už disponuje, a navíc nemusí mít zrovna přátelské úmysly, je proto pro mistry šifer noční můra. Zároveň jim ale rozvoj kvantových technologií dává zbraň, jak vytvořit principiálně neprolomitelné šifry. Je jí kvantový přenos klíče, který umožňuje sdílení tajného klíče pro šifrování a současné ověření jeho bezpečnosti.[4]

Čínští vědci tento měsíc oznámili, že se jim podařilo zprovoznit nejrozsáhlejší kvantovou síť, která umožňuje kvantový přenos klíče. Nabízí proto vyšší bezpečnost než současná internetová síť. Do kvantové sítě je napojeno na 150 uživatelů v podobě bank nebo úřadů, zajišťuje přenos dat až na vzdálenost 4600 kilometrů a součástí jsou kromě 700 pozemních optických kabelů i dvě linky mezi zemí a satelitem. Jde v podstatě o první stadium vývoje na cestě ke kvantovému internetu. O kvantovém internetu ve finální fázi ale bude možné mluvit až ve chvíli, kdy začne být využívána také kvantová teleportace informací. Ta zatím zůstává za dveřmi laboratoří.

Demonstrovat se ji podařilo například v roce 2016 na Calgarské univerzitě. Teleportace byla provedena na vzdálenost šesti kilometrů (udávána je jako délka optického vlákna), což byl tehdy rekord a mezi vědci byl vnímán jako velký úspěch. Ve zmiňovaném loňském experimentu už se přenos podařil na vzdálenost 44 kilometrů, a navíc byl stabilní.

Právě se stabilitou systému bývá jak u kvantových počítačů, tak kvantových sítí největší problém. Superpozice či kvantové provázání fotonů nebo elektronů dokáže narušit sebemenší šum. Proto se s částicemi pracuje ve vakuu nebo za extrémně nízkých teplot. U kvantových počítačů vede každý šum k chybám. Existující kvantové počítače navíc nemají korekci chyb. To je hlavní důvod, proč se zatím nepoužívají pro řešení praktických úloh. Úlohy použité pro dokázání kvantové nadřazenosti nejsou tak citlivé na chyby jako zmiňovaný Shorův algoritmus, takže je bylo možné demonstrovat i bez korekce chyb. Pro kvantové sítě je navíc jakékoliv narušení přenosu informace nerozlišitelné od vnějšího útoku. Schopnost udržet systém stabilní je naprosto klíčová, a proto je úspěch loňského experimentu v Calgary a Fermilabu tak významný.

Jak ale kvantová teleportace informací funguje? Nejdříve je potřeba vytvořit dvě vzájemně provázané částice, v aktuálním experimentu to byly fotony, ale může jít i o elektrony nebo atomy. Provázané částice se chovají jako jeden celek.[5] Provázané fotony mohou vzniknout například vyzářením fotonů z jednoho atomu. Po výrobě provázaných částic se jedna z částic vezme a pošle na místo, kam má být provedena teleportace.

První foton je tak v laboratořích Fermilabu a druhý foton je poslán do Calgary. Oba fotony zůstávají provázané a v superpozici.[6] Teleport je připravený. Druhým krokem je výroba třetího fotonu. Následně k fotonu ve Fermilabu přidáme tento třetí foton, který chceme teleportovat do Calgary. Na dvojici fotonů ve Fermilabu se provede speciální typ měření a výsledek se pošle do Calgary.[7]

Na základě této informace je možné foton v Calgary upravit tak, že se de facto stane kopií třetího fotonu, s nímž se ale sám fyzicky nikdy nesetkal. Došlo k teleportaci stavu třetího fotonu (informace), který ani vědci nemusí znát.

Znamená to několik věcí, teleportovat informace není možné vyšší rychlostí než rychlostí světla kvůli potřebě vytvořit teleport a také přenést výsledky měření do Calgary tradiční cestou.

Také to znamená, že teleportovat je možné pouze informace, nikoliv fyzické předměty. A nakonec se znovu vynořuje potřeba zajistit stabilní síť, přes niž je možné provázané částice distribuovat. Pozitivní naopak je, že kvantová teleportace umožňuje obejít problém mikrosvěta, kdy měření ovlivňuje stav dané částice, a není proto možné nikdy měřením zjistit o dané částici všechny informace. Tedy kdyby vědci chtěli prostým měřením získat informace k vytvoření přesné kopie molekuly nebo třeba kočky v daný okamžik, nikdy se jim to nepovede. Pokud by k tomu ale použili kvantové provázání a teleportaci, měli by šanci. Teleportovat lze totiž i neznámý stav. Pokud by existovalo zařízení schopné složit z atomů kočku, teleport by mu poskytl veškeré potřebné informace. Trochu nepříjemné ale je, že původní teleportovaný objekt by byl při procesu teleportace zničen.

Kvantová teleportace informací umožní, aby byl kvantový internet nebývale rychlý a zvenčí nenapadnutelný. To bude probíhat tak, že se mezi uživatele distribuují provázané částice. Sebemenší narušení částic při přenosu způsobí kolaps jejich provázání, útočník nic nevyčte a uživatel se o útoku dozví. Kvantové počítače zase přinesou pokrok v chemii, lékařství, ale i ve výzkumu vesmíru. Revoluce čeká i metrologii. Díky kvantovému provázání bude možné velmi přesně seřizovat GPS satelity nebo atomové hodiny. Vědci by mohli být schopni například měřit gravitační pole Země tak přesně, že by viděli i gravitační vlnění.

Bohužel postoj České republiky tomu podle Jexe neodpovídá. Financování výzkumu je v tomto směru tristní, a to i ve srovnání s okolními státy. Čína žene výzkum kupředu, protože si uvědomuje jeho strategický význam. Spojené státy zase drží na špičce výzkumu i soukromé firmy jako Google nebo IBM. Rozsáhle do tohoto výzkumu investují Rakušané, Britové, Švýcaři. Dobře si totiž uvědomují, jak fatální by bylo zaspat. Lidský kapitál přitom Česká republika má. Koneckonců, Čína dosáhla kvantové nadřazenosti díky algoritmu, za nímž stojí čeští vědci a jejich němečtí kolegové.

Text před vydáním několikrát pročetl tým profesora Igora Jexe a všechny faktické připomínky byly zapracovány.

** Představa zápisu qubitu v článku je pořád oproti realitě značně zjednodušená, neboť amplitudy α a β ve skutečnosti nemusí být reálná čísla jako třeba právě 0 a 1, nebo 0,6 a 0,8, nýbrž jde často o čísla komplexní. Komplexní čísla mají dvě části, imaginární a reálnou složku. Reálná složka je*

běžné číslo, například 2. Imaginární složka se pak značí jako násobek písmena i, kdy i odpovídá odmocnině z minus 1. Komplexní číslo tak může být například 2 + 3i. *Zpět*

[1] Pro spin je možné si kvantový stav představit geometricky - pomocí jednotkového vektoru (směru) na tzv. Blochově kouli. *Zpět*

[2] V zápisu $\alpha|00\rangle + \beta|11\rangle + \gamma|01\rangle + \delta|10\rangle$ se u popisovaného stavu rovnají koeficienty α a β nule, zůstává tak pouze část $\gamma|01\rangle + \delta|10\rangle$, kdy koeficient γ je roven δ, a proto lze zapsat uváděný provázaný stav jako $\gamma|01\rangle + \gamma|10\rangle$ nebo po úpravě jako $\gamma(|01\rangle + |10\rangle)$. *Zpět*

[3] Takto je to zjednodušené, ve skutečnosti z n qubitů není možné získat více než n bitů informace. Rozdíl mezi klasickým a kvantovým registrem n bitů/qubitů (registr je malé a rychlé úložiště dat, které používá procesor při své činnosti) můžeme popsat následovně. V klasickém případě nejsou možné superpozice, takže hodnota n-bitového registru je určena n bity. Naproti tomu n qubitů může být ve stavu superpozice 00... 0 až 11... 1. Těchto "bazických stavů" je celkem 2^n, takže k popisu stavu n qubitů je obecně potřeba 2^n amplitud. To na jednu stranu znamená, že simulovat, co dělá kvantový počítač (nebo obecně kvantový systém) na klasickém počítači je extrémně náročné (a náročnost roste exponenciálně s n). Simulovat kvantový počítač Sycamore s 53 qubity je na hraně možností nejvýkonnějších superpočítačů (mají dostatek operační paměti na to, aby se do ní vešlo všech 2^{53} amplitud), pro simulaci kvantového počítače s 60 qubity už bychom potřebovali alespoň 100x více operační paměti. Jsme tak výrazně za hranou kapacit klasických superpočítačů. Kvantová nadřazenost se ukazuje v plné síle. Na druhou stranu se nám může podařit navrhnout výpočet na kvantovém počítači tak, že amplitudy možností vedoucích ke správnému výsledku interferují konstruktivně (sčítají se a tím posilují), ostatní budou interferovat destruktivně (odečítají se a tím zeslabují), takže najdeme správné řešení s velkou pravděpodobností, a to podstatně rychleji (s výrazně menším počtem jistých elementárních operací) než na klasickém počítači. *Zpět*

[4] Šifrování probíhá "klasicky", pomocí sdíleného tajného jednorázového klíče. Kvantový je přenos klíče (1 bit klíče je zakódován např. do polarizace jednoho fotonu). Díky zákonitostem kvantové mechaniky lze vytvořit sdílený klíč a ověřit, jestli je bezpečný (nezná ho nikdo jiný než strany, které spolu chtějí tajně komunikovat). Využívají se především dva principy. Za prvé není možné "zkopírovat" neznámý stav kvantové částice (tj. např. polarizaci fotonu, do které je zapsán 1 bit klíče). Za druhé měření ovlivní stav částice (tj. není možné měřením určit neznámý kvantový stav, pokud máme k dispozici jen jednu částici - první měření nám neposkytne všechny informace o stavu, další měření nemá smysl dělat, protože stav se prvním měřením změnil). Pokud se k přenosu 1 bitu klíče použije 1 kvantová částice (typicky foton), pro útočníka není možné získat klíč "nepozorovaně", jeho vliv je možné odhalit. *Zpět*

[5] Přesněji lze říci, že jejich individuální vlastnosti jsou zcela potlačeny. *Zpět*

[6] Zmiňovaný experiment pracoval s fotony. Teleportaci kvantového stavu u hmotných částic (tedy i elektronů) se zatím povedlo ukázat jen na velmi malých vzdálenostech (milimetry). Prodloužení vzdáleností teleportace u hmotných částic na kilometry není příliš reálné, ale u fotonů to možné je. *Zpět*

[7] Přesněji jde o měření Bellova stavu, resp. měření v Bellově bázi. *Zpět*