

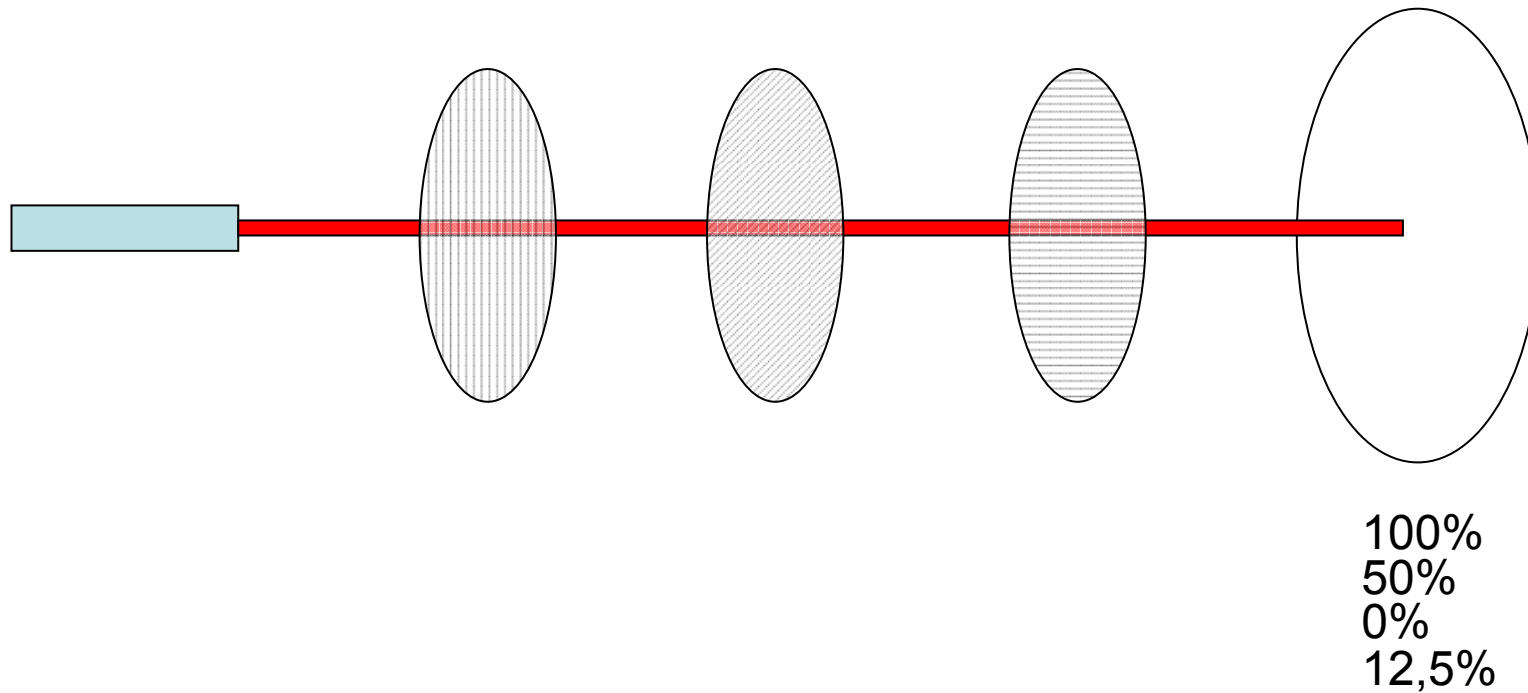
# Quantum computing

Libor Váša

# Outline

- Zvláštní chování fyziky
  - Kvantové jevy, polarizace etc.
- Abstrakce quantum computing
  - PTM vs. QTM
  - Hilbertovy prostory
  - Qubit
  - Kvantový registr
  - Kvantová logika
- Kvantové algoritmy
- Kvantové šifry

# Experiment s polarizací fotonů



# Zvláštní chování fyziky

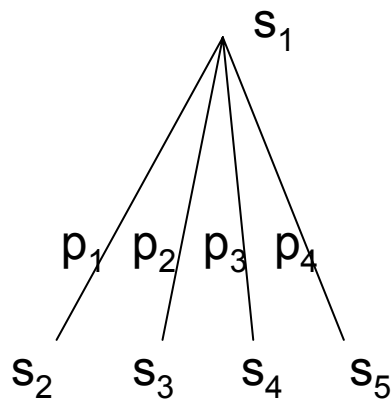
- rozměrová úroveň elementárních částic
- rezignujeme na otázku „proč?“ a „jak to?“
- odpovídáme na otázku „jak?“
- pouze snaha předpovědět chování systému
- pouze pravděpodobnostní předpovědi

# Quantum computing

- pohled na „počítač“ jako na „stroj s předpověditelným výsledkem“
- z tohoto hlediska je počítačem téměř cokoli co se dá nějak popsat
- idea – miniaturizovat
- využít toho že kvantová mechanika je popsána
- náznaky ideje – R. Feynman
- dodnes téměř výhradně teoretický obor

# PTM a QTM

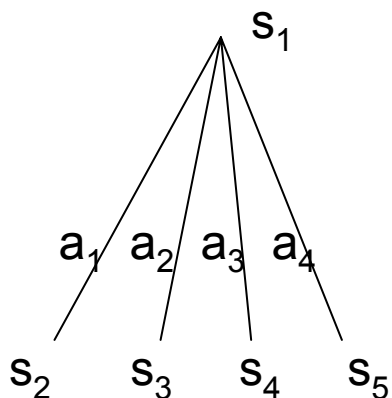
- Probabilistic Turing Machine
- přiřazuje pravděpodobnosti přechodům mezi stavy
- suma pravděpodobností přechodu z jednoho konkrétního stavu musí být 1 (lokální podmínka)



- stav ve stromu nastane s pravděpodobností rovnou násobku pravděpodobností všech větví od kořene
- suma pravděpodobností stavů na jedné úrovni stromu musí být rovna jedné (globální podmínka, splněna automaticky s lokální podmínkou)
- PTM je možno popsat maticí pravděpodobností přechodů

# Quantum Turing Machine

- Popisují chování kvantového systému
- Každému stavovému přechodu je přiřazena komplexní amplituda
- Každému stavu ve stromu je přiřazena komplexní amplituda určená jako násobek všech amplitud přechodů od kořene
- Pravděpodobnost stavu ve stromu se určí jako druhá mocnina velikosti amplitudy daného stavu



$$p_1 = |a_1|^2$$
$$p_2 = |a_2|^2$$
$$p_3 = |a_3|^2$$
$$p_4 = |a_4|^2$$

# QTM

- konkrétní stav se na některé úrovni stromu může vyskytnout několikrát
- v takovém případě se amplituda takového stavu určí jako suma amplitud jednotlivých výskytů
- amplituda je komplexní -> stavy mohou interferovat
- konstruktivní interference
  - shodná orientace amplitud
- destruktivní interference
  - opačná orientace amplitud
  - může vést až k tomu že pravděpodobnost daného stavu je nulová (pouze na dané úrovni stromu)



# QTM

- lokální podmínka (jsme-li někde pak musíme někam jít)

$$|a_1|^2 + |a_2|^2 + \dots + |a_k|^2 = 1$$

pro přechody z jednoho konkrétního stavu

- globální podmínka (vždycky musíme někde být)

$$p_1 + p_2 + \dots + p_k = 1$$

pro všechny stavy na jedné úrovni stromu

- platnost globální podmínky nevyplývá z platnosti lokální podmínky

# QTM

- QTM je možno popsat přechodovou maticí
- euklidovská norma všech sloupců je rovna jedné (lokální podmínka)
- matice je *unitární*

$$MM^* = M^*M = I$$

kde  $M^*$  je matice konjugovaná transponovaná

- (lze odvodit, netriviální)
- implikuje reverzibilitu

# QTM

- práci QTM nelze pozorovat
- QTM prochází všechny možnosti (exponenciální počet)
- z QTM je obtížné získat výsledek
- měření
  - dotaz na jeden konkrétní stav
  - kladná odpověď s danou pravděpodobností
  - dotaz nevratně zničí konfiguraci QTM

# Hilbertovy prostory

- abstrakce popisující stavy a chování kvantových systémů
- vektorový prostor se zavedenou operací součinu (tzv. inner product, výsledek je komplexní číslo)
- musí navíc být tzv. complete
  - odvození této podmínky netriviální
  - bez vlivu na další úvahy

vektor v prostoru  $\cong$  stav systému

výsledek součinu  $v_1$  a  $v_2 \cong$  amplituda že za předpokladu že systém je ve stavu  $v_2$  je zároveň ve stavu  $v_1$

# Bra-ket

- každému stavu kvantového systému odpovídá jeden bra-vektor a jeden -ketvektor
  - bra vektor:  $\langle x|$
  - ket vektor:  $|x\rangle$
- obdoba řádkového a sloupcového vektoru
- inner product je násobek bra- -ket
  - $\langle x||y\rangle$
  - zapisuje se  $\langle x|y\rangle$

# Báze stavového prostoru QS

- pro každý „pure“ stav  $x$  platí
$$\langle x|x \rangle = 1$$
- pro některé dvojice stavů  $x$   $y$  může platit
$$\langle x|y \rangle = 0$$
- Hledejme největší množiny stavů jejichž vzájemný inner product je nulový
  - kardinalita takových množin je pro daný QS konstantní (tak je chová fyzika)
  - takové množiny se chovají jako ortonormální báze Hilbertova prostoru příslušejícího danému systému (model se chová stejně, proto byl také vybrán)

# Ekvivalence QS a HS

- důsledky:
  - zvolme nějakou bázi HS
    - jakýkoli stav  $|x\rangle$  je možno vyjádřit jako
    - kde  $a_i$  jsou komplexní kombinační koeficienty a  $b_i$  jsou  
bázové vektory HS dimenze  $n$
    - Inner product je možno vyjádřit jako

kde  $a_i$  jsou kombinační koeficienty stavu  $x$  a  $b_i$  jsou  
kombinační koeficienty stavu  $y$

# Qubit

- kvantový systém ekvivalentní dvourozměrnému HS
- někdy ve významu „stav kvantového systému...“
- označme nějakou ortonormální bázi HS  $|0\rangle$  a  $|1\rangle$ , pak stav qubitu je možno vyjádřit jako

$$|s\rangle = a |0\rangle + b |1\rangle, |a|^2 + |b|^2 = 1$$

kde  $a, b$  jsou komplexní čísla

- qubit nese neomezené množství informace, není ale možné ji extrahovat



# Měření v abstrakci HS

- měření je operace nad systémem jejímž parametrem je tzv. measurable
- measurable je ortonormální báze HS (nebo úplná množina jejích disjunktních podmnožin)
- operace měření zahrnuje následující děje:
  - určení amplitudy stavu systému vzhledem k measurable (inner product)
  - „náhodná“ volba některé ze složek measurable (určená amplitudami)
  - projekce stavu systému do zvolené složky measurable (systém je změněn)
  - do „makrosvěta“ se dostane informace o tom která ze složek measurable byla zvolena

# Vývoj QS

- lze vyjádřit jako operátor nad příslušným HS
- základní otázka: jaká je amplituda stavu  $Y$  za předpokladu že systém prošel vývojem  $A$  a původně se nacházel ve stavu  $X$ ?

$$\langle Y|A|X \rangle$$

- v zavedené notaci HS a vzhledem k dané bázi lze  $A$  vyjádřit jako unitární matici
- unitární matice je v zásadě matice rotace (vektory si zachovávají délku)

# Reverzibilita

- Každý QS je tedy reverzibilní (existuje operace, která z výsledků odvodí argumenty)
- Žádná informace nemůže zmizet (to je dobře, protože mazání informací spotřebovává energii)

# Kompozice QS

- kompozice klasických systémů se chová jako kartézský součin
- dimenze klasického složeného systému je

$$d(x+y) = d(x)+d(y)$$

- kompozice QS se chová jako tenzorový součin
- Dimenze složeného qs je

$$d(x+y) = d(x)*d(y)$$

# Kvantový registr

- složen z qubitů
- stavový prostor se chová jako tenzorový součin
  
- (pokud qubit je „trochu jednička a trochu nula“ pak kvantový registr je „trochu od každé možné kombinace bitů, trochu nula, trochu jednička, trochu dvojka, trochu trojka, ...“)

# Kvantový registr

- jednotlivé složky jsou těsněji vázané než u klasického registru
- obsah informace je větší než v jednotlivých složkách dohromady
- stavový prostor roste exponenciálně
  - pro popsání stavu stoqubitového registru je potřeba  $2^{100}=1267650600228229401496703205376$  komplexních čísel
  - kvantové registry (a kvantové počítače obecně) se „obtížně“ simulují klasickou výpočetní technikou
  - Současný hardware „naštěstí“ umožňuje max. 3qb

# Quantum entanglement

- jeden z nejdůležitějších jevů QC
- báze kombinace Hilbertových prostorů je tenzorový součin bází složek
- tenzorový součin stavů složek je stav kompozice HS

ale nejen to!

# Entangled state

- stav  $|\psi\rangle$  nelze vyjádřit jako tenzorový součin stavů podsystemů
- má takový stav fyzikální smysl?



# Ano.

- jedná se o tzv. entangled state (vázaný stav)
- pokud např. stav  $|0\rangle$  vyjadřuje spin up a stav  $|1\rangle$  vyjadřuje spin down, pak komponovaným stavem je popsán systém dvou částic opačného (ale obecně neznámého) spinu, což je ve fyzice běžné
- „vázaný“ se stav nazývá proto, že nese menší množství informace
- zde uvedený stav je tzv. maximálně vázaný – nese tolik informace jako každý subsystém (změření jednoho qubitu získáme také plnou informaci o druhém)
- každý vázaný stav dvou qubitového registru se dá při vhodné volbě bází zapsat jako

# Paradoxy vázaných stavů

- změřením jednoho qubitu vázaného stavu se automaticky „změří“ a tudíž promítne i druhý (ačkoli mohou být libovolně daleko)
- bohužel nelze využít ke komunikaci (nemůžeme zjistit jestli je qubit promítnutý)
- lze využít k jiným účelům (šifrování, dense coding)
- vázané stavy jsou skutečnou příčinou nesimulovatelnosti kvantového počítače (kvantový počítač se chová nelokálně)

# Quantum gates

- vývoj QS = operace nad QS
- operace = brána (gate)
- obdoba klasických logických hradel
- musí splňovat podmínky pro QS
  - unitární matice
  - reverzibilita
- kvantový výpočet – série vývoju QS

# Klonovati nemožno (no cloning)

- problém: *Je možno vytvořit kopii kvantového stavu aniž by byl tímto procesem zničen?*
  - (to by se hodilo, protože bychom mohli přesněji určit v jakém stavu vlastně částice je)
- Matematicky: existuje binární unitární transformace (gate)  $U$  taková, že platí

$$U(|a0\rangle) = |aa\rangle$$

?

- Dejme tomu že by existovala. Pak:

Neexistuje

# Důsledky no cloning

- konec kvantového pirátství
- z neznámého kvantového stavu opravdu nezískáme žádnou informaci navíc
- umožňuje kvantové šifrování
- existují transformace které některé stavy klonují (ale ne všechny)
- existují transformace které téměř klonují (vytvářejí kopie, ale ty nejsou přesné)
- existuje transformace realizující tzv. kvantovou teleportaci, což je prakticky klonování, ve kterém je originál zničen

# Toffoli gate

- „Existuje univerzální quantum gate?“
  - obdoba NAND z klasické logiky
  - problém s reverzibilitou
  - Toffoliho brána (Controlled Not)
  - jakákoli binární funkce stavu QS se dá vyjádřit jako posloupnost Toffoliho bran

a	b	c	a'	b'	c'
0	0	0	0	0	0
0	0	1	0	0	1
0	1	0	0	1	0
0	1	1	0	1	1
1	0	0	1	0	0
1	0	1	1	0	1
1	1	0	1	1	1
1	1	1	1	1	0

# Hadamard Gate

- unární hradlo
- převádí zcela určený stav na zcela neurčený (vzhledem k dané bázi)
- výsledek je zcela určený vzhledem k bázi nazývané Hadamardova (nebo též duální, značení s čárkou)
- dvojitá aplikace Hadamardovy brány je negací vstupu (jeden bázevý stav se změní na druhý)
  - proto též označována jako odmocnina z NOT
  - obecně ale neexistuje negující brána ve smyslu  $\langle f(x)|x \rangle = 0$





$$U_f$$

- definováno pro libovolnou binární funkci
- platí že existuje transformace
- protože
  - transformace je reverzibilní
  - máme k dispozici Toffoli gate
- aplikujeme-li na superpozici vstupů, pak dostaneme superpozici výsledků (všechny najednou, hned)

$$V_f$$

- mějme funkci
- pak existuje transformace
  - není to na první pohled zřejmé, ale uvažme že platí

# Groverův hledací algoritmus (GS)

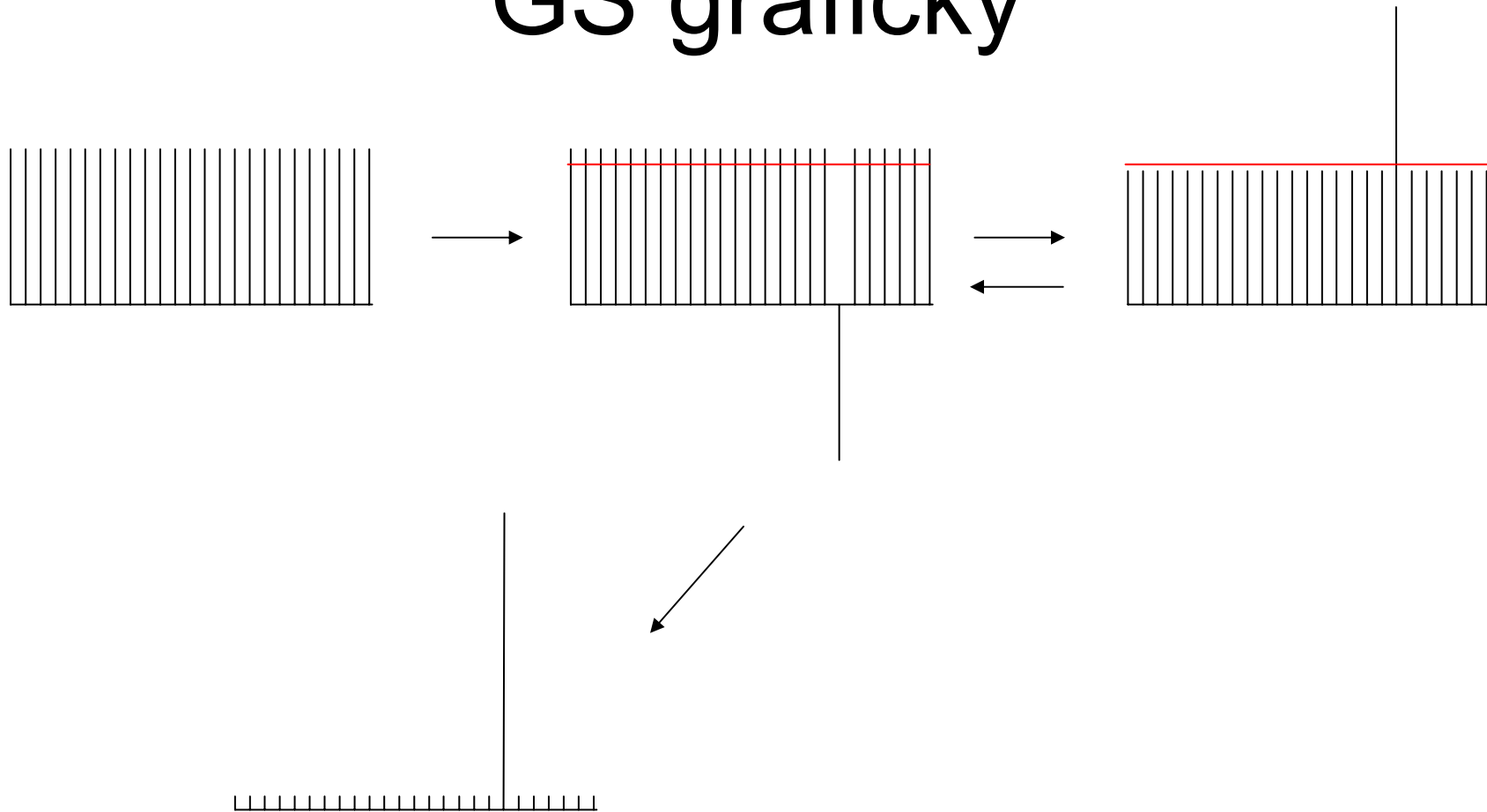
- úloha:
  - *Mějme diskrétní množinu možných hodnot  $x$  a funkci  $f(x)$  zobrazující každou z těchto hodnot do binární hodnoty. Najděme  $x$  takové, že  $f(x)=1$ .*
- mnoho úloh se dá na takovouto úlohu převést
- Groverův algoritmus umožňuje hledat v exponenciálně rozsáhlé množině v čase  $O(n^{1/2})$



# Intuitivní pohled na GS

- amplitudy stavů jsou na začátku kladná a stejně velká čísla
- amplituda hledaného stavu se aplikací  $V_f$  převrátí, tj. je záporná
- průměr je kladný
- převrácením okolo průměru se amplituda většiny stavů zmenší, ale amplituda hledaného stavu se zvětší
- funguje jenom dokud je průměr kladný!
  - tato podmínka platí právě  $\frac{1}{2}$  krát
  - obvykle je třeba o iteraci míň/víc, tj. amplituda hledaného stavu není přesně jedničková

# GS graficky



# Kvantová radiozita s GS

- připravíme kvantové registry pro radiozity jednotlivých trojúhelníků (zcela neurčené)
- připravíme unitární matici, která z radiozit vypočítá zbytkovou energii v systému (suma absolutních reziduí v radiozitní matici)
- připravíme matici  $V_f$  pro funkci určující zda je reziduum nulové
- aplikujeme GS



# Quantum SR s GS

1. vytvořit  $U_f$  pro odchylku při simulaci degradace
2. opakovat:
  1. zvolit práh chyby
  2. vytvořit  $V_f$  pro  $U_f < \text{práh}$
  3. vytvořit Hadamard state reprezentující všechny možné obrazy
  4. amplifikovat amplitudy obrazů podle  $V_f$
  5. provést projekci, eventuálně snížit práh

# Shorův faktorizační algoritmus

- jeden z prvních kvantových algoritmů
- rozkládá čísla na součin
- běží v čase polynomiálním k logaritmu rozkládaného čísla
- konkrétní postup je netriviální (zahrnuje QFT – Quantum Fourier Transform)
- (není ovšem dokázáno že faktorizace je NPC problém – Shorův algoritmus nedokazuje že kvantové stroje dokáží řešit NPC úlohy)

# Kvantové šifrování

- Shorův algoritmus je vážnou hrozbou pro asymetrické šifry s veřejným klíčem
  - založeny na předpokladu že neexistuje polynomiální faktorizační algoritmus
- quantum computing ale poskytuje jiné prostředky zabezpečení přenosu poskytující bezpečnost založenou na zatím nevyvrácených přírodních zákonech
- QKG je prakticky vyzkoušený postup (polarizovaný laser v optickém vlákně)

# Šifrování tajným klíčem

- jedna z nejjednodušších šifer
- pokud je zaručeno zcela náhodné generování klíče, který je stejně dlouhý jako zpráva a který není použit více než jednou, pak je zaručena úplná bezpečnost.
- binární verze
- problém – generování a distribuce klíče

# QKG Benetta a Brassarda

- **Alice** chce poslat **Bobovi** zprávu
  - je třeba vygenerovat a přenést klíč
- Alice vygeneruje dvě náhodné sekvence
- Alice zakóduje bit z první sekvence ve standardní nebo duální bázi, podle bitu z druhé sekvence
  - neortogonální stavy
  - neexistuje measurable který je spolehlivě odliší

# QKG

- Bob vygeneruje také náhodnou sekvenci, podle které volí measurable
  - pokud zvolí bázi odpovídající kódování, pak dostane právě hodnotu bitu
  - pokud zvolí nesprávnou bázi, pak je pravděpodobnost správné hodnoty  $\frac{1}{2}$
- Bob zveřejní jaké použil báze (nikoli co naměřil)
- Alice mu odpoví v kterých případech zvolil správnou bázi
- sekvence hodnot naměřených se správnou bází je klíčem
  - je nutno provést test konzistence klíče

# QKG - příklad

Alicina sekvence	0	1	0	1	0	1	0	1
Alicina kódovací sekvence	0	0	1	1	0	0	1	1
Odeslaný stav	$ 0\rangle$	$ 1\rangle$	$ 0'\rangle$	$ 1'\rangle$	$ 0\rangle$	$ 1\rangle$	$ 0'\rangle$	$ 1'\rangle$
Bobova měřicí sekvence	0	0	0	0	1	1	1	1
Výsledek Bobova měření	0	1	R	R	R	R	0	1

# Lámání QKG

- eavesdroper Eve
- nemůže provádět měření, protože zvolením špatné báze by změnila výsledek Bobova měření
  - Bob a Alice by neměli shodný klíč
  - při testovací fázi by se na to přišlo
- nemůže si udělat kopii sekvence, protože stavy není možno klonovat



# Zdroje

- Andrew Glassner  
*Andrew Glassner's Notebook*  
*Quantum Computing, Part 1-3,*  
July-December 2001
- Josef Gruska  
*Quantum Computing,*  
McGraw-Hill Publishing Company, 1999
- John Preskill  
*Lecture Notes for Physics 229*  
*Quantum Information and Computation,*  
California Institute of Technology, September 1998

**Děkuji za pozornost**