Optické kvantové zpracování informace

L. Čelechovská, M. Dušek, H. Fikerová, R. Filip, M. Gajdacz, M. Gavenda, Z. Hradil, M. Ježek, P. Marek, M. Mičuda, M. Miková, L. Mišta, T. Opatrný, L. Slodička, I. Straka,V. Usenko, J. Fiurášek

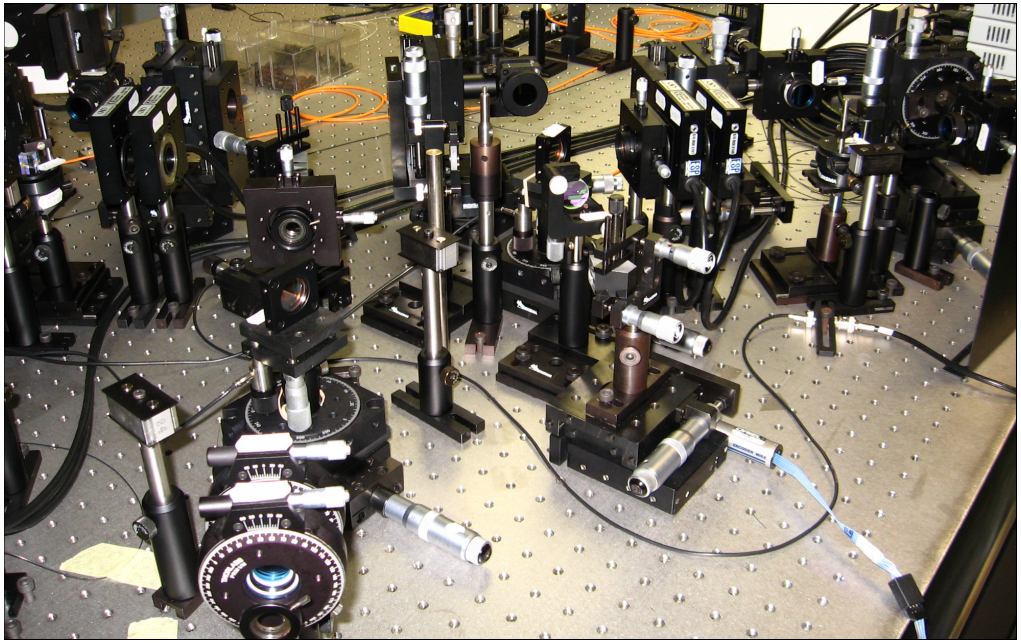
Katedra optiky, Univerzita Palackého, tř. 17. listopadu 12, 77146 Olomouc, Česká republika

Tato prezentace je spolufinancována Evropským sociálním fondem a státním rozpočtem České republiky.

Kvantová fyzika a zpracování informace

- Donedávna se o informaci uvažovalo jen v pojmech klasické fyziky.
- Kvantová mechanika hrála jen podpůrnou roli.
- Informace je fyzikální (její zpracování je závislé na fyzikálním systému, v nemž je zakódována).
- Kvantové systémy se chovají jinak než klasické (podivuhodněji).
- Využití kvantových jevů nabízí řešení některých problémů neřešitelných v rámci klasické teorie informace.

Kvantové zpracování informace



Klasický bit:

$$0, 1$$

Kvantový bit:

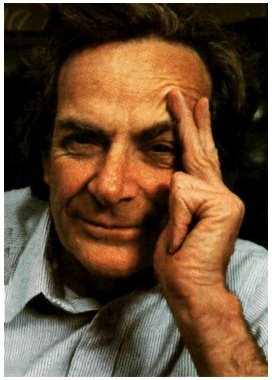
$$\alpha|0\rangle + \beta|1\rangle$$

Nové paradigma:

- **Využití zákonů kvantové fyziky pro zpracování a přenos informace**
- **Informace uložena do kvantových stavů světla či atomů**
- **Princip superpozice -> kvantový paralelismus**

Hlavní aplikace

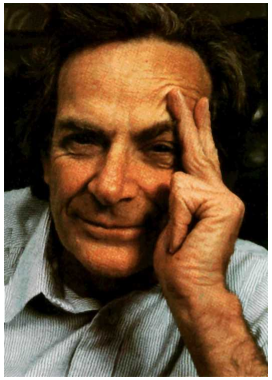
Kvantový počítač



- simulace kvantových systémů (R.P. Feynman)
- Exponenciální zrychlení výpočtu oproti klasickým algoritmům (P. Shor, faktorizace)

Hlavní aplikace

Kvantový počítač



- simulace kvantových systémů (R.P. Feynman)
- Exponenciální zrychlení výpočtu oproti klasickým algoritmům (P. Shor, faktorizace)

Kvantová komunikace

- kvantová distribuce tajného klíče (Ch. Bennett and G. Brassard)
- kvantový generátor náhodných čísel

Plán přednášky

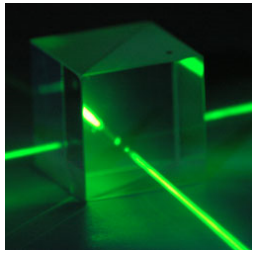
I. Kvantová fyzika

II. Kvantové počítače

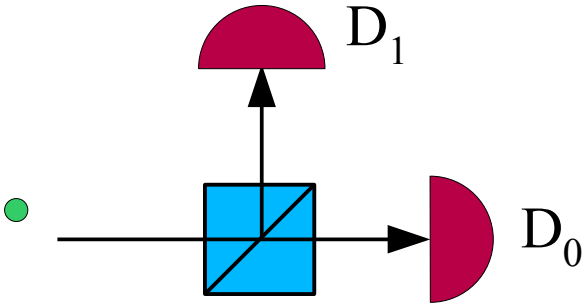
III. Kvantová kryptografie

I. Kvantová fyzika

Kvantové měření, náhoda a statistika



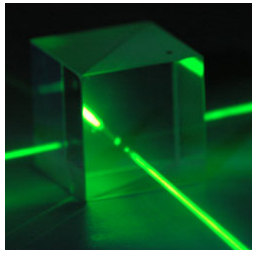
dělič svazku



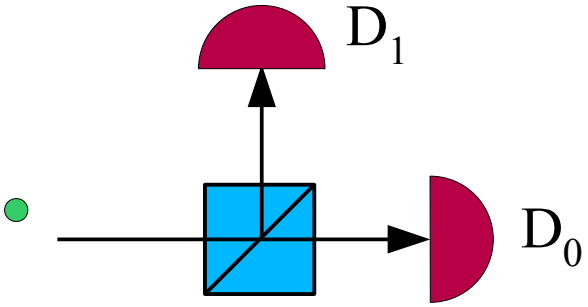
jednofotonový detektor

Dělič svazku s propustností T

Kvantové měření, náhoda a statistika



dělič svazku



jednofotonový detektor

Dělič svazku s propustností T:

$$p_0 = T \qquad p_1 = 1 - T$$

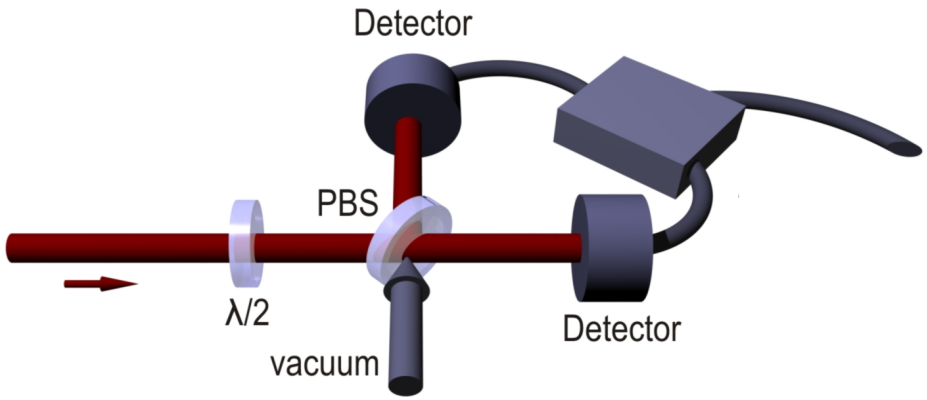
$$p_0 + p_1 = 1$$

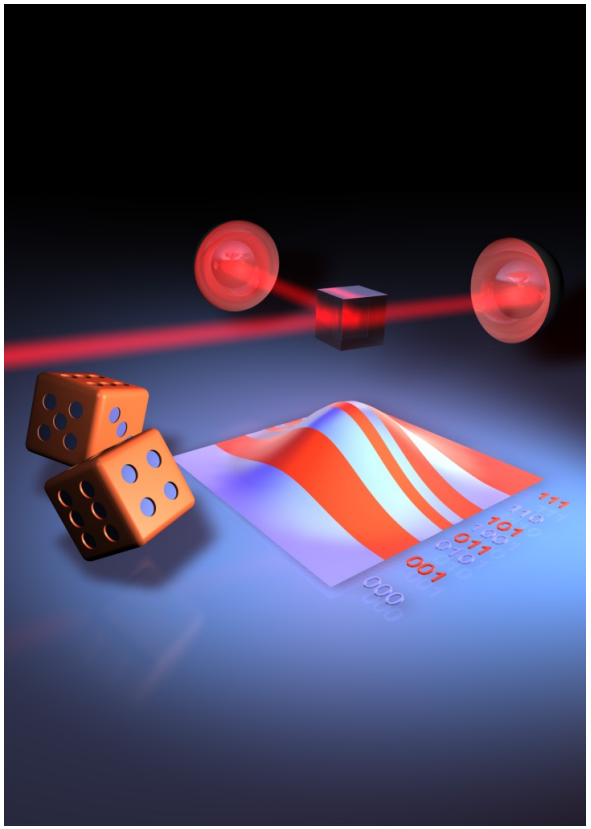
Výsledek kvantového měření je fundamentálně náhodný jev.

Proces měření ovlivňuje stav měřeného kvantového systému

→ kolaps vlnové funkce

Kvantový generátor náhodných čísel

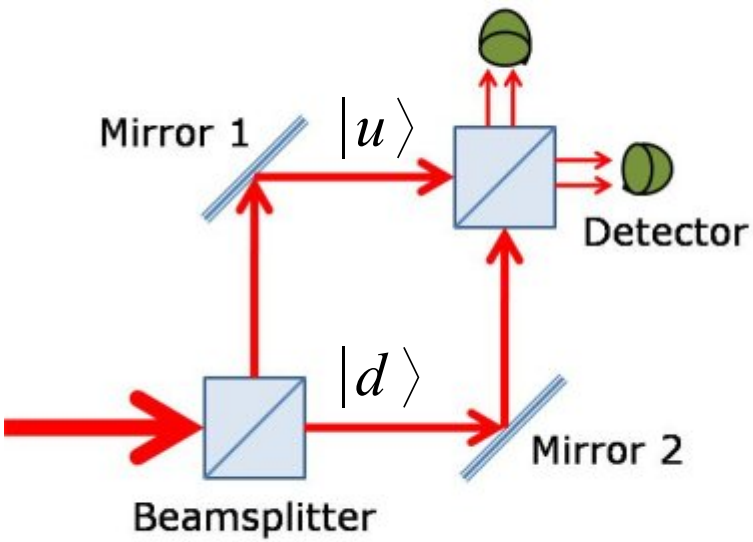




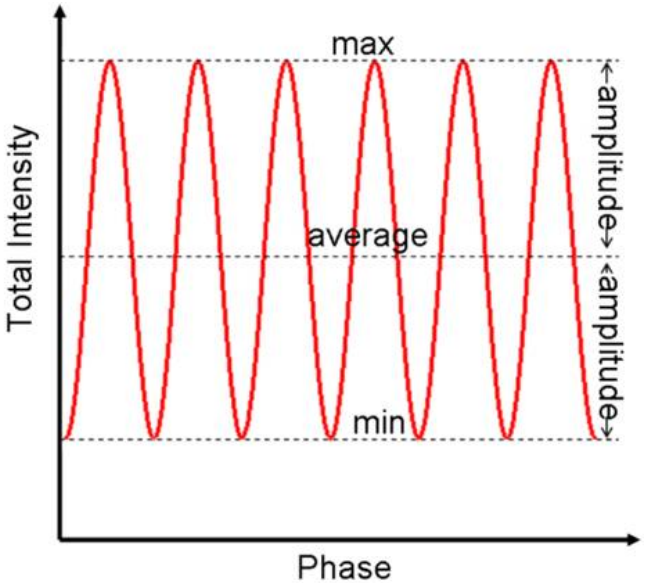
Náhodnost sekvence generovaných bitů garantována zákony kvantové fyziky.

Komerčně dostupný produkt – firma ID Quantique.

Kvantová interference a princip superpozice

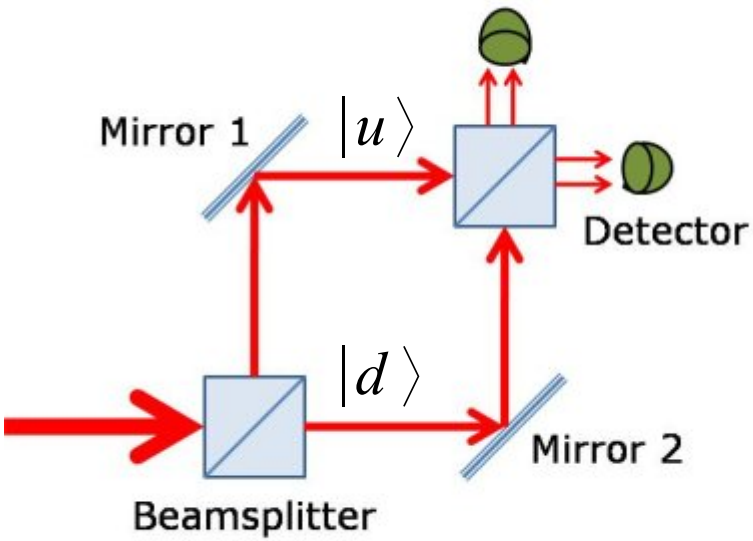


Mach-Zehnderův interferometr

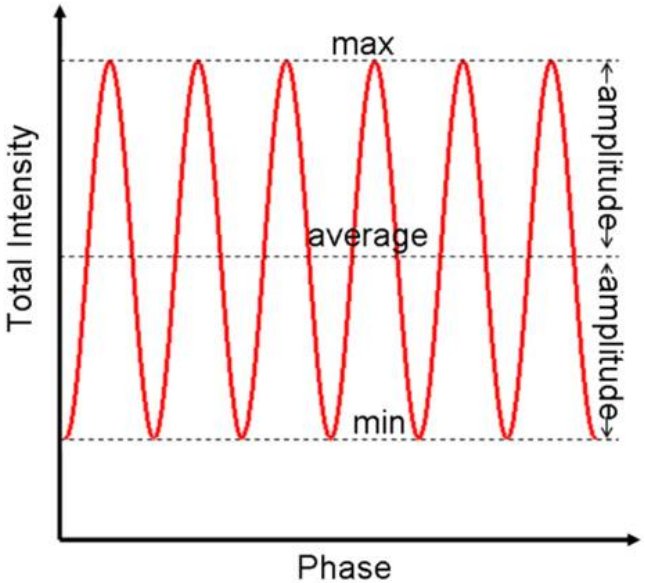


Interferenční proužky

Kvantová interference a princip superpozice



Mach-Zehnderův interferometr



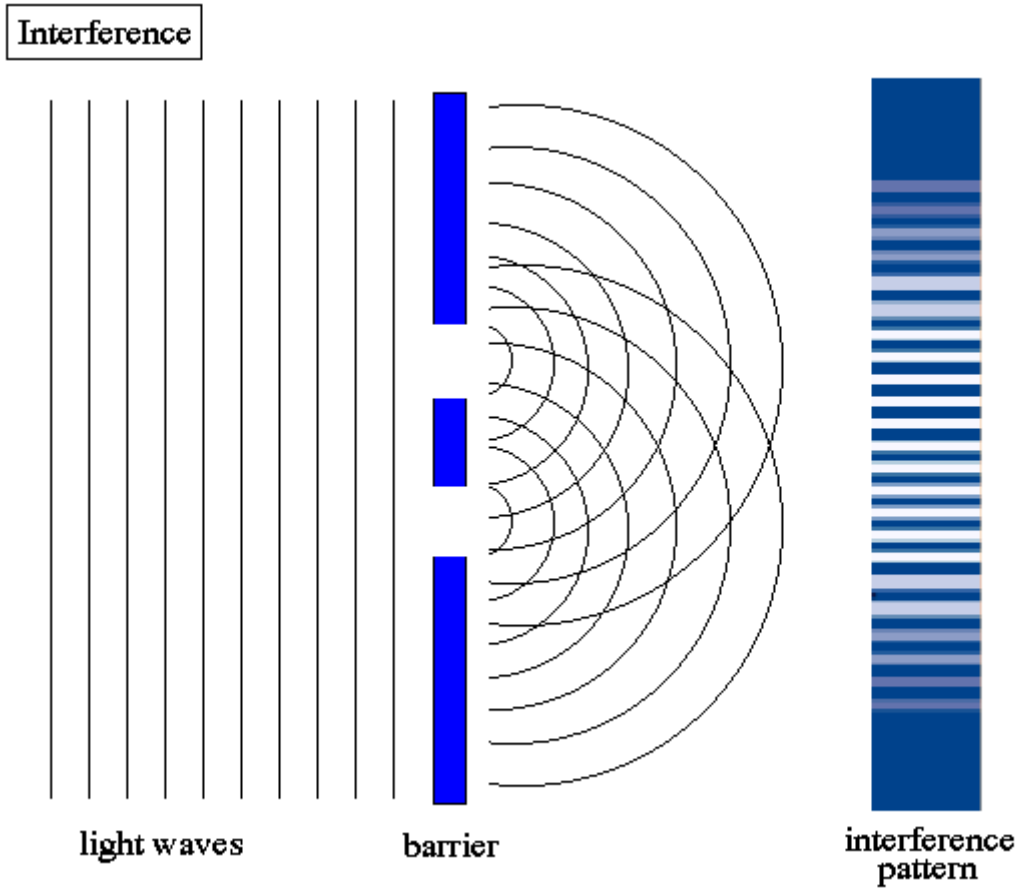
Interferenční proužky

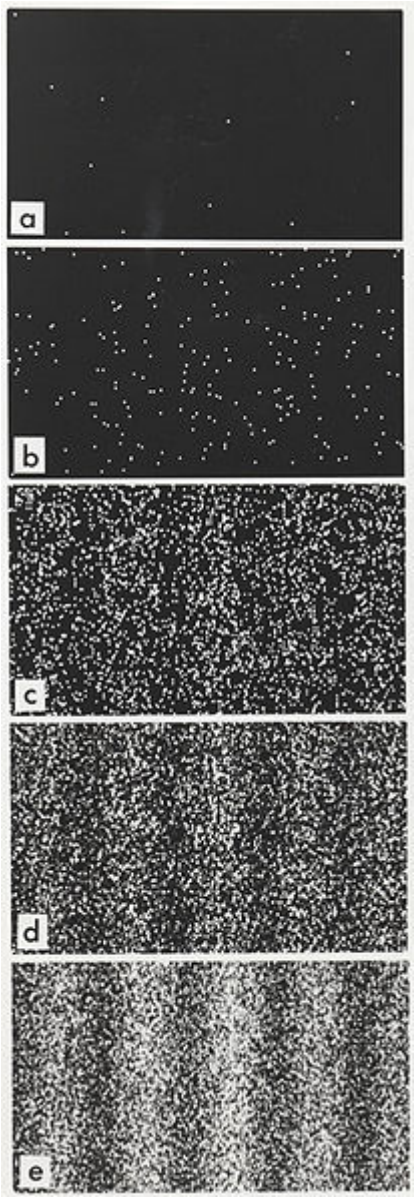
Foton se současně šíří oběma rameny interferometru

$$|\psi\rangle = \frac{1}{\sqrt{2}}(|u\rangle + |d\rangle)$$

Kvantová superpozice.

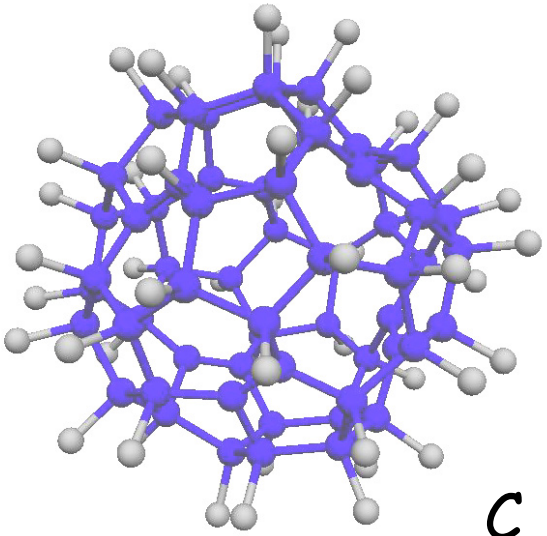
Kvantová interference a princip superpozice



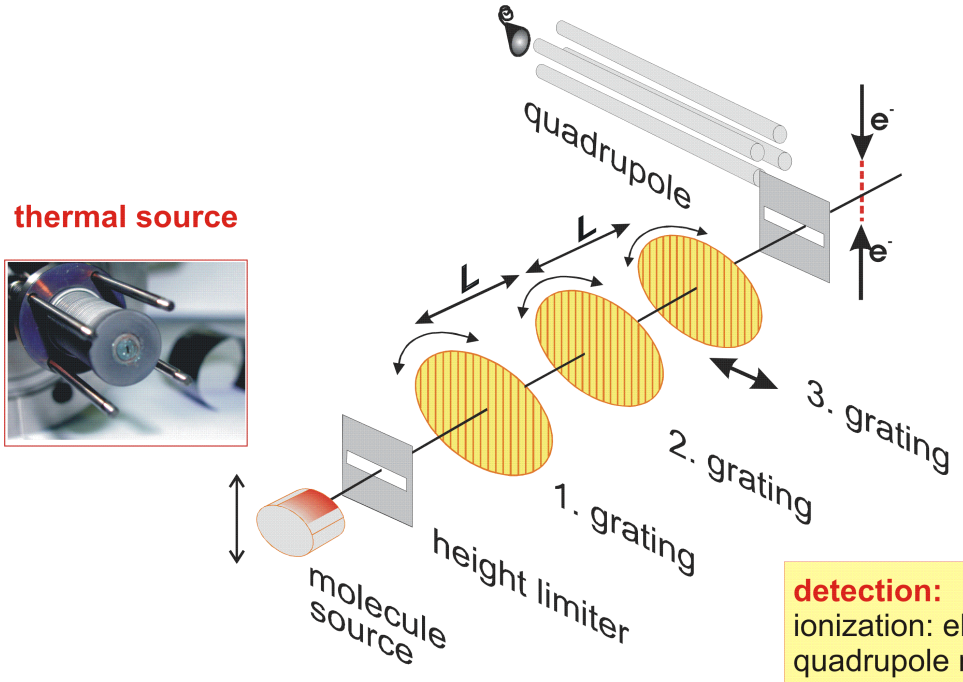


Jednofotonový Youngův interferenční experiment

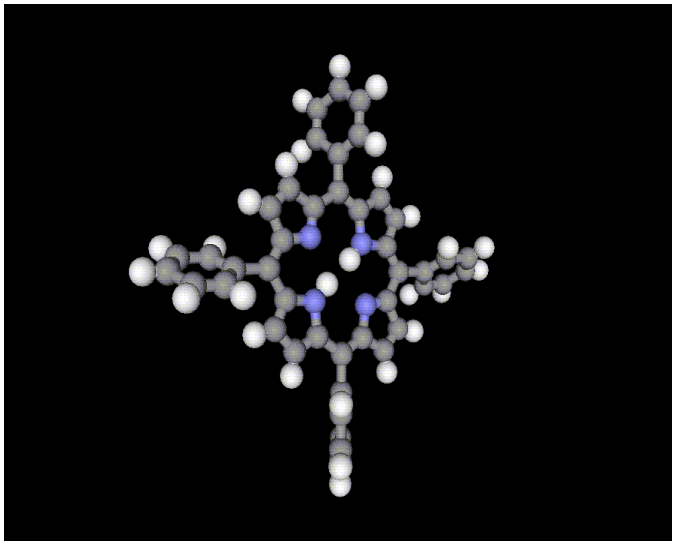
Interference fullerenů a organických molekul



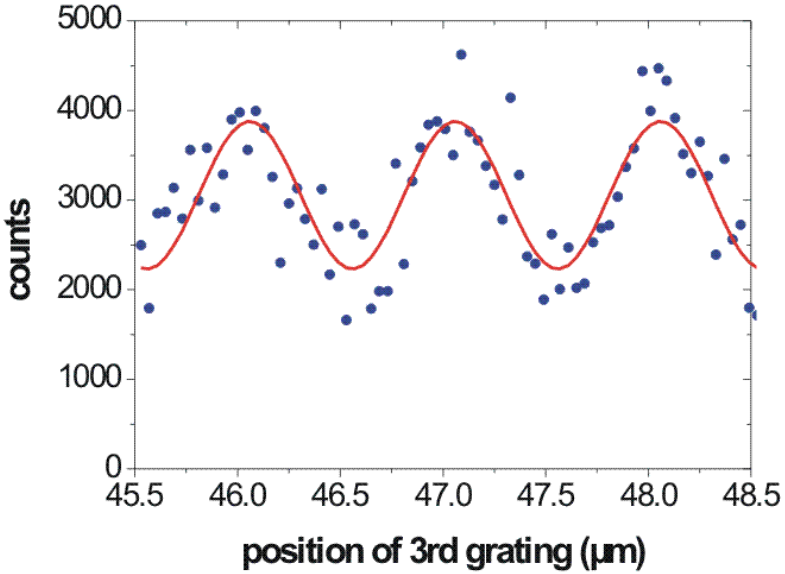
$C_{60}F_{48}$



detection:
ionization: electron beam
quadrupole mass spectrometer (2000 amu)

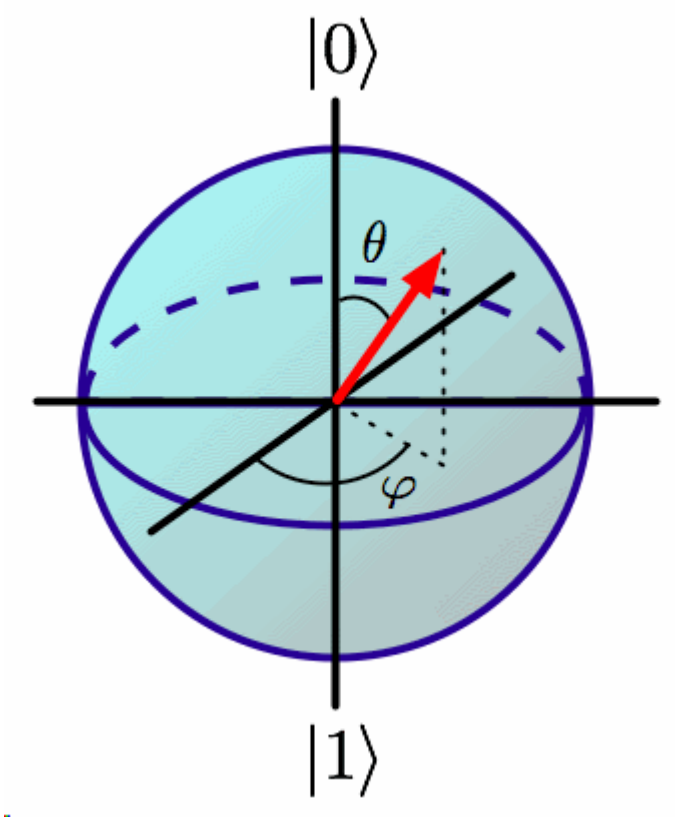


porphyrin



II. Kvantový počítač

Kvantový bit



- dvouhladinový kvantový systém
- výpočetní báze

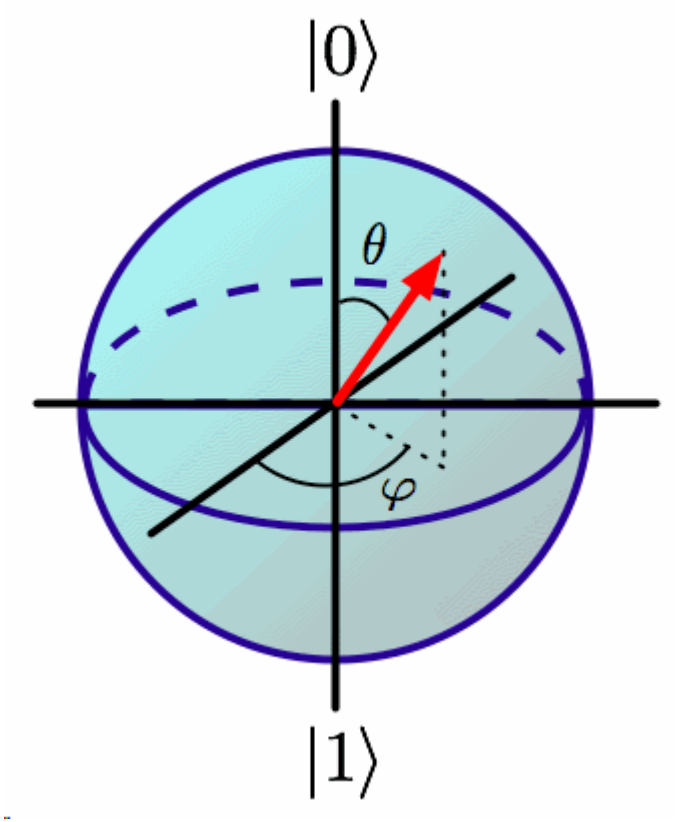
$$0 \Leftrightarrow |0\rangle \qquad 1 \Leftrightarrow |1\rangle$$

- libovolná superpozice bázových stavů

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

$$\langle 0|1\rangle = 0$$

Kvantový bit



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

$$\langle 0|1\rangle = 0$$

- dvouhladinový kvantový systém
- výpočetní báze

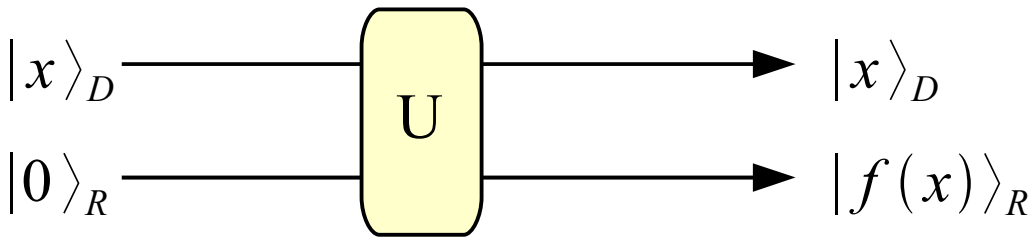
$$0 \Leftrightarrow |0\rangle \qquad 1 \Leftrightarrow |1\rangle$$

- libovolná superpozice bázových stavů

Příklady kvantových bitů:

- spin elektronu
- polarizační stav fotonu
- jaderný spin (NMR)
- dvě hladiny atomu
- atd.

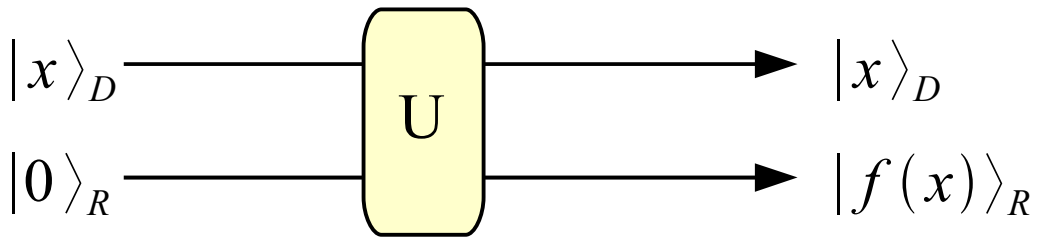
Kvantový paralelismus



$$|0\rangle_D|0\rangle_R \rightarrow |0\rangle_D|f(0)\rangle_R$$

$$|1\rangle_D|0\rangle_R \rightarrow |1\rangle_D|f(1)\rangle_R$$

Kvantový paralelismus



$$|0\rangle_D|0\rangle_R \rightarrow |0\rangle_D|f(0)\rangle_R$$

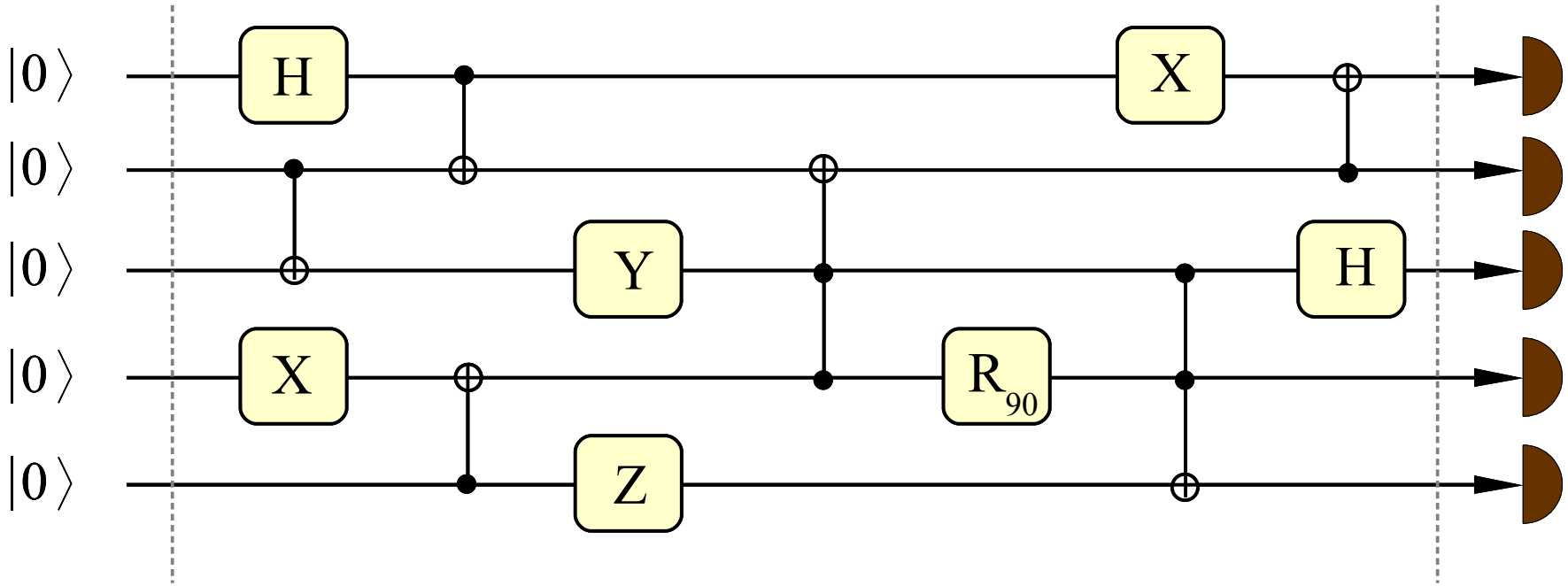
$$|1\rangle_D|0\rangle_R \rightarrow |1\rangle_D|f(1)\rangle_R$$

Datový qubit v superpozici bázových stavů:

$$(|0\rangle_D + |1\rangle_D)|0\rangle_R \rightarrow |0\rangle_D|f(0)\rangle_R + |1\rangle_D|f(1)\rangle_R$$

Paralelní výpočet hodnoty funkce pro obě hodnoty argumentu!

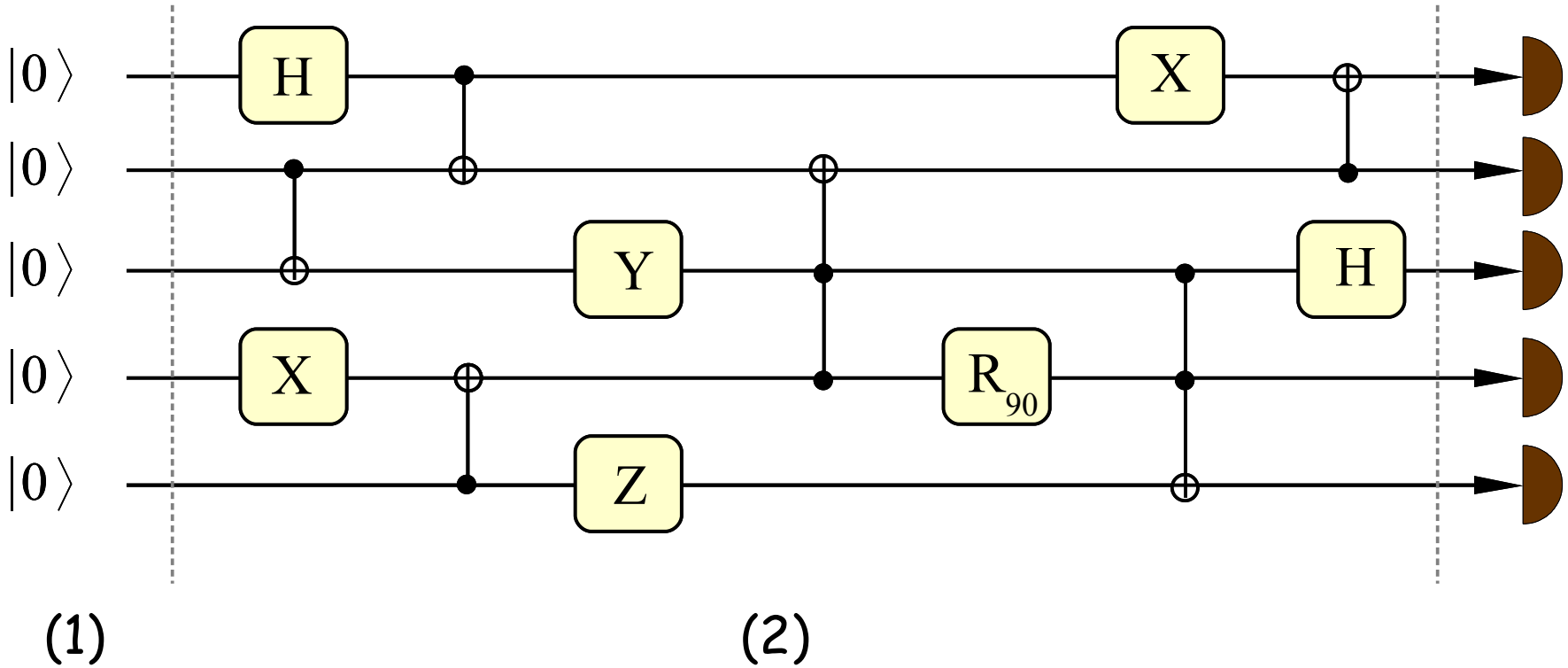
Architektura kvantového počítače



(1)

(1) Příprava vstupních kvantových bitů (kvantový datový registr)

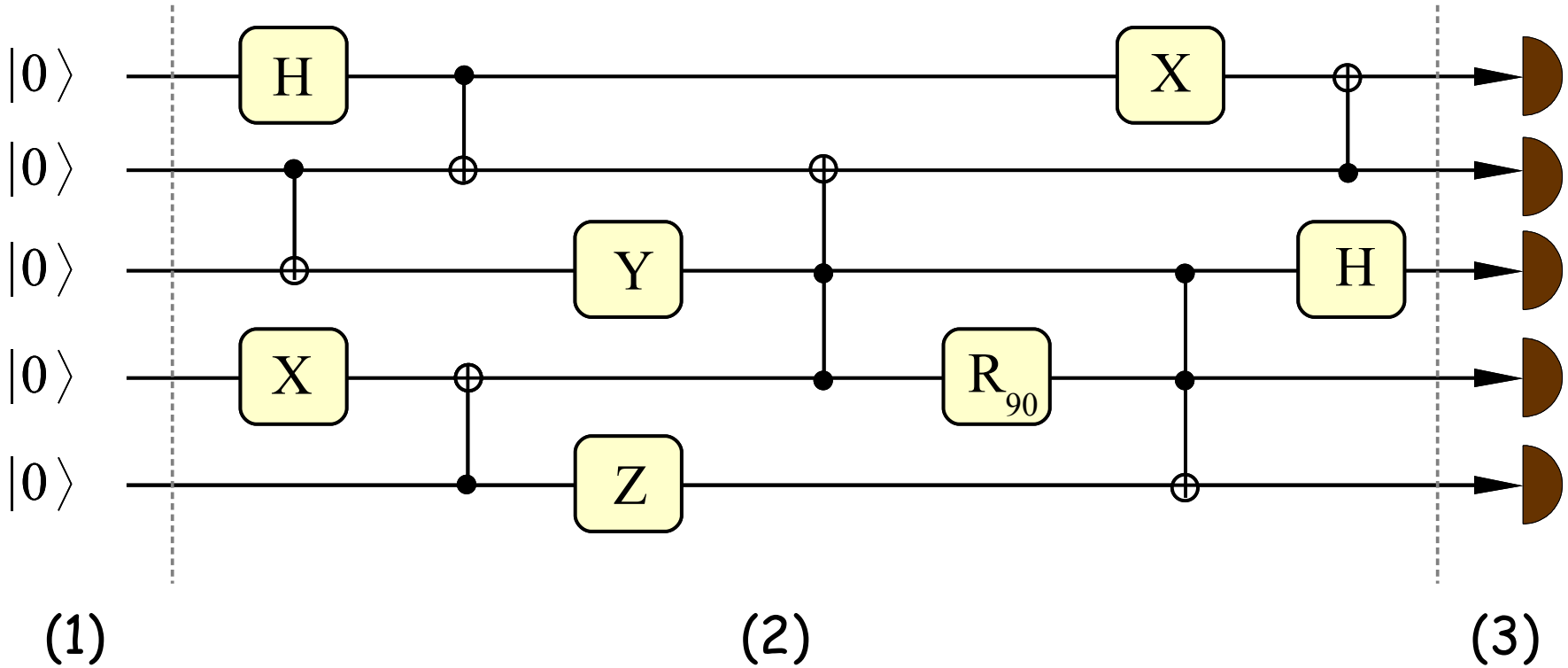
Architektura kvantového počítače



(1) Příprava vstupních kvantových bitů (kvantový datový registr)

(2) Unitární operace na vstupním stavu (sekvence kvantových hradel)

Architektura kvantového počítače



(1) Příprava vstupních kvantových bitů (kvantový datový registr)

(2) Unitární operace na vstupním stavu (sekvence kvantových hradel)

(3) Měření na výstupních kvantových bitech (výsledek výpočtu)

Kvantové algoritmy

Efektivní řešení určitých specifických výpočetních úloh.

Kvantové algoritmy

Efektivní řešení určitých specifických výpočetních úloh.

Exponenciální zrychlení díky kvantovému paralelismu:

- Deutschův algorithmus
- Deutsch-Jozsův algoritmus (rozlišení konstantní a vyvážené funkce)
- Shorův algoritmus (faktorizace)

Kvantové algoritmy

Efektivní řešení určitých specifických výpočetních úloh.

Exponenciální zrychlení díky kvantovému paralelismu:

- Deutschův algorithmus
- Deutsch-Jozsův algoritmus (rozlišení konstantní a vyvážené funkce)
- Shorův algoritmus (faktorizace)

Kvadratické zrychlení:

- Groverův algoritmus (prohledávání nesetříděné databáze)

$$O(N) \rightarrow O(\sqrt{N})$$

Shorův algoritmus

Problém faktorizace:

$$15 = 5 \times 3$$

$$12532552843 = ? \times ?$$

Shorův algoritmus

Problém faktorizace:

$$15 = 5 \times 3$$

$$12532552843 = 180811 \times 69313$$

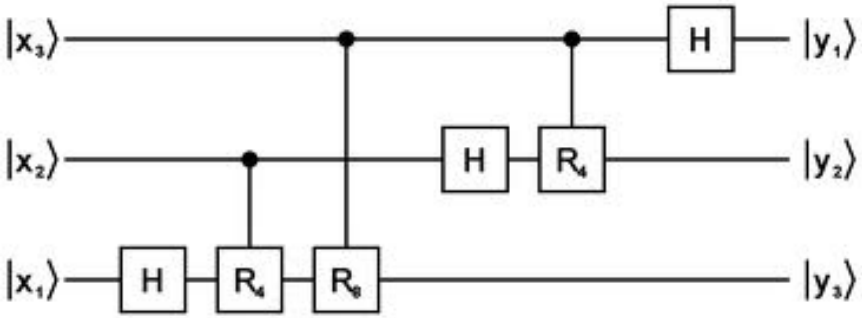
Klasické algoritmy – výpočetní čas roste exponenciálně s počtem číslic faktorizovaného čísla.

Shorův algoritmus

Problém faktorizace:

$$15 = 5 \times 3$$

$$12532552843 = 180811 \times 69313$$



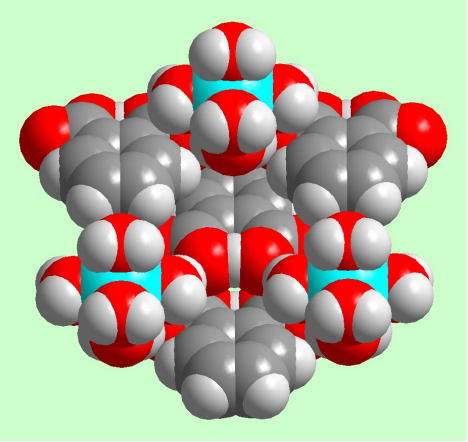
Klasické algoritmy – výpočetní čas roste exponenciálně s počtem číslic faktorizovaného čísla.

Shorův kvantový algoritmus:

- polynomiální škálování výpočetního času
- možnost faktorizace extrémně velkých čísel
- prolomení šifry RSA (šifra s veřejným klíčem)

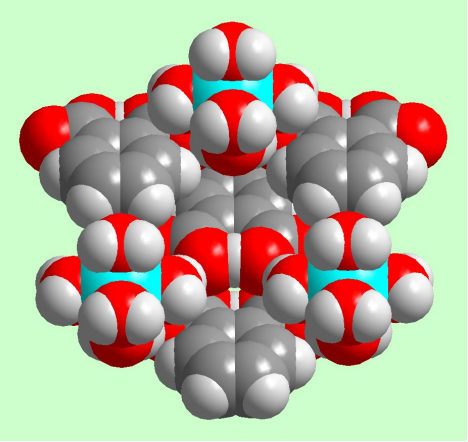
Simulace dynamiky komplexních kvantových systémů

Simulace kvantové dynamiky N spinů – kvantových bitů



Simulace dynamiky komplexních kvantových systémů

Simulace kvantové dynamiky N spinů – kvantových bitů



Dimenze prostoru stavů N kvantových bitů:

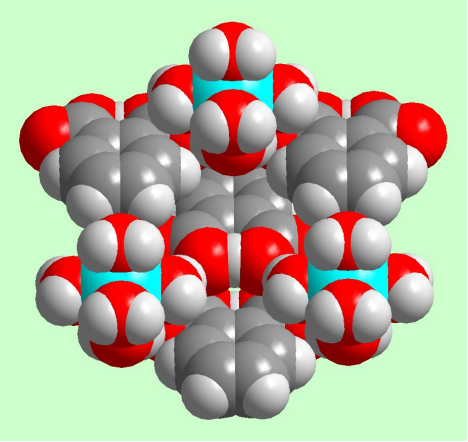
$$d_N = 2^N$$

roste **exponenciálně** s počtem kvantových bitů.

Simulace na klasickém počítači je neefektivní, současná mez je cca N=40

Simulace dynamiky komplexních kvantových systémů

Simulace kvantové dynamiky N spinů – kvantových bitů



Dimenze prostoru stavů N kvantových bitů:

$$d_N = 2^N$$

roste **exponenciálně** s počtem kvantových bitů.

Simulace na klasickém počítači je neefektivní, současná mez je cca N=40

Kvantový počítač:

- umožní efektivní simulaci dynamiky kvantových systémů
- poskytne netriviální výsledky již pro datový registr v řádu desítek qubitů
- aplikace v kvantové chemii, materiálovém inženýrství, nanotechnologii atd.

DiVincenzova kritéria

1. Dobře definované kvantové bity

2. Inicializace kvantových bitů v čistých stavech

3. Univerzální sada kvantových hradel

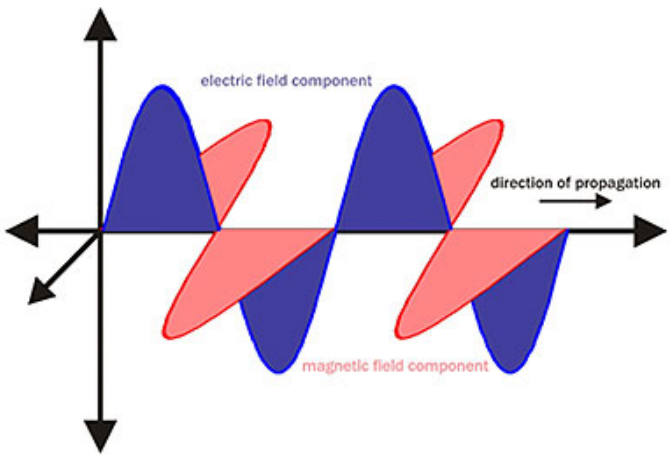
4. Libovolná měření na výstupních qubitech

5. Dlouhá koherenční doba

D. DiVincenzo
IBM Research

Optické kvantové počítače

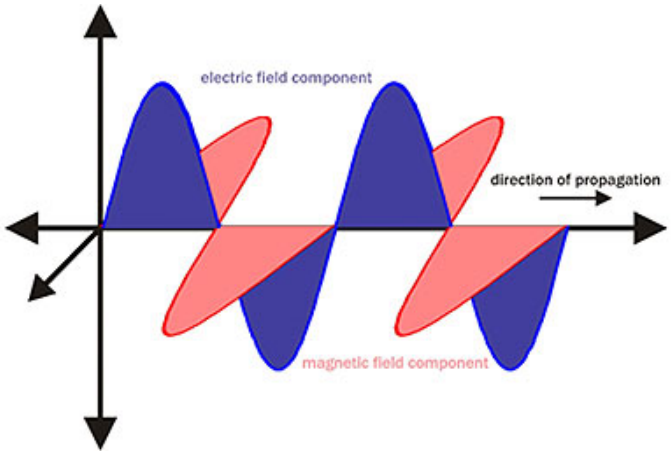
Kvantové bity kódované do polarizačních stavů jednotlivých fotonů



Optické kvantové počítače

Kvantové bity kódované do polarizačních stavů jednotlivých fotonů

Kvantová měření realizovaná s využitím polarizačních děličů svazku a jednofotonových detektorů

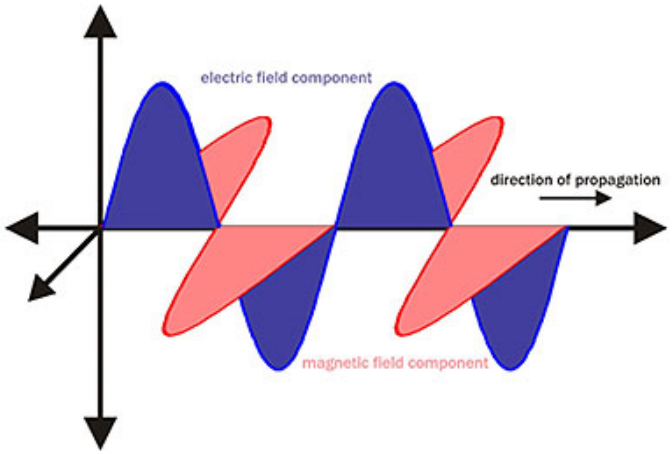


Optické kvantové počítače

Kvantové bity kódované do polarizačních stavů jednotlivých fotonů

Kvantová měření realizovaná s využitím polarizačních děličů svazku a jednofotonových detektorů

Jednoqubitová kvantová hradla implementovaná pomocí vlnových destiček



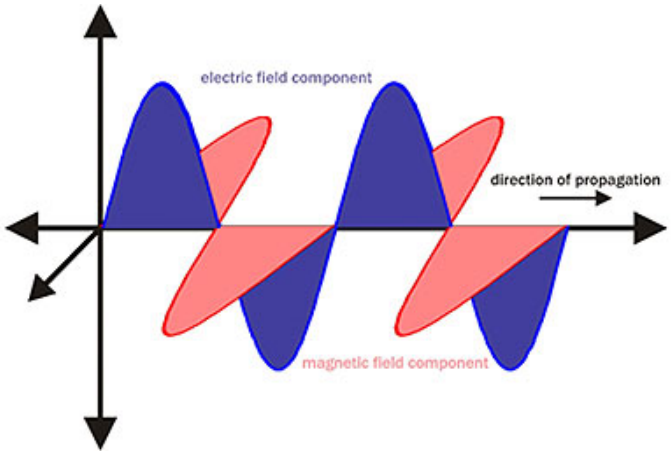
Optické kvantové počítače

Kvantové bity kódované do polarizačních stavů jednotlivých fotonů

Kvantová měření realizovaná s využitím polarizačních děličů svazku a jednofotonových detektorů

Jednoqubitová kvantová hradla implementovaná pomocí vlnových destiček

Dvouqubitová hradla ??? (viz dále)



Zdroje fotonů

Lasery

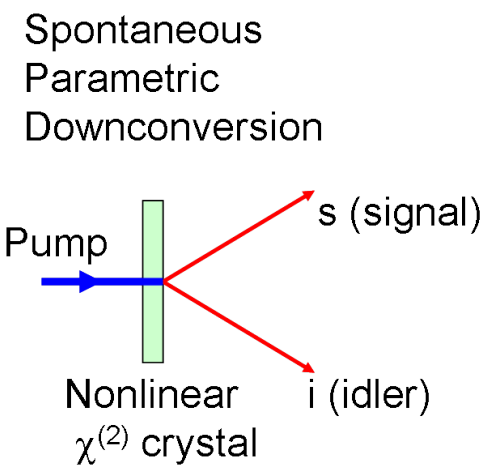
- zdroje koherentního světla
- kontinuální a pulzní lasery
- silně atenuované laserové záření → aproximace jednofotonového stavu

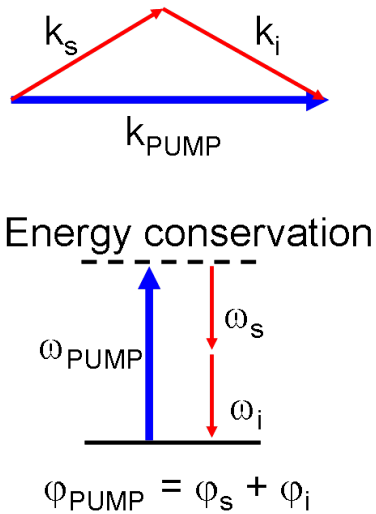
Zdroje fotonů

Lasery

- zdroje koherentního světla
- kontinuální a pulzní lasery
- silně atenuované laserové záření → aproximace jednofotonového stavu

Parametrická frekvenční konverze





- nelineární optický proces
- čerpaný laserem
- generace párů korelovaných fotonů
- podmíněná příprava jednofotonových stavů

Optické kvantové CNOT hradlo

Kontrolované NOT hradlo:

$$|00\rangle \rightarrow |00\rangle$$

$$|01\rangle \rightarrow |01\rangle$$

$$|10\rangle \rightarrow |11\rangle$$

$$|11\rangle \rightarrow |10\rangle$$

Optické kvantové CNOT hradlo

Kontrolované NOT hradlo:

$$|00\rangle \rightarrow |00\rangle$$

$$|01\rangle \rightarrow |01\rangle$$

$$|10\rangle \rightarrow |11\rangle$$

$$|11\rangle \rightarrow |10\rangle$$

Optická implementace vyžaduje interakci dvou fotonů

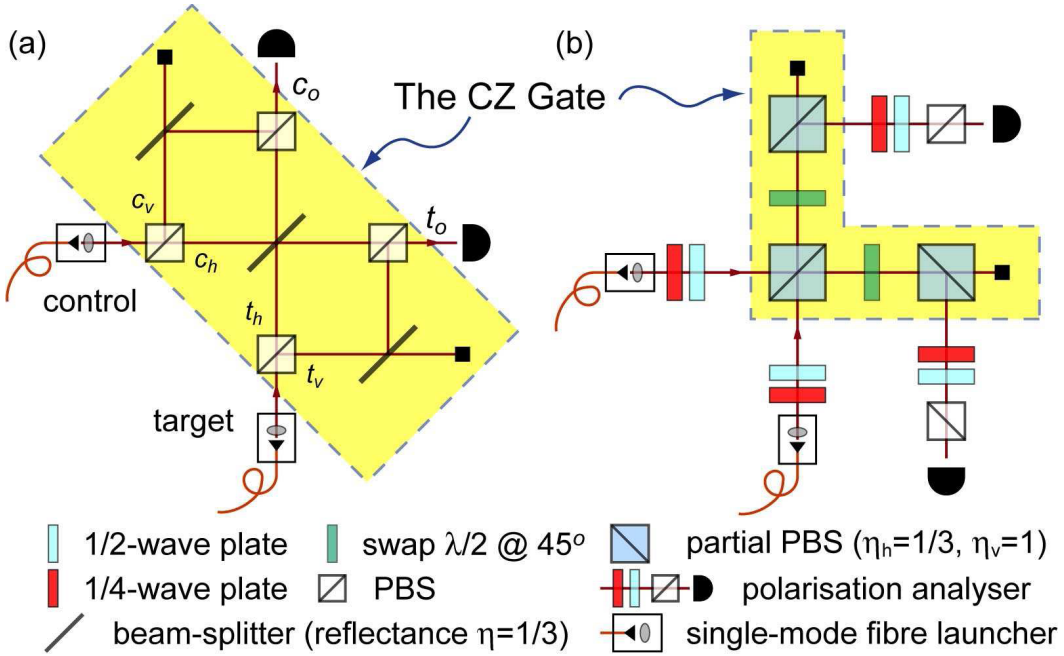
Dostatečně silná interakce však není k dispozici

Řesení – kvantové počítání s lineární optikou !!!

Lineárně optická kvantová logická hradla

Emulace nelineární interakce mezi dvěma fotony:

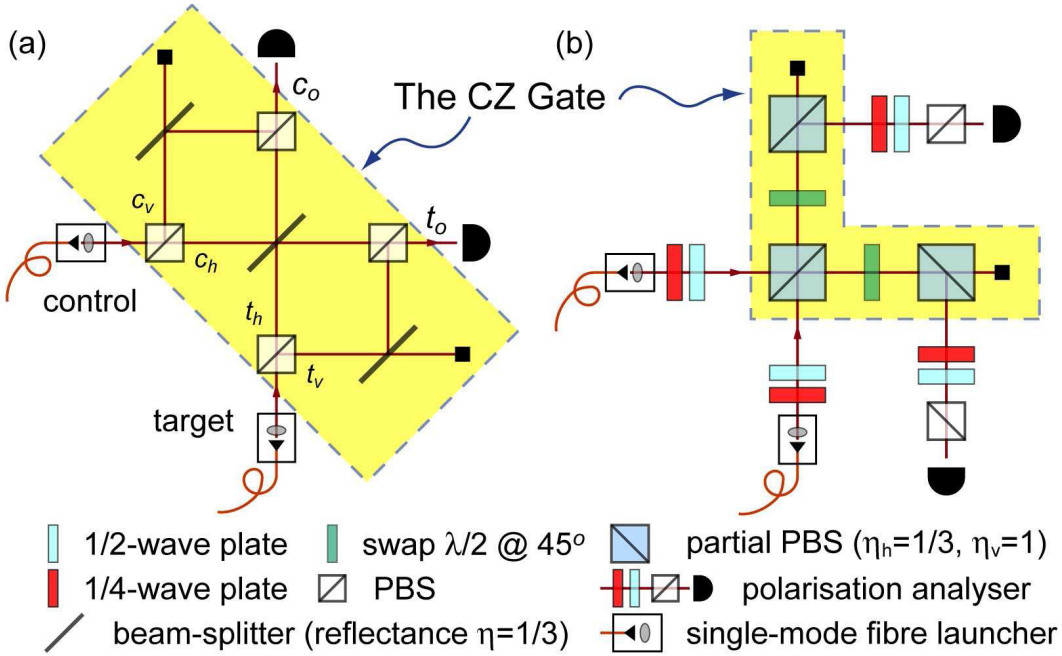
- lineární optické komponenty
- multi-fotonová interference
- jednofotonová detekce
- pomocné fotony



Lineárně optická kvantová logická hradla

Emulace nelineární interakce mezi dvěma fotony:

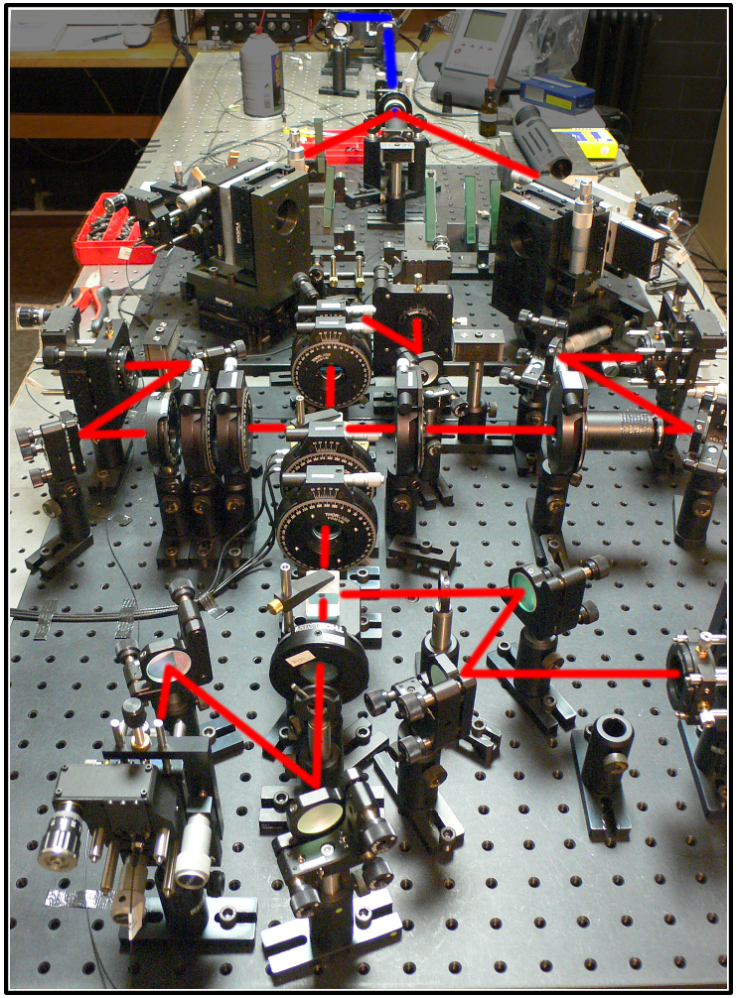
- lineární optické komponenty
- multi-fotonová interference
- jednofotonová detekce
- pomocné fotony



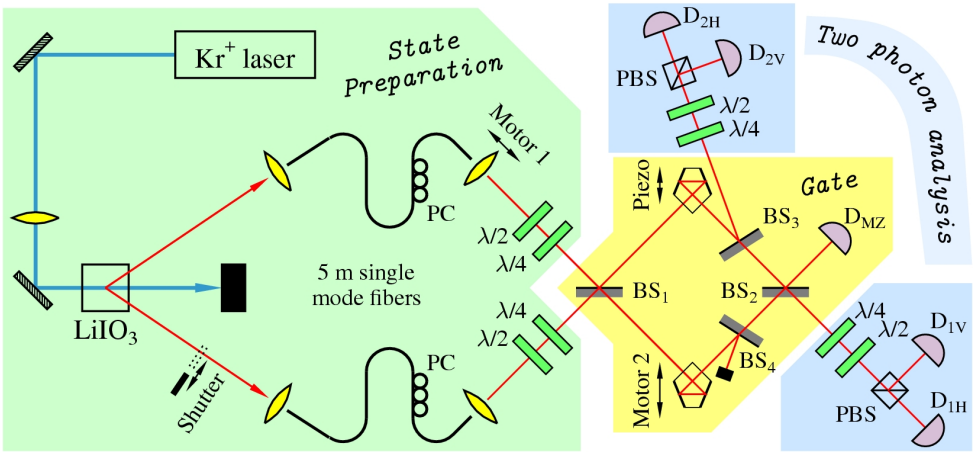
Probabilistická hradla – úspěch heraldován výsledkem měření

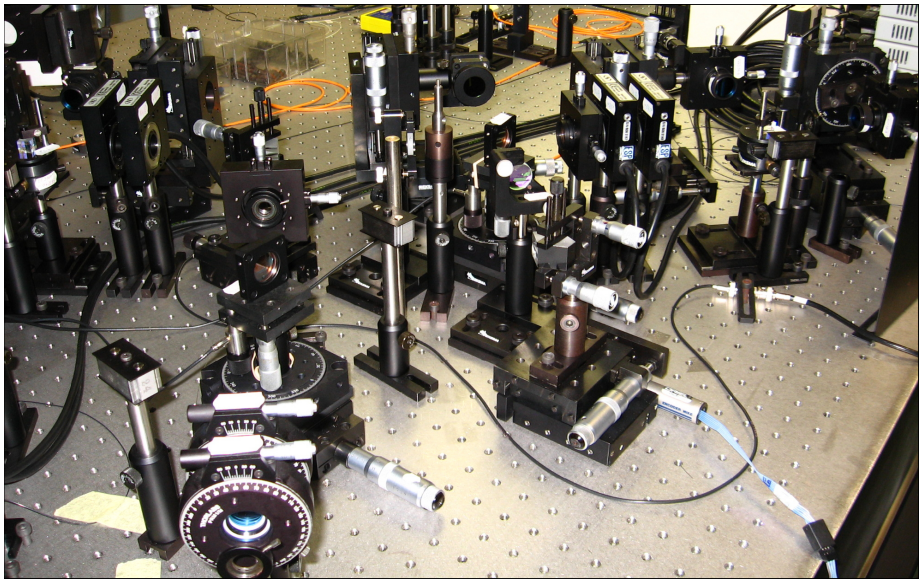
Pravděpodobnost úspěchu lze libovolně zvýšit s užitím pomocných fotonů a komplexnějších schémat.

Lineárně optická kvantová logická hradla implementovaná v Olomouci



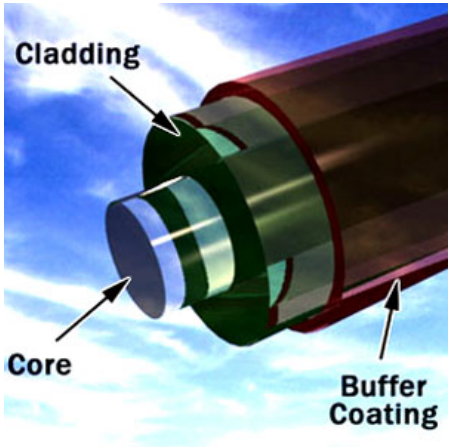
Programovatelné kvantové hradlo

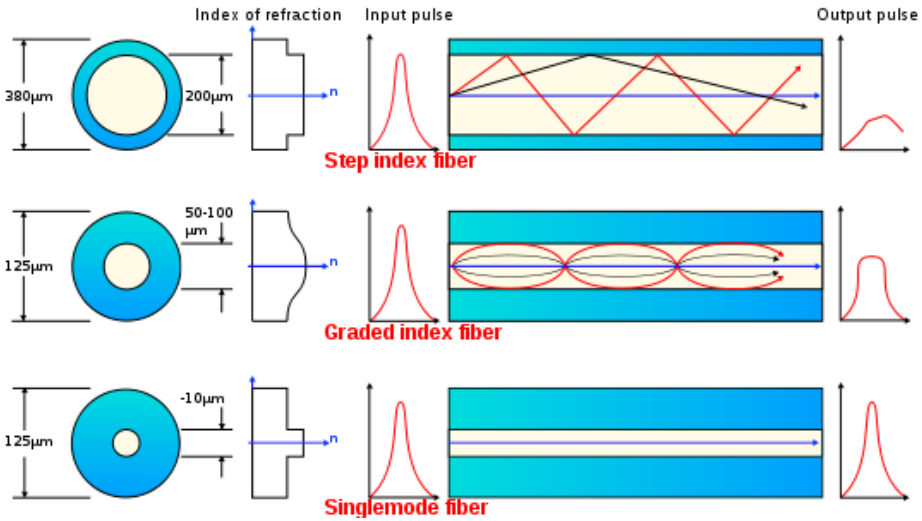




Partial-SWAP hradlo

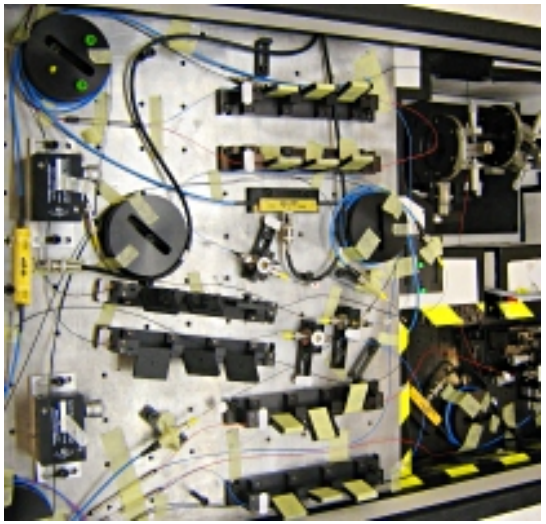
Vláknově optické implementace optických kvantových informačních procesorů



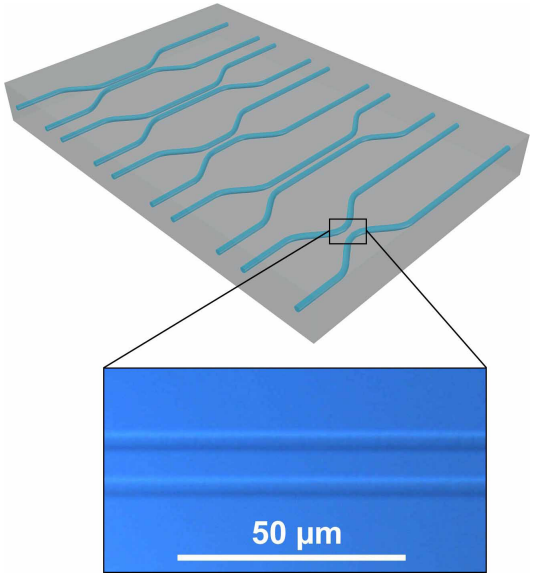


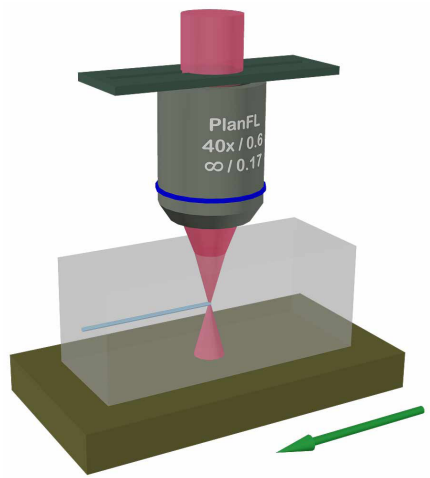
Optická vlákna:

- páteř optických komunikačních systémů
- signál veden pomocí totálního odrazu světla
- konstrukce procesorů kompatibilních s komerčními telekomunikačními systémy
- klíčové pro optickou komunikaci



Integrované optické kvantové procesory





Jeremy O'Brien

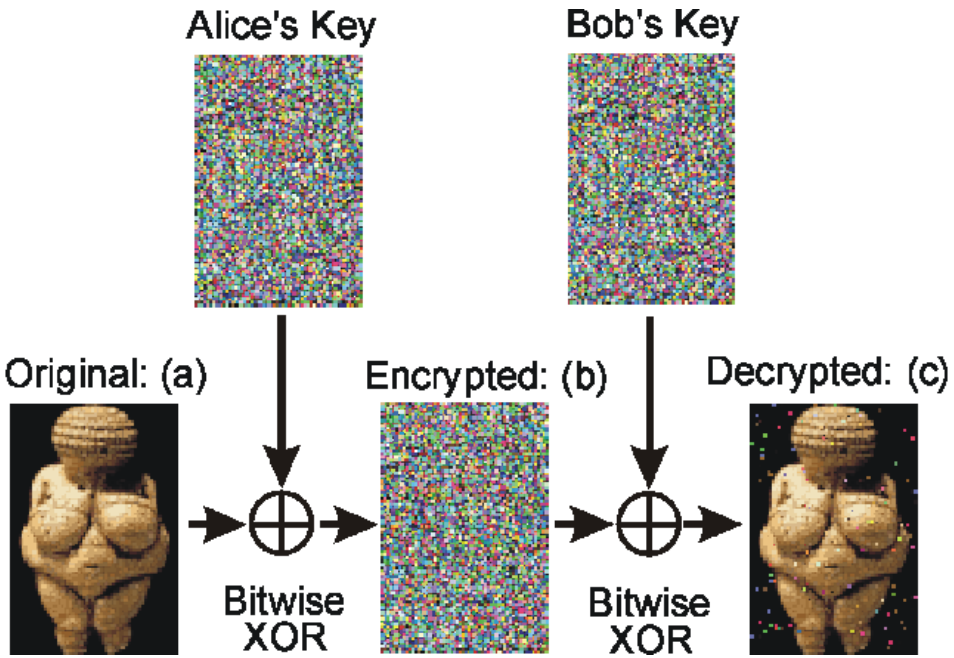
Optické vlnovody na silikonovém chipu

Inherentně stabilní, škálovatelná architektura

Možnost vytvářet optické obvody včetně 3D struktur femtosekundovým laserem

III. Kvantová kryptografie

Bezpečná komunikace - šifrování



Šifrovaná komunikace – bezpečný přenos citlivých informací a tajných dat.

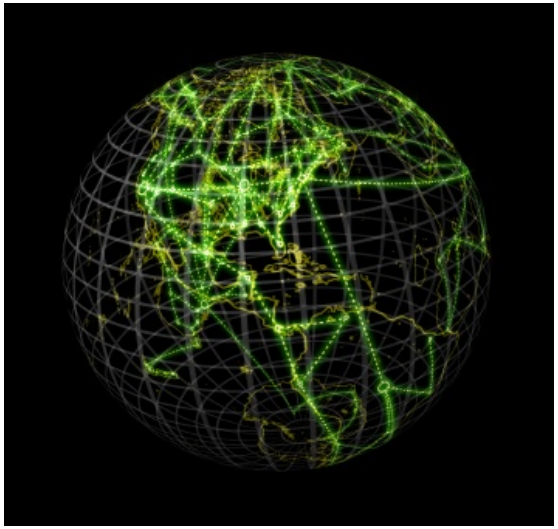
Tajný šifrovací klíč – náhodná sekvence bitů, sdílená jen autorem a příjemcem zprávy.

Vernamova šifra – prokazatelně bezpečná, klíč stejně dlouhý jako zpráva.

Šifrovaná komunikace na internetu

Problém distribuce tajného klíče:

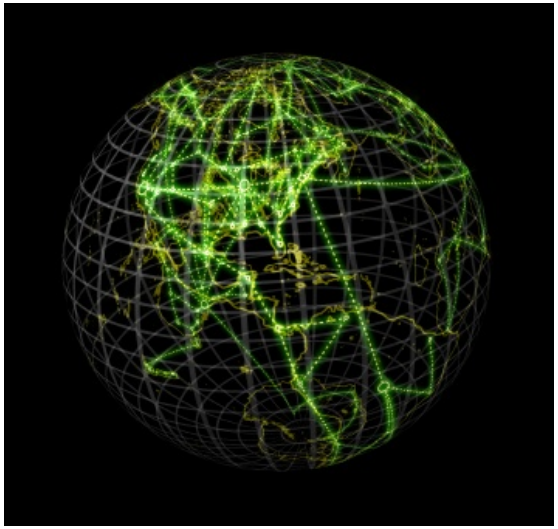
klasicky neřešitelný, nelze identifikovat možný odposlech.

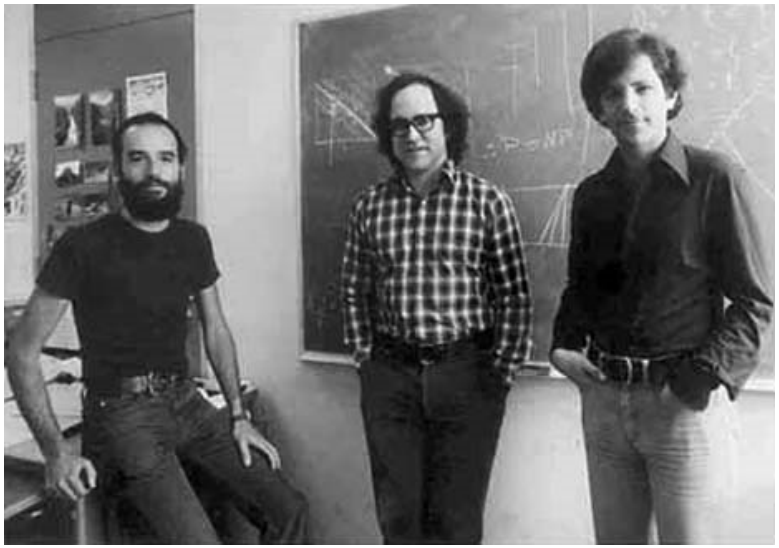


Šifrovaná komunikace na internetu

Problém distribuce tajného klíče:

klasicky neřešitelný, nelze identifikovat možný odposlech.



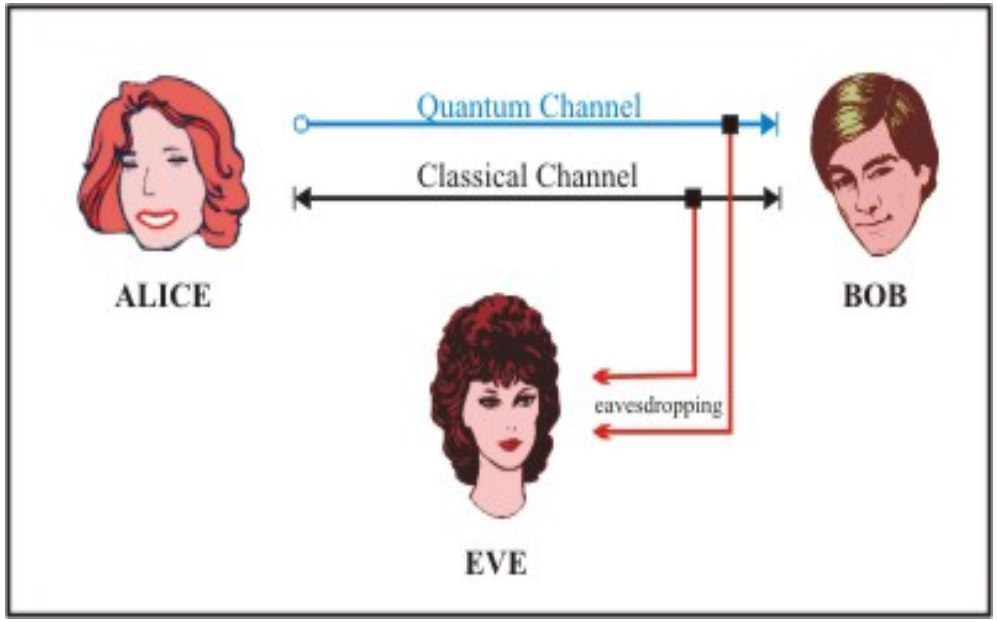


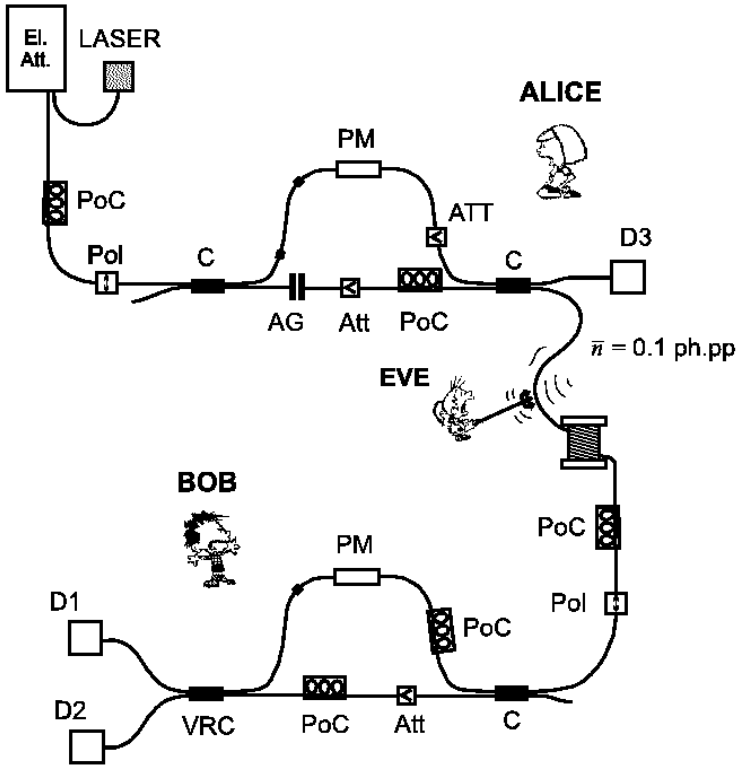
Rivest, Shamir, Adleman

Asymetrická šifra RSA:

- **kombinace veřejného a tajného klíče**
- **založena na náročnosti určitých matematických operací (faktorizace)**
- **bezpečnost není dokázána**
- **kvantový počítač by umožnil prolomení šifry RSA!**

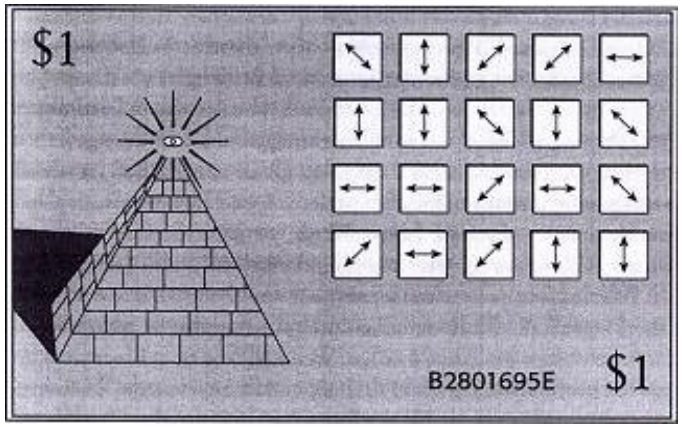
Kvantová kryptografie





- Prokazatelně bezpečný přenos tajného šifrovacího klíče
- Jakýkoliv pokus o odposlech je detekován – navyšuje šum
- Dosah kvantově kryptografických systémů činí 100 – 150 km

Trocha historie – kvantové peníze



Stephen Weisner, 70. léta 20. století

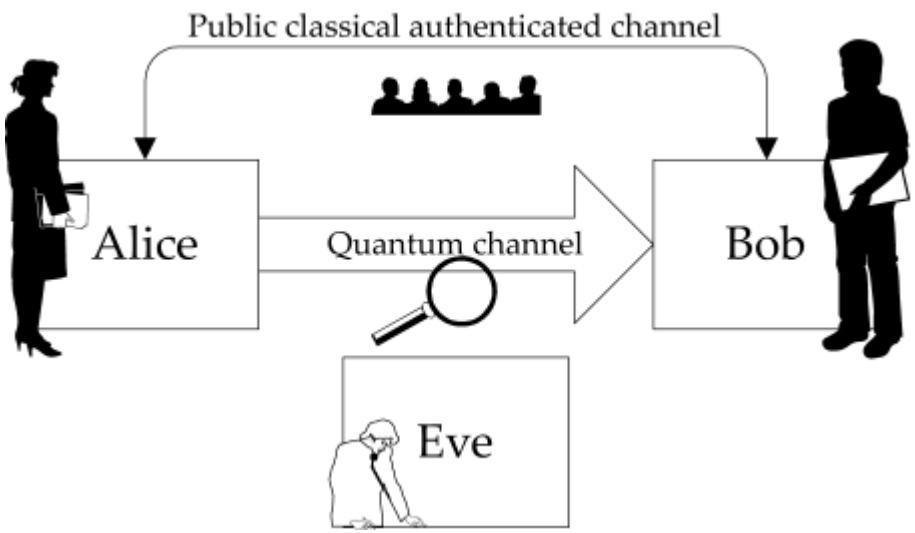
"Conjugate coding"

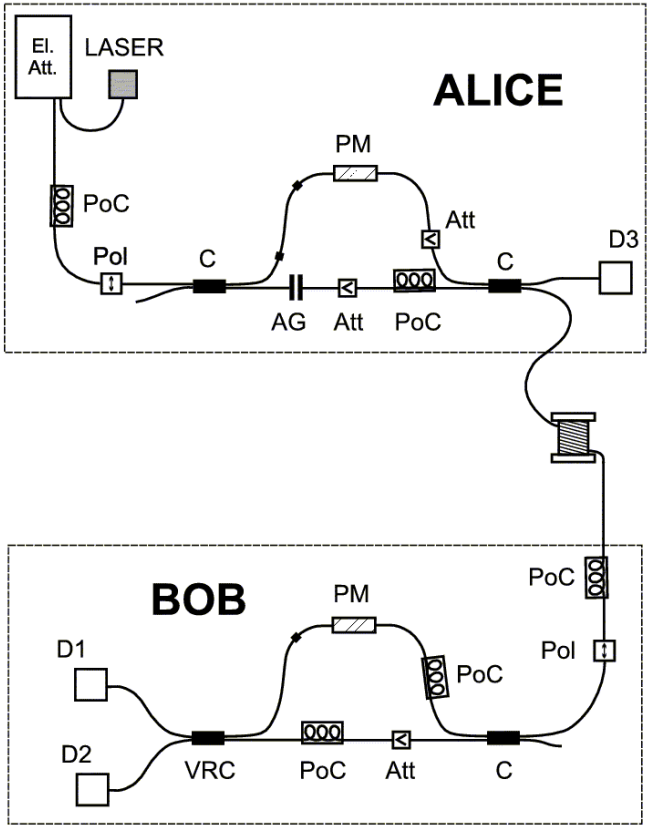
Návrh nepadělatelných bankovek:

- **každá bankovka obsahuje dvacet optických rezonátorů**
- **v každém rezonátoru (pasti) je zachycen právě jeden foton**
- **každý z fotonů je polarizován v náhodném směru, který zná jen banka**

Revoluční myšlenka, i když v původní podobě značně nepraktická.

Kvantová distribuce tajného klíče





- Bity tajného klíče jsou kódovány do kvantových stavů fotonů
- Jakýkoliv pokus o odposlech navyšuje šum v komunikačním protokolu
- Odposlech lze proto identifikovat a jeho vliv eliminovat!

Kvantová kryptografie – aktuální stav

- Vyvinuta řada komerčních prototypů (projekt SECOQC)
- Několik firem nabízí komerční kvantové kryptosystémy
- Současný dosah kvantové kryptografie omezen na cca 150 km
- Ztáty, temné county detektorů

Kvantová kryptografie – aktuální stav

- Vyvinuta řada komerčních prototypů (projekt SECOQC)
- Několik firem nabízí komerční kvantové kryptosystémy
- Současný dosah kvantové kryptografie omezen na cca 150 km
- Ztáty, temné county detektorů

Zvýšení dosahu QKD:

- kompenzace ztrát a potlačení šumu
- kvantová korekce chyb
- kvantové opakovače
- kvantová teleportace
- destilace kvantových korelací

Vize - Globální kvantová komunikační síť

- Satelitní komunikace
- Komunikace volným prostorem
- Optické vláknové komunikace

Děkuji Vám za pozornost!

http://optics.upol.cz

http://www.facebook.com/optika.olomouc