

Kvantová, atómová a subatómová fyzika

Kvantové technológie

Meranie spinu 1/2

Dva možné stavy s rôznymi priemetmi spinu na os z

$$|\uparrow_z\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \quad |\downarrow_z\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

Povolené sú aj superpozície

$$|\psi\rangle = a |\uparrow_z\rangle + b |\downarrow_z\rangle = a \begin{pmatrix} 1 \\ 0 \end{pmatrix} + b \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} a \\ b \end{pmatrix}$$

Operátor priemetu spinu na os z

$$\hat{s}_z = \frac{\hbar}{2} \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

$|\uparrow_z\rangle$ a $|\downarrow_z\rangle$ sú vlastné stavy operátora \hat{s}_z

Skalárny súčin a normalizácia

Bra vektory

$$\langle \uparrow_z | = (1 \ 0)$$

$$\langle \downarrow_z | = (0 \ 1)$$

Superpozícia bra vektorov

$$\langle \psi | = a^* \langle \uparrow_z | + b^* \langle \downarrow_z | = (a^* \ b^*)$$

Normalizácia stavu

$$\langle \psi | \psi \rangle = (a^* \ b^*) \begin{pmatrix} a \\ b \end{pmatrix} = |a|^2 + |b|^2 = 1$$

Priemet spinu v iných smeroch

Operátory spinu spĺňajú komutačné vzťahy a musia mať vlastné hodnoty $\pm\hbar/2$

$$[\hat{S}_x, \hat{S}_y] = i\hbar\hat{S}_z \quad [\hat{S}_z, \hat{S}_x] = i\hbar\hat{S}_y \quad [\hat{S}_y, \hat{S}_z] = i\hbar\hat{S}_x$$

Riešením sú Pauliho matice násobené $\hbar/2$

$$\hat{S}_x = \frac{\hbar}{2} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \quad \hat{S}_y = \frac{\hbar}{2} \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \quad \hat{S}_z = \frac{\hbar}{2} \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

Vlastné stavy pre priemet spinu na os x

$$|\uparrow_x\rangle = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 1 \end{pmatrix} = \frac{1}{\sqrt{2}} |\uparrow_z\rangle + \frac{1}{\sqrt{2}} |\downarrow_z\rangle$$

$$|\downarrow_x\rangle = \frac{1}{\sqrt{2}} \begin{pmatrix} -1 \\ 1 \end{pmatrix} = -\frac{1}{\sqrt{2}} |\uparrow_z\rangle + \frac{1}{\sqrt{2}} |\downarrow_z\rangle$$

Operátor spinu v ľubovoľnom smere

Smer daný jednotkovým vektorom

$$\vec{n} = (\sin \vartheta \cos \varphi, \sin \vartheta \sin \varphi, \cos \vartheta)$$

Operátor priemetu spinu vo vybranom smere

$$\hat{s}_n = \vec{n} \vec{\hat{s}} = \sin \vartheta \cos \varphi \hat{s}_x + \sin \vartheta \sin \varphi \hat{s}_y + \cos \vartheta \hat{s}_z$$

$$\hat{s}_n = \frac{\hbar}{2} \begin{pmatrix} \cos \vartheta & \sin \vartheta e^{-i\varphi} \\ \sin \vartheta e^{i\varphi} & -\cos \vartheta \end{pmatrix}$$

Meranie spinu

Pripomienka: **meranie mení kvantový stav!**

Príklad: majme stav $|\uparrow_z\rangle = \frac{1}{\sqrt{2}} |\uparrow_x\rangle - \frac{1}{\sqrt{2}} |\downarrow_x\rangle$ a merajme jeho s_x

Meranie zmení stav na $|\uparrow_x\rangle = \frac{1}{\sqrt{2}} |\uparrow_z\rangle + \frac{1}{\sqrt{2}} |\downarrow_z\rangle$ s ppodobnosťou 1/2

alebo $|\downarrow_x\rangle = \frac{1}{\sqrt{2}} |\uparrow_z\rangle - \frac{1}{\sqrt{2}} |\downarrow_z\rangle$ s ppodobnosťou 1/2

V druhom meraní merajme s_z

Môžeme namerať $|\uparrow_z\rangle$ s ppodobnosťou 1/2

alebo $|\downarrow_z\rangle$ s ppodobnosťou 1/2

Celkovo máme pravdepodobnosť $1/2 \times 1/2 = 1/4$, že sa $|\uparrow_z\rangle$ zmení na $|\downarrow_z\rangle$.

Kvantový bit (qubit)

Základná jednotka informácie (v klasickom počítači): bit = 0 alebo 1

Kvantový bit (qubit): $|q\rangle = a|0\rangle + b|1\rangle$ $a, b \in \mathbb{C}$

(Niektoré) možné realizácie:

štandardná báza

Hadamartova báza

spin 1/2

$$|1\rangle = |\downarrow_z\rangle \quad |0\rangle = |\uparrow_z\rangle$$

$$|+\rangle = |\uparrow_x\rangle \quad |-\rangle = |\downarrow_x\rangle$$

polarizácia fotónu

$$|1\rangle = |zvislo\rangle \\ |0\rangle = |vodorovne\rangle$$

$$|+\rangle = |/\rangle \quad |-\rangle = |\backslash\rangle$$

alebo inak...

Blochova sféra - grafické znázornenie qubitov

Stav qubitu môžeme písať aj ako

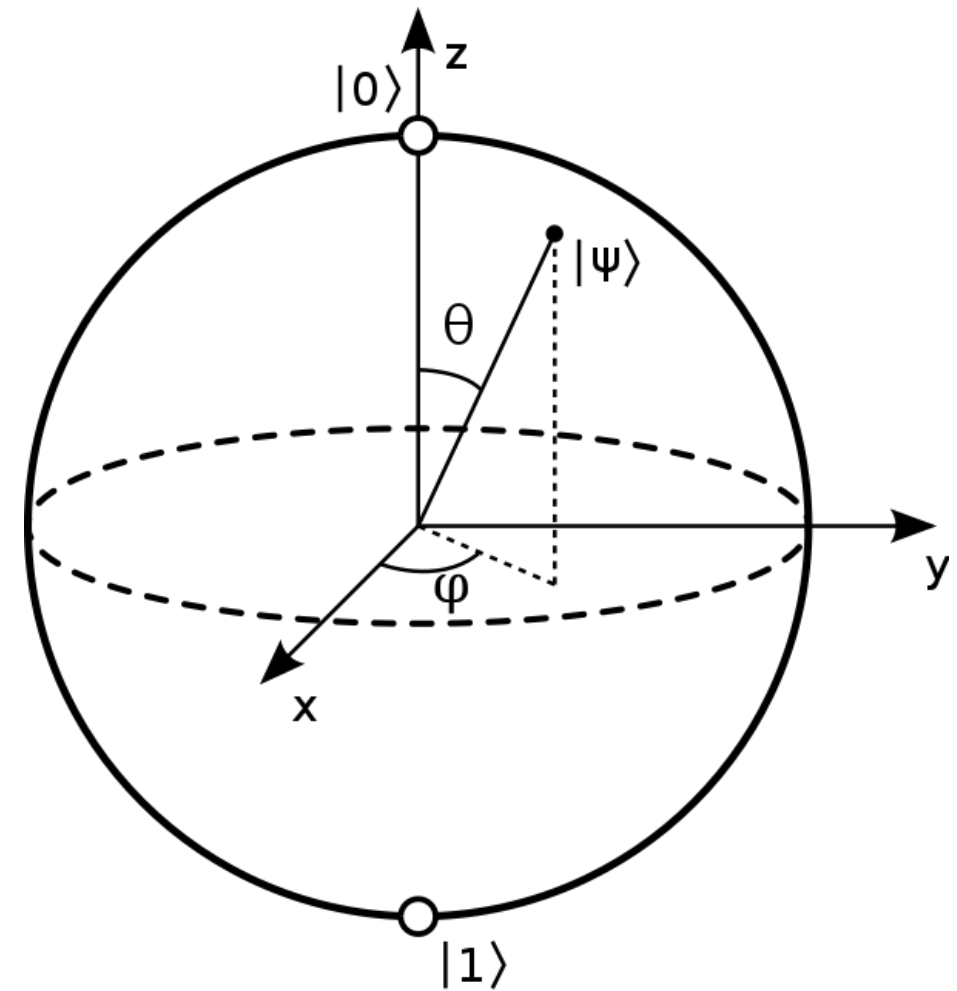
$$|q\rangle = a|0\rangle + b|1\rangle = e^{i\xi} \left(\cos \frac{\vartheta}{2} |0\rangle + e^{i\varphi} \sin \frac{\vartheta}{2} |1\rangle \right)$$

Celková fáza ξ je irelevantná

Uhly ϑ a φ úplne charakterizujú qubit

Každému izolovanému qubitu zodpovedá konkrétny bod na **Blochovej sfére**.

Zmena qubitu sa dá chápať ako rotácia stavu v priestore parametrov, teda na Blochovej sfére.



Veta o zákaze klonovania

Nie je možné vyrobiť nezávislú a identickú kópiu ľubovoľného neznámeho kvantového stavu.

[William K Wothers, Wojciech H Żurek, Nature 299 (1982) 802]

Dôkaz

Predpokladajme existenciu zariadenia (a operátora) na klonovanie, ktoré pôsobí na stav vákua.

$$\hat{T} : \quad \hat{T} |\psi\rangle |0\rangle = |\psi\rangle |\psi\rangle , \quad \hat{T} |\phi\rangle |0\rangle = |\phi\rangle |\phi\rangle$$

V kvantovej mechanike musí byť operátor lineárny.

$$\begin{aligned} \hat{T} (a |\psi\rangle + b |\phi\rangle) |0\rangle &= a \hat{T} |\psi\rangle |0\rangle + b \hat{T} |\phi\rangle |0\rangle \\ &= a |\psi\rangle |\psi\rangle + b |\phi\rangle |\phi\rangle \end{aligned}$$

$$\begin{aligned} \hat{T} (a |\psi\rangle + b |\phi\rangle) |0\rangle &= (a |\psi\rangle + b |\phi\rangle) (a |\psi\rangle + b |\phi\rangle) \\ &= a^2 |\psi\rangle |\psi\rangle + b^2 |\phi\rangle |\phi\rangle + ab |\psi\rangle |\phi\rangle + ba |\phi\rangle |\psi\rangle \end{aligned}$$

Výsledky sú rovnaké len pre $a = b = 0$

Kvantová kryptografia

Základná požiadavka: spoločný šifrovací kľúč = binárny reťazec

príklad kľúča: 00110101101011011011011100010101

príklad šifry: zmeň bit na mieste, kde je kľúč 0

správa	0	0	1	0	0	0	1	1	0	1	0	1	1	0	0	0	0	1	1	0	1	1	0	0	1	0	1	0	0	1	1	1
kľúč	0	0	1	1	0	1	0	1	1	0	1	0	1	1	0	1	1	0	1	1	0	1	1	0	0	0	1	0	1	0	1	
zašifrované	1	1	1	0	1	0	0	1	0	0	0	0	1	0	1	0	0	0	1	0	0	1	0	0	0	1	0	0	1	1	0	1

Stačí zabezpečiť privátnu distribúciu kľúča, ktorý bude známy len komunikujúcim stranám. Toto rieši kvantová kryptografia. Potom sa šifrované správy môžu posielat' klasickým kanálom.

Protokol BB84 - bezpečná distribúcia kľúča

[Charles H Bennet, Gilles Brassard: Proc. IEEE Int. Conf. Computers, Systems, and Signal Processing, Bangalore, India, 1984, p. 175]

komunikácia: Alica \rightarrow Bob

budeme používať značenie (inšpirované polarizáciou fotónu):

štandardná báza: +

$$1 = |1\rangle = |\text{zvislo}\rangle$$

$$0 = |0\rangle = |\text{vodorovne}\rangle$$

Hadamartova báza: X

$$1 = |1\rangle = |+\rangle = |/\rangle$$

$$0 = |0\rangle = |-\rangle = |\backslash\rangle$$

Protokol BB84 - základná distribúcia kľúča

1. Alica generuje sadu náhodných báz a v nich náhodných qubitov a posiela ich Bobovi
2. Bob zachytáva qubity a meria ich. Pre každé meranie náhodne zvolí bázu a zmeria hodnotu qubitu. Ak zvolí rovnakú bázu ako Alica, zmeria rovnakú hodnotu qubitu. Ak zvolí inú bázu, výsledok merania je 0 alebo 1 s rovnakou pravdepodobnosťou.
3. Alica a Bob si porovnajú **bázy**, ktoré použili a vyznačia si zhodu.
4. Zdieľaný kľúč tvoria qubity, pri ktorých bola báza rovnaká.

Alicine bázy	x	+	+	x	x	+	+	+	x	x	+	+	x	+	x	+	x	x	+	+	+	x	x	+	x	+	+	+	x	+	+	x	
Alicine qubity	1	1	0	0	1	0	0	1	0	1	0	1	1	0	0	1	0	1	1	0	0	0	0	1	1	1	0	1	0	1	1	1	
Bobove bázy	x	x	x	x	+	+	+	x	+	+	+	x	x	x	+	+	+	+	x	x	+	+	+	+	+	+	x	x	+	+	x	x	x
Bobove qubity	1	1	0	0	1	0	0	1	0	1	0	1	1	0	0	1	0	1	1	0	0	0	0	1	1	1	0	1	0	1	1	1	
zhoda	✓			✓		✓	✓				✓	✓				✓					✓			✓				✓				✓	
kľúč	1			0		0	0				0	1				1					0			1				1				1	

Protokol BB84 - vplyv odpočúvania

5. Eva zachytáva Alicine qubity a snaží sa ich merať. Bázu však musí voliť náhodne, lebo ju nepozná.
6. Ak Eva zvolí odlišnú bázu ako Alica, jej meranie zmení stav! Eva pritom nemôže urobiť klon stavu a merať na ňom (veta o zákaze).
7. Bob meria tak ako predtým, aj bázy si môžu s Alicou porovnať tak ako predtým. Eva môže odpočúvať túto komunikáciu.
8. Ak Eva zmenila akceptovaný qubit, majú Alica a Bob odlišné kľúče.

Alicine bázy	x	+	+	x	x	+	+	+	x	x	+	+	x	+	x	+	x	x	+	+	+	x	x	+	x	+	+	+	x	+	+	x	
Alicine qubity	1	1	0	0	1	0	0	1	0	1	0	1	1	0	0	1	0	1	1	0	0	0	0	0	1	1	1	0	1	0	1	1	1
Evine bázy	x	+	x	+	x	x	+	+	x	+	x	+	+	+	x	x	+	x	+	x	+	+	x	x	x	+	+	+	+	x	+	x	
Evine qubity	1	1	0	1	1	1	0	1	0	0	1	1	0	0	0	1	1	1	1	0	0	1	0	0	1	1	0	1	0	1	0	1	
Bobove bázy	x	x	x	x	+	+	+	x	+	+	+	x	x	x	+	+	+	+	x	x	+	+	+	+	+	x	x	+	+	x	x	x	
Bobove qubity	1	1	0	0	1	1	0	1	0	0	1	1	1	0	0	0	1	1	1	0	0	1	0	1	1	1	0	1	0	1	1	1	
zhoda	✓			✓		✓	✓					✓		✓							✓			✓				✓				✓	
klúč Alica	1			0		0	0					0		1							0			1				1				1	
klúč Bob	1			0		1	0							1							0			1				1				1	

Protokol BB84 - odhalenie odpočúvania

9. Alica a Bob si porovnajú (obmedzený počet) n bitov. Ak nájdú odlišný bit, **odhalili odpočúvanie!** (A nebudú používať tento kľúč!)

Pravdepodobnosť, že Eva bude odhalená pri 1 porovnanom bite: $1/4$
 { $1/2$ (že E meria v inej báze ako A) x $1/2$ (B nameria opačne ako A)}

Pravdepodobnosť, že Eva ostane utajená pri n porovnaných bitoch: $3/4^n$

Pravdepodobnosť odhalenia odpočúvania: $P = 1 - (3/4)^n$

Alicine bázy	x	+	+	x	x	+	+	+	x	x	+	+	x	+	x	+	x	x	+	+	+	x	x	+	x	+	+	+	x	+	+	x
Alicine qubity	1	1	0	0	1	0	0	1	0	1	0	1	1	0	0	1	0	1	1	0	0	0	0	1	1	1	0	1	0	1	1	1
Evine bázy	x	+	x	+	x	x	+	+	x	+	x	+	+	+	x	x	+	x	+	x	+	+	x	x	x	+	+	+	+	x	+	x
Evine qubity	1	1	0	1	1	1	0	1	0	0	1	1	0	0	0	1	1	1	1	0	0	1	0	0	1	1	0	1	0	1	0	1
Bobove bázy	x	x	x	x	+	+	+	x	+	+	+	x	x	x	+	+	+	+	x	x	+	+	+	+	+	x	x	+	+	x	x	x
Bobove qubity	1	1	0	0	1	1	0	1	0	0	1	1	1	0	0	0	1	1	1	0	0	1	0	1	1	1	0	1	0	1	1	1
zhoda	✓			✓		✓	✓					✓		✓							✓			✓					✓			✓
klúč Alica	1			0		0	0					0		1							0			1				1			1	
klúč Bob	1			0		1	0					1		1							0			1				1			1	

Operácie na (klasických) bitoch - hradlá (gates)

NOT

0	1	1	0
1	0	0	1

OR

0	1	1	0
1	1	0	0
1	1	1	0

AND

0	1	1	0
1	1	0	0
0	1	0	0

XOR

0	1	1	0
1	1	0	0
1	0	1	0

SÚČET

	0	1	1	1	0
	1	1	1	0	0
1	0	1	0	1	0

SÚČIN

				0	1	1	0	6
				1	1	0	0	12
				0	0	0	0	
			0	0	0	0		
		0	1	1	0			
	0	1	1	0				
	1	0	0	1	0	0	0	72

Operácie na qubitoch - kvantové hradlá (quantum gates)

V kvantovej mechanike môžeme na qubit aplikovať akýkoľvek unitárny operátor. Príslušnú transformáciu stavu vieme znázorniť ako rotáciu na Blochovej sfére. (Unitárny operátor je taký, ktorý zachováva správnu normalizáciu stavu.)

Pauliho matice σ_i

$$\text{---} \boxed{X} \text{---} = \text{---} \boxed{\neg} \text{---} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \quad \text{---} \boxed{Y} \text{---} = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \quad \text{---} \boxed{Z} \text{---} = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

$$\text{---} \boxed{\sqrt{\neg}} \text{---} = \sqrt{\text{NOT}} = \frac{1}{2} \begin{pmatrix} 1+i & 1-i \\ 1-i & 1+i \end{pmatrix}$$

Hadamartov operátor

$$\text{---} \boxed{H} \text{---} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

Identita

$$\text{---} \boxed{I} \text{---} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

Príklad použitia (zmeny stavu)

$$|\psi\rangle \text{---} \boxed{H} \text{---} \boxed{X} \text{---} = \hat{X} \hat{H} |\psi\rangle$$

“otočenie” spinu do smeru x
a negácia stavu

Kvantové previazanie

Môže k nemu dôjsť, ak sú dve alebo viac častíc navzájom ovplyvnené jedna druhou. V takom prípade sú spoločne popísané **jedným** kvantovým stavom, a nie každá zvlášť.

Príklad: rozpad častice so spinom 0 na dve častice so spinom 1/2.



Celkový spin musí byť 0, ale nevieme, aký spin letí na akú stranu.

Vlnová funkcia v spinovej časti musí byť

$$|\psi^+\rangle = \frac{1}{\sqrt{2}} \left(|\uparrow_{\text{right}}\rangle |\downarrow_{\text{left}}\rangle + |\downarrow_{\text{right}}\rangle |\uparrow_{\text{left}}\rangle \right)$$

alebo

$$|\psi^-\rangle = \frac{1}{\sqrt{2}} \left(|\uparrow_{\text{right}}\rangle |\downarrow_{\text{left}}\rangle - |\downarrow_{\text{right}}\rangle |\uparrow_{\text{left}}\rangle \right)$$

Konečný stav sa nedá zapísať len ako jednoduchý súčin stavov jednotlivých qubitov. Takého stavu nazývame **previazané** (entangled).

Bellove stavy

Sada úplne previazaných stavov, ktorá tvorí **Bellovu bázu** systému 2 qubitov

$$|\phi^+\rangle = \frac{1}{\sqrt{2}} (|0_A\rangle|0_B\rangle + |1_A\rangle|1_B\rangle)$$

$$|\psi^+\rangle = \frac{1}{\sqrt{2}} (|0_A\rangle|1_B\rangle + |1_A\rangle|0_B\rangle)$$

$$|\phi^-\rangle = \frac{1}{\sqrt{2}} (|0_A\rangle|0_B\rangle - |1_A\rangle|1_B\rangle)$$

$$|\psi^-\rangle = \frac{1}{\sqrt{2}} (|0_A\rangle|1_B\rangle - |1_A\rangle|0_B\rangle)$$

V Bellových stavoch môžeme pri meraní na jednom qubite dostať 0 aj 1.

Merania na jednotlivých qubitoch vedú na vlastné stavy, ktoré tvoria **základnú bázu**:

$$|00\rangle = |0_A\rangle|0_B\rangle$$

$$|10\rangle = |1_A\rangle|0_B\rangle$$

$$|01\rangle = |0_A\rangle|1_B\rangle$$

$$|11\rangle = |1_A\rangle|1_B\rangle$$

Kvantová teleportácia

Spôsob, ako na inom mieste urobiť kópiu qubitu. Veta o zákaze klonovania vyžaduje, aby pôvodný qubit zanikol.

Úloha: Alica má stav $|q_A\rangle = a|0_A\rangle + b|1_A\rangle$

a chce ho preniesť Bobovi.

(a, b a priori nepoznáme, index A znamená, že stav je u Alice)

Podmienka: Alica a Bob musia zdieľať úplne previazaný stav (každý má z neho jeden qubit). Môže to byť ktorýkoľvek Bellov stav. Zvoľme ϕ^+ (indexy ukazujú, u koho sa daný qubit nachádza) a máme stav 3 qubitov

$$|q_A\rangle|\phi^+\rangle = (a|0_A\rangle + b|1_A\rangle) \frac{1}{\sqrt{2}} (|0_{A'}\rangle|0_B\rangle + |1_{A'}\rangle|1_B\rangle)$$

$$\begin{aligned} |q_A\rangle|\phi^+\rangle &= \frac{a}{\sqrt{2}} |0_A\rangle|0_{A'}\rangle|0_B\rangle + \frac{a}{\sqrt{2}} |0_A\rangle|1_{A'}\rangle|1_B\rangle \\ &+ \frac{b}{\sqrt{2}} |1_A\rangle|0_{A'}\rangle|0_B\rangle + \frac{b}{\sqrt{2}} |1_A\rangle|1_{A'}\rangle|1_B\rangle \end{aligned}$$

Kvantová teleportácia - postup

Alice na svojich dvoch qubitoch musí zmerať Bellov stav. Tým sa jej dva qubity previažu a stav pôvodného qubitu $|q_A\rangle$ zanikne. Systém skolabuje do jedného zo štyroch stavov, v ktorých superpozícii sa nachádzal:

$$\begin{aligned} |q_A\rangle|\phi^+\rangle &= \frac{1}{2} |\phi_A^+\rangle (a|0_B\rangle + b|1_B\rangle) + \frac{1}{2} |\phi_A^-\rangle (a|0_B\rangle - b|1_B\rangle) \\ &\quad + \frac{1}{2} |\psi_A^+\rangle (b|0_B\rangle + a|1_B\rangle) - \frac{1}{2} |\psi_A^-\rangle (b|0_B\rangle - a|1_B\rangle) \end{aligned}$$

Alica pošle Bobovi informáciu, ktorý zo štyroch Bellovych stavov zmerala.

Ak Alica našla $|\phi_A^+\rangle$ Bob na svoj qubit aplikuje \hat{I}

Ak Alica našla $|\phi_A^-\rangle$ Bob na svoj qubit aplikuje \hat{Z}

Ak Alica našla $|\psi_A^+\rangle$ Bob na svoj qubit aplikuje \hat{X}

Ak Alica našla $|\psi_A^-\rangle$ Bob na svoj qubit aplikuje \hat{Y}

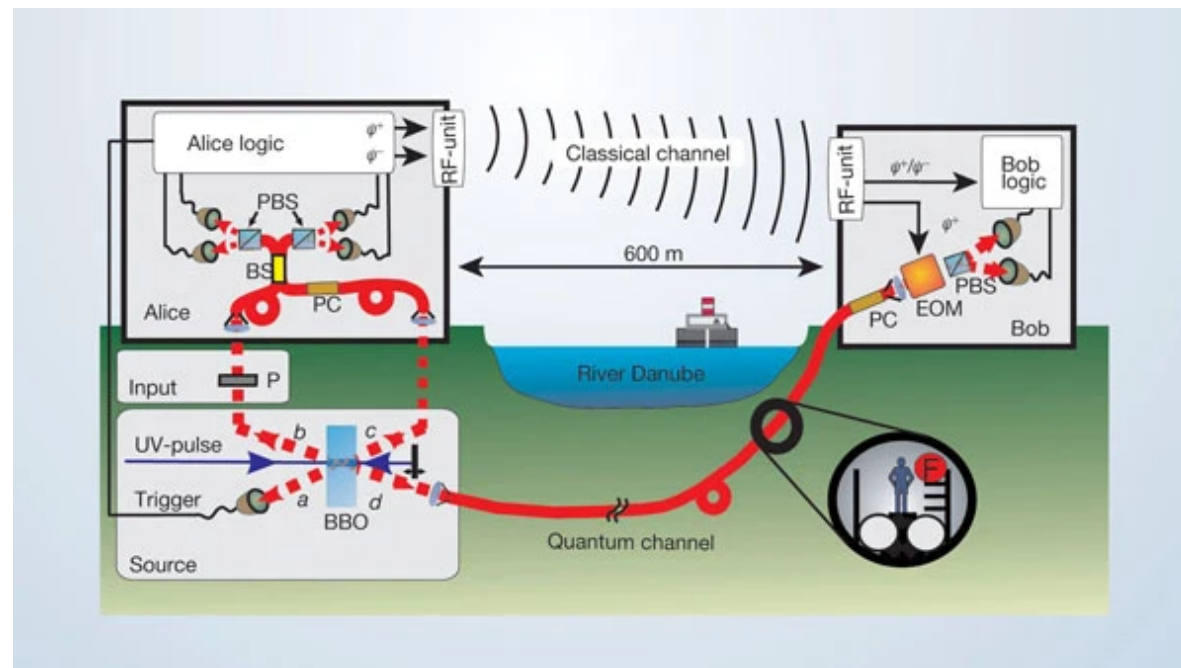
V každom prípade Bob získa stav $(a|0_B\rangle + b|1_B\rangle)$ ktorý u Alice zanikol

Kvantová teleportácia - realizácia

Návrh 1993: Bennet, Brassard, Crepeau, Josza, Peres, Wootters

Prvá realizácia 1997: Sandu Popescu, Anton Zeilinger

2004: teleportácia 600 cez Dunaj vo Viedni (Zeilinger), použité fotóny



[R. Ursin et al., Nature 430, 849 (2004)]

2012: teleportácia 143 km na Kanárskych ostrovoch (Zeilinger)

2015: teleportácia viacerých stupňov voľnosti, Hefei, Čína,
Chao-Yang Lu, Jian-Wei Pan

Maticová reprezentácia základnej bázy

Maticová reprezentácia základnej bázy pre 2 qubity

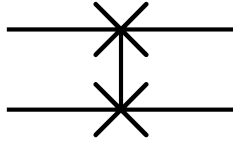
$$|ba\rangle = \begin{pmatrix} b_0 \times \begin{pmatrix} a_0 \\ a_1 \end{pmatrix} \\ b_1 \times \begin{pmatrix} a_0 \\ a_1 \end{pmatrix} \end{pmatrix} = \begin{pmatrix} b_0 a_0 \\ b_0 a_1 \\ b_1 a_0 \\ b_1 a_1 \end{pmatrix} \quad |00\rangle = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} \quad |01\rangle = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix}$$
$$|10\rangle = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix} \quad |11\rangle = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix}$$

Podobne je zostavená základná báza aj pre stavy z viacerých qubitov

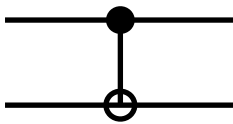
Hradlá pre viacero qubitov

Hradlá môžu prijímať aj viacero qubitov (matice sa vzťahujú na základnú bázu)

Príklady:

SWAP 
$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

vymieňa stavy dvoch qubitov

CNOT 
$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

neguje stav $|a\rangle$, ak je $|b\rangle$ v stave 1

... a iné. Kvantové algoritmy sa zostavujú z takýchto hradiel.

Kvantové počítače

- Špeciálne algoritmy!
- (Napríklad Shorov algoritmus na faktorizáciu (veľkých) čísel. Relevantné na prelomenie šifrovania v RSA algoritme.)
- Qubity sú obvykle realizované supravodivými obvodmi. (IBM, Google, Intel - v roku 2021 do 80 qubitov)
- Je možné navrhnuť vlastný kvantový algoritmus a poslať ho do IBM.
- Dosiahnutá **kvantová prevaha** (quantum supremacy): kvantový počítač rieši vybrané problémy rýchlejšie ako klasický. [Jiuzhang, Čína, fotónové qubity, 2020]

Procesor Sycamore (Google), inštalovaný v kryostate. Bol použitý na demonštráciu kvantovej prevahy a na veľké výpočty v kvantovej chémii.

