Kvantový paralelismus a kvantové počítače

Limity v konstrukci počítačů

- **Mooreův zákon** říká, že přibližně **každých 18 měsíců se zdvojnásobuje počet tranzistorů**, které tvoří jeden čip
  - dnes se jich na **běžném čipu** tísní až **30 milionů**
  - dnešní **0,13 mikronová technologie** umožňuje propojovat **tranzistory** šířky **70nm**
  - obvykle se považuje **0,02 mikronová hranice** za mez v **klasické konstrukci počítačů** → mělo by být dosaženo kolem roku 2020
  - bude dosažena **hranice velikosti jednotlivých molekul a atomů**, tj. rozměrů kolem 0,1-0,5 nm
    - Na částicové úrovni přestávají platit jindy běžné fyzikální zákony makroskopického světa a na svém významu začíná nabývat **kvantová mechanika**

Kvantová mechanika

Kvantový stav

- **Kvantový stav** představuje v kvantové mechanice **reprezentaci fyzikální reality**, která má dvě části:
  - **část klasického světa**, která odpovídá tomu, jak se na tento svět díváme a jaký jej registrujeme
    - kvantový systém nabývá při měření (například energetická hladina elektronu v atomu vodíku nebo spin elektronu) pouze diskrétní hodnoty odpovídající skokům v celkové energii daného systému
  - druhou součástí je **kvantový svět**, který není přímo přístupný
    - můžeme z něj však pomocí aktu měření extrahovat určité informace
    - na kvantové úrovni mohou sledované veličiny nabývat nekonečně mnoho hodnot odpovídajících nekonečně mnoho kvantovým stavům

- Existuje **zásadní rozdíl** mezi **systémem**, na němž bylo **provedeno měření** a takovým, který je **izolován od okolí** a spojitě se vyvíjí

- Spojitý a deterministický vývoj kvantového systému v kvantové mechanice popisuje Schrödingerova vlnová rovnice, jejímž řešením je vlnová funkce **(φ_i)** odpovídající danému kvantovému systému
  - **kvantový systém** se však může skládat z více **vlnových funkcí**, o kterých říkáme, že jsou **v superpozici** – lineární kombinaci
  - **kvantový stav** **(ψ)** je vyjádřen jako **součet několika vlnových funkcí**:

$$|\psi\rangle = \sum_i \alpha_i \cdot |\varphi_i\rangle$$

    - Diracova notace vektoru: $\vec{x} \rightarrow |x\rangle$

- Každému stavu přísluší komplexní hodnota tzv. **amplituda pravděpodobnosti** (α_i)
  - jakým příspěvkem se podílí každá vlnová funkce (φ_i) na celkovém stavu
  - **druhá mocnina** její absolutní hodnoty udává, s jakou **pravděpodobností** bude **změřen každý z možných stavů**

$$\sum_i |\alpha_i|^2 = 1$$

Kvantový bit

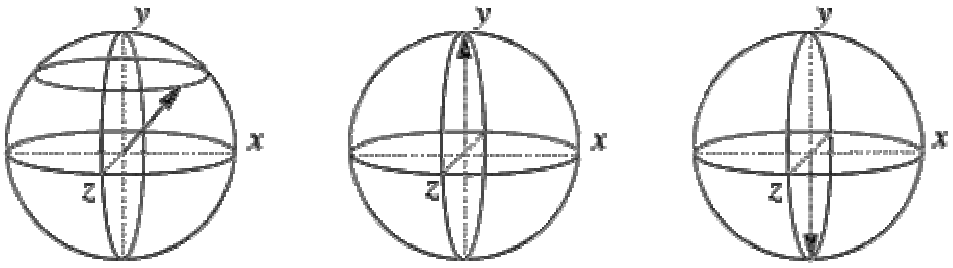
- Jak můžeme z kvantového systému **získat určitou informaci**?
  - Měření většinou provádíme tak, že vyšleme foton ke zkoumanému systému
  - Foton v podobě změny své energie unáší ze systému informaci, kterou zpětně detekujeme
  - Taková interakce fotonu s kvantovým systémem má však za následek tzv. **kolaps** (redukci) vlnové funkce, která náhodně přejde do jednoho z možných stavů složeného systému

- U klasických počítačů jsme zvyklí reprezentovat bit napěťovými úrovněmi, které dostatečně odlišují 0 od 1

- U kvantových bitů – **qubit** (*quantun bit*) je možné použít některý z dvoustavových kvantových systémů jako je například spin částice
  - lze si představit, že bity 0 a 1 zakódujeme pomocí jednoho a druhého spinového stavu
  - kromě klasických stavů $|0\rangle$ a $|1\rangle$ musíme uvažovat ale i libovolné superpozice stavu

$$\alpha_0 \cdot |0\rangle + \alpha_1 \cdot |1\rangle$$

    - pravděpodobnost zastoupení jednotlivých stavů je dána koeficienty α_0 a α_1
    - kvantový bit tak může existovat současně ve stavu 1 i 0



    - $|1\rangle$ je reprezentována jako vektor směřující k severnímu pólu, $|0\rangle$ k jižnímu
    - z úhlu, který vektor svírá se svislou osou je možné vyčíst poměrné zastoupení $|1\rangle$ a $|0\rangle$ ve stavovém vektoru

- **Kvantový bit** (qubit) existuje tedy ve třech stavech
  - logické 0, logické 1 a superpozice obou
  - Superpozice jednoho qubitu je dána dvěma numerickými koeficinty → **N-bitovému kvantovému stavu jich odpovídá 2^N**
  - ve všech možných stavech lze provádět paralelně příslušné operace

- **1 qubit:** $|\psi\rangle = \alpha_0 \cdot |0\rangle + \alpha_1 \cdot |1\rangle$

$$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \quad |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \quad |\psi\rangle = \begin{pmatrix} \alpha_0 \\ \alpha_1 \end{pmatrix}$$

- **2 qubity** - **direktní tenzorový součin** více stavů ($\otimes$)

$$|\psi_{ab}\rangle = |\psi_a\rangle \otimes |\psi_b\rangle = \begin{pmatrix} \alpha_{0a} \\ \alpha_{1a} \end{pmatrix} \otimes \begin{pmatrix} \alpha_{0b} \\ \alpha_{1b} \end{pmatrix} = \begin{pmatrix} \alpha_{0a} \cdot \alpha_{0b} \\ \alpha_{0a} \cdot \alpha_{1b} \\ \alpha_{1a} \cdot \alpha_{0b} \\ \alpha_{1a} \cdot \alpha_{1b} \end{pmatrix} = \begin{pmatrix} \alpha_{00} \\ \alpha_{01} \\ \alpha_{10} \\ \alpha_{11} \end{pmatrix}$$

$$|00\rangle = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} \quad |01\rangle = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix} \quad |10\rangle = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix} \quad |11\rangle = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix}$$

- **n-bitový** kvantový registr → **2^n amplitud zároveň**

Propletené qubity

- Předpokládali jsme, že vždy jsou na sobě jednotlivé **qubity zcela nezávislé**
- Můžeme připravit registr, jenž nelze vyjádřit jako tenzorový součin dílčích qubitů → říkáme, že jsou **qubity propleteny** *(entangled)*
  - propletení je stav, ve kterém jsou qubity na sobě v nějakém smyslu závislé (jejich stavy jsou přes určitý atribut korelovány)
  - konkrétně provedením měření na jednom qubitu víme (již bez měření), jaká je hodnota druhého qubitu
- Možné případy pro propletené qubity lze vyjádřit pomocí pravděpodobností jako:

$$p(|\psi_a\rangle = 0 | |\psi_b\rangle = 0) = 1$$
$$p(|\psi_a\rangle = 0 | |\psi_b\rangle = 1) = 0$$
$$p(|\psi_a\rangle = 1 | |\psi_b\rangle = 0) = 0$$
$$p(|\psi_a\rangle = 1 | |\psi_b\rangle = 1) = 1$$

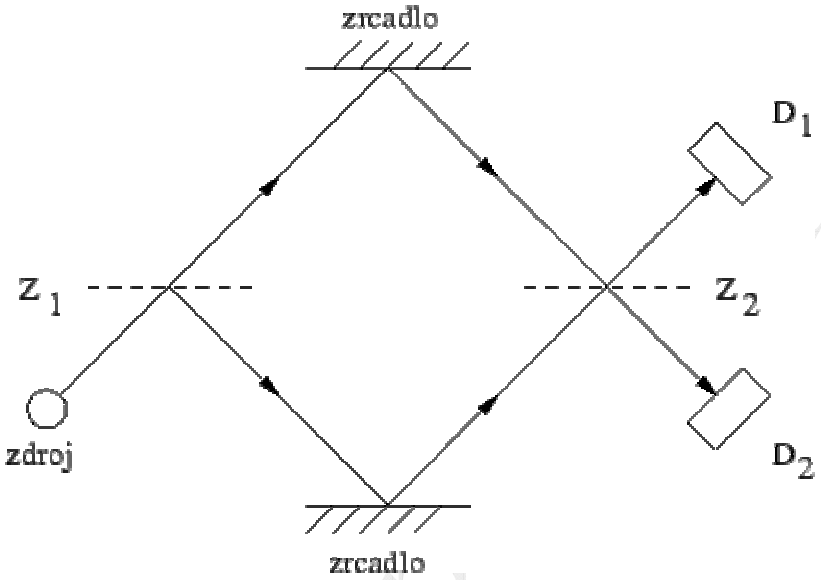
- Propletení dvou qubitů lze pak vyjádřit:

$$|\psi_{ab}\rangle = \frac{1}{\sqrt{2}}\left(|00\rangle + |11\rangle\right)$$
$$|\psi_{ab}\rangle = \frac{1}{\sqrt{2}}\left(|01\rangle + |10\rangle\right)$$

- Měřením se propletení rozpadá a oba qubity nabývají klasických hodnot

Kvantová interference

- **Machův-Zehnderův interferometr**
  - zdrojem vygenerovaný foton má možnost projít více (dvěmi) experimentálními cestami
  - přístroj se skládá ze zdroje fotonů světla, dvou klasických zrcadel, dvou polopropustných zrcadel (které polovinu intenzity světla propouští a druhou odráží) a dvou detektorů



  - Polopropustná zrcadla jsou navržena tak, že pokud se na nich paprsek láme, pak se **fáze jeho vlny posune o 1/4 vlnové délky (λ)**
  - Pokud vyšleme ze zdroje **spojité světlo**, je rozděleno prvním polopropustným zrcadlem Z_1 na dvě části
    - Část, která prochází spodní větví je posunuta o λ/4; při průchodu polopropustným zrcadlem Z_2 ve směru detektoru D_2 je to již o λ/2
  - V této chvíli ale potká neposunutou vlnu světla z horní větve
  - V takovém případě dochází ke klasické interferenci dvou vln
    - Kvůli posunutí jedné vlny o λ/2 je tato **interference destruktivní** a na detektoru D_2 nic nenaměříme
    - Druhá část rozděleného světla se naopak v obou větvích posune po jednom odrazu shodně o λ/4 a za zrcadlem Z_2 dojde ke **konstruktivní interferenci**, takže celou intenzitu zdrojového světla registrujeme jen na detektoru D_1

- Co se však stane, vyšleme-li z generátoru **pouze jediný foton**?
  - Na předchozím výsledku se nic nemění a foton vždy registrujeme v detektoru D_1
    - to je možné vysvětlit pouze jediným způsobem - **foton musel projít oběma rameny současně** a na zrcadle Z_2 interferovat sám se sebou - ve směru detektoru D_1 konstruktivně a ve směru D_2 destruktivně

- V případě, že ale odstraníme zrcadlo Z_2, nemá elektron na čem interferovat a my jej po odraze na zrcadle Z_1 naměříme se stejnou pravděpodobností buď na detektoru D_1 nebo D_2

- Tento experiment dobře potvrzuje nedělitelnou vlastnost kvantových systémů - jejich **vlnově-částicovou dualitu**
  - S klasickým myšlením bychom chtěli mezi oběmi povahami částic rozlišovat, v kvantově mechanickém světě to však není možné
  - Dualizmus však uvažujeme do chvíle kolapsu vlnové funkce → potom si již musíme vybrat jen jednu možnost

- **Interference** má v kvantovém počítání rozhodující význam při získávání **výsledku z kvantového registru**
  - Podobně jako se elektronové vlny navzájem interferenčně skládaly, dochází také mezi jednotlivými qubity registru ke vzájemným interferenčním působením, což má za následek úpravy amplitud pravděpodobností stavů v superpozici
  - To umožňuje příznivé stavy (správná řešení) zvýraznit (konstruktivní interference) a nepříznivé potlačit (destruktivní interference)

Teleportace qubitu

- **Heisenbergův princip neurčitosti** nedovoluje změřit přesně všechny charakteristiky kvantového systému současně → nebylo by možné získat informaci o celém kvantovém systému před tím, než bychom jej přenesli.

- **Teleportace stavu** kvantového systému s využitím fenoménu propletení kvantových stavů
  - Fyzikálně mají propletené částice korelován nějaký atribut, který se při jejich vzniku zachovává (spin nebo polarizace)
    - Jestliže má jedna částice spin nahoru, pak druhá má s jistotou spin dolů a naopak
  - Při měření na jedné částici dojde ke kolapsu vlnové funkce systému v celém prostoru a k přechodu do jednoho z možných vlastních stavů
    - Tím se jednoznačně určí, která z částic má spin dolů a která nahoru
  - Je s podivem, že lze bez přítomnosti výměnných částic ovlivňovat částici, která je třeba na opačné straně vesmíru
    - Tento problém byl později nazván **EPR** (Albert Einstein, Boris Podolsky, Nathan Rosen) **paradox**
  - Fyzikové dokázali, že obě částice nabývají hodnoty daného atributu až v momentě měření a náhodného přechodu do vlastního stavu korelovaného se stavem druhé částice
    - stavu propletení se také jinak říká EPR stav nebo EPR efekt

- Předpokládejme, že Alice má nějakou částici **A v neznámém kvantovém stavu** a chce tento stav poslat Bobovi
  - Víme, že změřit částici nemůže, protože by tím křehký kvantový stav porušila. Jediné co ji zbývá, je stav teleportovat
    - K tomu ale bude muset využít triku s propletením stavů částic
  - Nejprve si Alice a Bob připraví **propletený EPR pár** dvou částic **B** a **C**
    - Alice si z tohoto páru ponechá částici **B**, Bobovi zašle částici **C**

- Alice pak **spojí** svoji částici **A** a **propletený pár** do systému tří částic
- K provedení teleportace musí nyní Alice provést **měření na sloučeném stavu** obou částic (**A** a **B**)
  - Protože jsou však částice propleteny, změní se přitom projekcí i stav Bobovy částice
  - Alice svým měřením prvních dvou qubitů neodkryla nic konkrétního o stavu částice **A**
  - Místo toho pouze odhalila, kterou kombinaci sloučených stavů všech tři částic u sebe má
- V tuto chvíli má u sebe Bob jeden ze čtyř možných teleportovaných stavů
  - Pouze v jednom případě jsou však správně zachovány amplitudy, ostatní výsledky jsou různě rotovány
  - Alice s Bobem spojí klasickým komunikačním kanálem a sdělí mu, jaký výsledek naměřila
  - Bob tuto klasickou (2-bitovou) informaci použije k tomu, aby na stav částice **C** aplikoval příslušnou rotaci

Shrnutí kvantové mechaniky

- Nejdůležitější **poznatky kvantové mechaniky**, které se uplatňují **v kvantové informatice**

  - **Superpozice**
    - Kvantový stav se může nacházet v superpozici, která je součtem příspěvků více vlastních stavů, které odpovídají vlastním vlnovým funkcím
    - umožňuje **masivní kvantový paralelismus**, který je příčinou exponenciálního zrychlení některých algoritmů

  - **Interference**
    - umožňuje měnit amplitudy pravděpodobností vlastních stavů tak, že stav odpovídající řešení má co nejvyšší klasickou pravděpodobnost následného změření

  - **Propletení**
    - vlastnost kvantových systémů, které mohou existovat ve stavu, jenž nelze vyjádřit jako tenzorový součin jeho složek
    - propletení má nelokální povahu a využívá se například u kvantové teleportace nebo u superhustého kódování

Kvantová informatika

Kvantové obvody

- Aby bylo možné **kvantový systém** udržet v nenarušeném stavu (koherenci), je zapotřebí jej (v ideálním případě) **zcela izolovat od okolí**
  - Takovému systému tím znemožníme, aby si s okolím vyměňoval například teplo nebo s ním jinak přímo interagoval

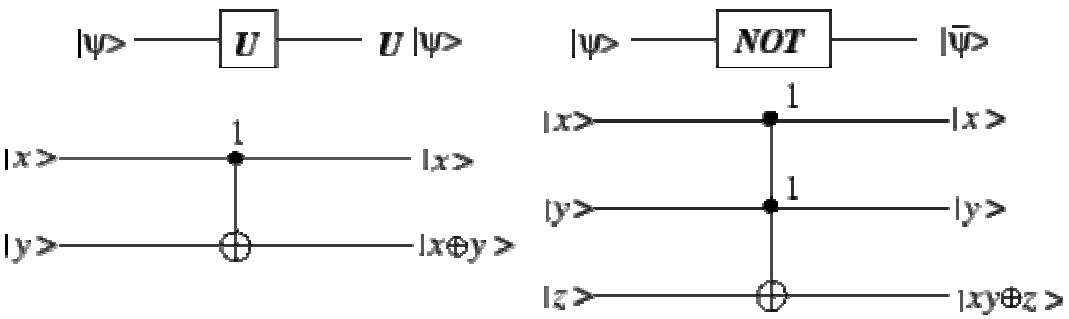
- **Landauerův princip** nám říká, že ke smazání jednoho bitu informace z paměti je zapotřebí ze systému vyvést jeden bit entropie
  - To se obvykle projevuje vyzářením tepla do okolí
  - Jelikož je při svém vývoji kvantový systém izolován od okolí, nemůže z něj žádná informace volně unikat

- V klasickém počítači, složeném z **klasických bran** jako je **AND**, **NAND** či **OR**, není vždy reverzibilita mezi vstupy a výstupy zachována
  - Například u klasického výpočtu víme, že lze libovolnou logickou funkci kombinačního obvodu realizovat pouze použitím univerzální brány **NAND**
  - Tato brána má ale pro použití u kvantových počítačů tu nevýhodu, že z výstupů nelze jednoznačně určit kombinaci vstupů - brána **NAND** tedy **není reverzibilní**
  - V takovém procesu se **ztrácí část informace** a systém se tím zahřívá

- U kvantových počítačů ale můžeme používat jen ty brány, které podmínku reverzibility (a tím i unitárnosti operací) splňují
  - Jako první nás asi napadne brána **NOT**
  - Podobně jsou na tom i brány **CNOT** a **CCNOT**

brána	jiný název	qubity	funkce
NOT		1	$\|x\rangle \rightarrow \|\bar{x}\rangle$
CNOT	controlled *NOT*, *XOR*	2	$\|x,y\rangle \rightarrow \|x, x \oplus y\rangle$
CCNOT	controlled-controlled *NOT*, Toffoliho brána	3	$\|x,y,z\rangle \rightarrow \|x, y, xy \oplus z\rangle$

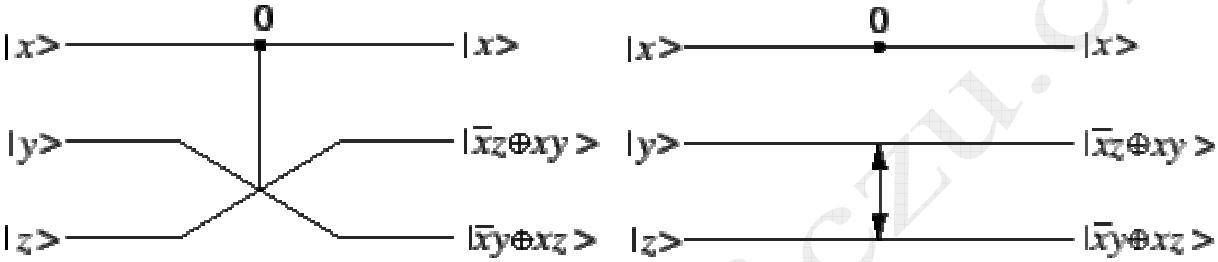
- **Bránové operace** na qubitech se v kvantové informatice obvykle zapisují pomocí kvantových obvodů, které se **v čase vyvíjí zleva doprava** a každá **vodorovná hrana** (drát) **odpovídá jednomu qubitu**



- brána **CNOT** a **CCNOT**
  - Tyto brány mají jako **kontrolní qubit 1**. To znamená, že pokud jsou například u brány *CCNOT* oba qubity **x** a **y** rovny 1, provede se operace na qubitu **z**

- Jinou důležitou kvantovou bránou je **Fredkinova brána**
  - **prohodí druhý a třetí bit v případě, že první bit je 0**
  - i zde je podmíněno provedení operace stavem určitého bitu → **podmíněná kvantové brány**
  - jedná se o univerzální bránu – může realizovat libovolný kombinační obvod
  - realizuje funkci:

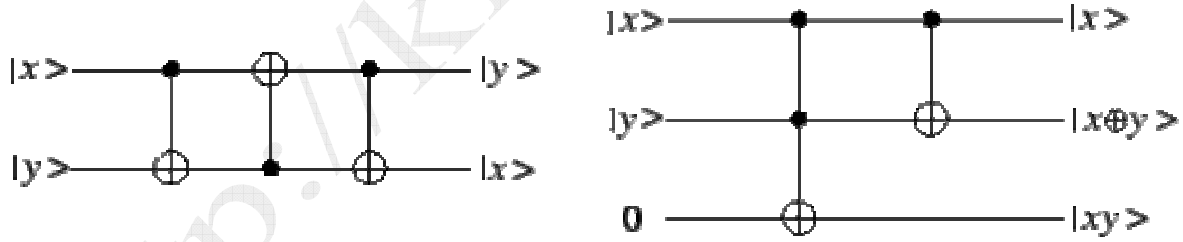
$$|x, y, z\rangle \rightarrow |x, \bar{x}z \oplus xy, \bar{x}y \oplus xz\rangle$$



- Další užitečnou bránou je **SWAP**
  - spolu prohazuje 2 qubity a provádí tak funkci: $|x, y\rangle \rightarrow |y, x\rangle$

- Z univerzálních bran je možné konstruovat obvody různých funkcí a složitostí
  - např. 2-qubitovou sčítačku (2.qubit obsahuje sumu a 3. přenos)

$$|x, y, 0\rangle \rightarrow |x, x \oplus y, xy\rangle$$



Kvantové algoritmy

- **Kvantová Fourierova transformace**
  - Fourierova transformace mapuje funkce v časové doméně na funkce frekvenčního spektra
  - Její hlavní vlastností z pohledu kvantové mechaniky je, že mezi qubity vyvolává kvantovou interferenci, která je buď konstruktivní nebo destruktivní
  - Konstruktivní interference v signálu zvýrazňuje jisté charakteristiky (frekvence) nad charakteristikami jinými

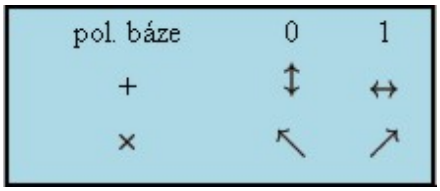
Kryptografie

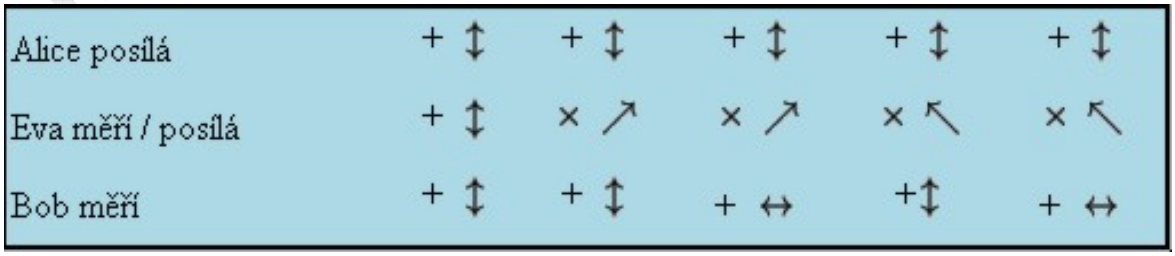
- Jedním ze základních algoritmů je tzv. **One-time pad**
  - Pokud chtějí dvě strany (Alice a Bob) komunikovat, je zapotřebí se předtím sejít a dohodnout si (náhodně vygenerovat) několik sad tajných klíčů, které budou při komunikaci potřeba
  - Tento druh algoritmu je zajímavý tím, že u něj lze za předpokladu kvalitního zdroje klíčů dokázat tzv. **nepodmíněnou bezpečnost**, to znamená odolnost vůči luštění bez ohledu na výpočetní sílu útočníka
  - Nevýhodou tohoto algoritmu je, že klíč je možné použít jen jednou - vzniká zde tedy problém s bezpečným přenosem klíče

- **Kryptosystém RSA** (který v roce 1978 vymysleli Ronald Rivest, Adi Shamir a Leonard Adlemann) je založen na problému faktorizace velkých čísel (rozkladu na prvočinitele – obvykle velká prvočísla)
  - Nejprve musí přijímající strana (v tomto případě Bob) vygenerovat pár klíčů, z nichž jeden je tzv. **veřejný klíč**, který je k dispozici všem a Bob jej sdělí veřejným kanálem Alici
  - Alice tímto klíčem zprávu zašifruje
  - V této chvíli přichází na řadu druhý klíč - **privátní**, který Bob nikomu nesdělil
  - Alice pošle zašifrovanou zprávu Bobovi, který si ji svým privátním klíčem dešifruje
  - Aby to však bylo možné, je nutné, aby byly oba klíčem určitým způsobem propojeny

- Jak si s **prolomením metody RSA** poradí kvantový počítač?
  - může totiž využít kvantového paralelismu
  - např. algoritmus **Petera Shora** na faktorizaci velkých celých čísel **snižuje exponenciální složitost** (klasickým způsobem) na pouze **polynomální**

- **Kvantová kryptografie**
  - např. zaměření se na bezpečný přenos klíče a použití klasického algoritmu (One-time pad)
  - BB84 protokol – přenos pomocí polarizace fotonů
  - při „odposlouchávání“ dojde ke změně polarizace a odhalení





Kvantové procesory a počítače

- **Výhoda kvantového počítače**
  - jakákoliv operace s qubitem se vykoná současně s oběmi jeho hypotetickými hodnotami
  - s rostoucím počtem qubitů se exponenciálně zvětšuje tzv. **kvantový paralelismus**
  - některé druhy výpočtů lze tím řádově urychlit

- **Nevýhoda kvantového počítače**
  - pokud je quibit ve stavu superpozice, je stabilní
  - **jakákoliv interakce s okolím** – měření, detekce stavu – má ale za následek **náhodný rozpad** do jednoho ze stavů
    - pravděpodobnost stavu je dána α_0^2 a α_1^2

- Jak zjistit správné heslo, jestliže víme, že je obsaženo ve známé množině 10^9 hesel?
  - **klasický počítač** (Von Neumann)
    - sekvenční vkládání 10^9 hesel (1, 2, … 10^9) a čekání na objevení správného hesla
    - časově velmi náročné
  - **více počítačů**
    - nastavení 10^9 počítačů na jedno heslo
    - výsledek znám okamžitě, technicky neproveditelné
  - **kvantový počítač**
    - stačí jeden kvantový počítač s paralelně uloženou maticí všech 10^9 hesel (superpozice)
    - výsledek znám okamžitě, ale zatím jen teoreticky

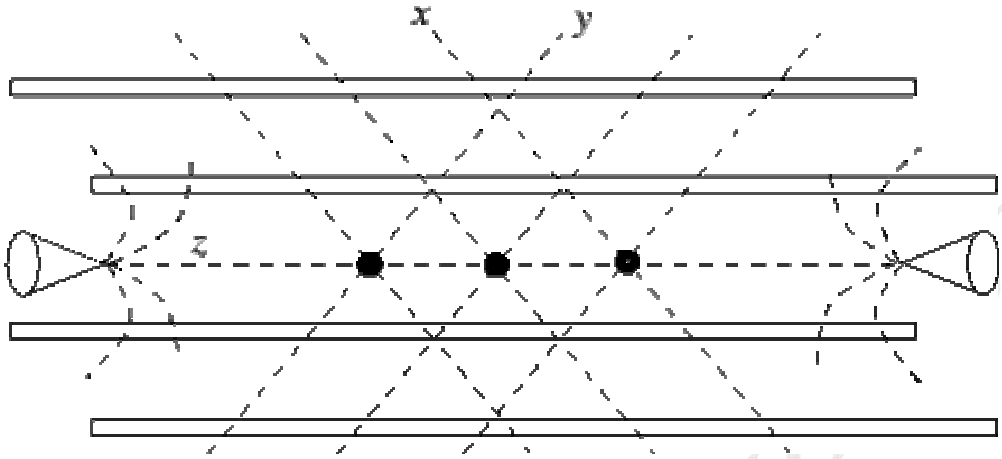
Kvantové procesory

- Vědci se snaží na bázi dnešních technologií konstruovat **první ovladatelné kvantové systémy**, které by bylo možno alespoň vzdáleně považovat za předchůdce kvantových počítačů

- Při konstrukci **budeme především chtít**
  - aby byl náš procesor **dostatečně jednoduchý** na ovládání
  - aby byl zároveň **dostatečně** (dlouho) **izolovatelný** od okolí
  - aby byl schopen pojmout **dostatečný objem informací**

- **Iontová past**
  - Uvěznění iontů v prostoru tak, aby co nejméně vzájemně působily s okolím, a tím prodloužily dobu koherence systému
  - Aparatura se skládá ze čtyř podélných elektrod uvězňujících ionty ve směrech **x** a **y** a dvou menších, které znemožňují iontům pohyb mimo aparaturu v ose **z**
  - Nyní máme několik iontů připraveno k provádění operací - počet uvězněných iontů (max. desítky) odpovídá šířce kvantového registru
  - Operace se provádí zaměřením laseru (pulsem) na iont, který koherentně změní stav iontu

- Čtení se provádí tak, že mu laserem dodáme energii, která způsobí přechod mezi $|0\rangle$ stavem a vyšším vybuzeným stavem, který není stabilní a rychle se vrací na $|0\rangle$
  - Pokud byla hodnota qubitu právě $|0\rangle$, pak iont vyzáří příslušný foton, kdežto qubit ve stavu $|1\rangle$ zůstane temný



- **Slabiny**
  - počet iontů je omezen asi na stovce
  - technika pokusu je velmi náročná (vakuum, chlazení, ovládání laserem)
  - dekoherující ionty nelze vracet do koherentního stavu

Nukleární magnetická rezonance – NMR

- U uvězněných iontů jsme ovlivňovali pokaždé jen jeden qubit a měřili jeho vlastní stav
- NMR místo toho využívá velkého počtu jedno-molekulových kvantových počítačů, jejichž měřením obdržíme střední hodnotu výsledku
- Tyto molekuly tvoří kapalinu, která je uzavřena v nádobě obsahující asi 10^{22} molekul
- NMR používá ke kódování qubitů spinové stavy jader atomů, které jsou elektronovým mrakem dobře od okolí izolovány a samotné jádro zabírá v porovnání s celým atomem minimální objem
- Každé jádro navíc tvoří určitý magnetický dipól a chová se tak jako malý magnet
- Pokud na kapalinu aplikujeme vnější magnetické pole, nastaví se spiny ve dvou možných směrech: paralelním nebo anti-paralelním vzhledem k orientaci pole. To odpovídá hodnotám qubitu $|0\rangle$ a $|1\rangle$
- Pokud k vnějšímu poli přidáme působení pomocí elektromagnetického pole s radiovými frekvencemi, pak je možné stavy spinů jemně upravovat a vytvářet tak superpozice stavů
- Protože nikdo není schopen ovlivňovat ani měřit stavy jednotlivých jader, je zapotřebí měřit průměrný spinový stav v celém objemu kapaliny
- Do tohoto průměrného stavu vlastně kódujeme jednotlivé qubity, jejichž stavy ovládáme externími poli
- Různé spinové stavy vyvolávají po odečtu pomocí NMR různá NMR-spektra, která prozrazují stav qubitů
- Pro logické operace zahrnující více qubitů, je zapotřebí měnit energie atomů tak, aby v molekulách docházelo k tzv. **spinovým vazbám** *(spin-spin coupling)*, které umožňují ovlivňovat sousední atomy a tím implementovat například operaci **CNOT**

- **Nukleární magnetická rezonance – omezení**
  - velikost použitelných molekul a tím i složitost možných operací je technologicky omezena
  - technologie je velmi špatně škálovatelná - objem kapaliny roste exponenciálně s větším počtem qubitů (několik desítek qubitů je zřejmě maximum)
  - obtížná příprava počátečního stavu

Budoucnost kvantových počítačů

- Přestože se zdá, že současné technologické problémy zatím nedovolují plně rozvinout potenciál kvantové informatiky, je možné s nadějí prohlásit, že budoucnost kvantových počítačů vypadá slibně

1982: Richard Feynman - navrhl použití kvantových systémů k výpočtům
1984: Charles Bennett a Gilles Brassard - komunikační protokol BB84
1985: David Deutsch - kvantový Turingův stroj
1994: Peter Shor - faktorizační algoritmus
1995: poslána zpráva kvantovým kanálem
1996: Lov Grover - vyhledávací algoritmus
1996: Peter Shor a Andrew Steane - kvantová oprava chyb možná
1997: uskutečněna kvantová teleportace
1999: Richard Huges - iontové pasti s desítkami qubitů
2000: v Los Alamos byl vytvořen 7-qubitový NMR počítač
2000: společnost IBM ohlásila vytvoření 5-qubitového NMR počítače

- Efekt tzv. **kvantového přízraku** *(quantum mirage)*
  - na měděné destičce je umístěno ve tvaru elipsy 36 atomů kobaltu tvořících tzv. **kvantovou hradbu** *(quantum corral)*
    - Tato hradba působí na elektronová mračna v destičce mědi uvnitř elipsy atomů kobaltu
  - Když byl do jednoho ohniska elipsy umístěn další atom kobaltu, začal interagovat s vlnami elektronů v destičce
  - Stejně ale elektrony působily na okolí v druhém ohnisku elipsy a vytvářely tam jakousi **kopii (přízrak) atomu kobaltu o třetinové intenzitě**, přestože tam žádný nebyl předtím umístěn
  - Tento efekt může mít v principu vliv na přenos informace mezi dvěma místy (například v kvantovém procesoru)