Wyklad9

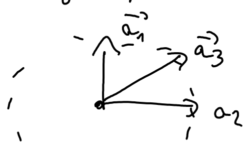
12 kwietnia 2011
22:39

1. Kryptografia kwantowa przy użyciu stanów splątanych (protokół Ekerta 1991, Ekert urodzony we Wrocławiu.)

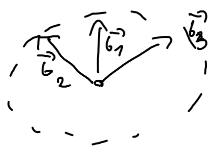
$$|\psi^-\rangle = \frac{1}{\sqrt{2}}(|0\rangle\otimes|1\rangle - |1\rangle\otimes|0\rangle)$$

A ——————————————— B

A wybiera 3 rodzaje pomiarów



B :



{ kierunki na sferze Blocha
odpowiadają wyborom bazy
$\vec{a}_1$ = pomiar $\updownarrow$
$\vec{a}_2$ = pomiar $\hat{X}$
$\vec{a}_3$ = pomiar $(22{,}5^\circ, 112{,}5^\circ)$

Wiemy że $C(\vec{a},\vec{b}) = \langle\psi^-| \vec{\sigma}\cdot\vec{a} \otimes \vec{\sigma}\cdot\vec{b}\, |\psi^-\rangle = -\vec{a}\cdot\vec{b}$

A i B wykonują pomiary przypadkowo w każdej z 2 baz

$\vec{a}_1, \vec{b}_1$
$\vec{a}_3, \vec{b}_2$ } wyniki idealnie antyskorelowane – mogą użyć jako klucz

ale muszą mieć pewność, że E nic nie wie

Upubliczniają pozostałe pomiary i liczą wielkość

Liczą:

$$S = C(\vec{a}_1,\vec{b}_2) + C(\vec{a}_1,\vec{b}_3) + C(\vec{a}_2,\vec{b}_3) - C(\vec{a}_2,\vec{b}_2)$$

Widzimy, że to jest ta sama wielkość występująca w nierównościach Bella. (czyli wiemy, że dla $|\psi^-\rangle$, $S = 2\sqrt{2}$

(Co więcej $2\sqrt{2}$ może dać tylko stan maks splątany)

A i B mają pewność, że ich bity są bezpieczne

(tak jak w BB84 gdy nie było błędów)

(więcej na ćwiczeniach)

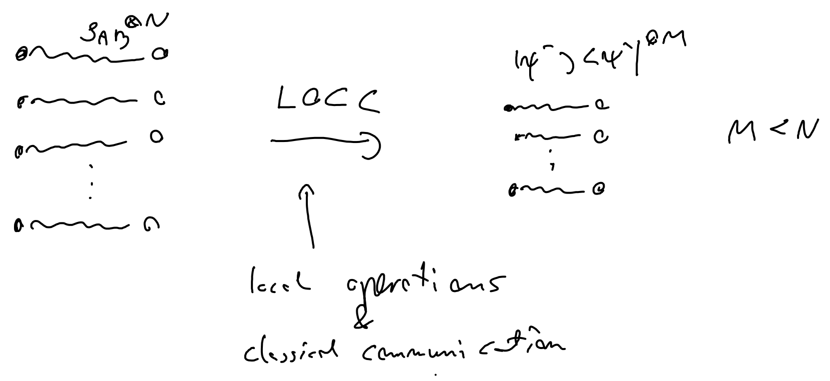
Intuicja: łamanie nierówności Bella oznacza, że nie istnieją „local realities", czyli w

nie istnieją „local realities", czyli w szczególności E nie mogła mieć osobno wysyłając stany o określonych polaryzacjach.

Innymi słowy nawet jeśli nasz stan przygotowała E to pomiary bezpieczne „bo wartości bitów klucza stają się określone dopiero w wyniku naszych pomiarów". Wcześniej ich nie było a E nie jest z nami splątana.

W praktyce oczywiście mogłby nie zmierzyć $2\sqrt{2}$, będzie trochę mniej. Ważne i trudne pytanie o ile mniej może być żeby wciąż można było zrobić privacy amplification?

Ciekawe podejście: Quantum privacy amplification (Destylacja splątania)



2. Klonowanie stanów kwantowych

Jeśli myślimy o stanach kwantowych jako o nośnikach informacji, pojawia się naturalne pytanie: Czy można informację zapisaną w stanach kwantowych kopiować? Kluczowa kwestia bo jeśli się da ...

Kluczowa kwestia bo pozli się do ....

a) BB84 nie jest bezpieczne ▽

b) Można jest rozróżnić nieortogonalnych stanów kwantowych

$|\psi\rangle, |\varphi\rangle$ st. nie ortogonalne. $0<\langle\psi|\varphi\rangle<1$

Wiemy że $p_e = \frac{1}{2}\left(1 - \sqrt{1-|\langle\psi|\varphi\rangle|^2}\right)$

Ale jeśli można je przepisać przez mocowanie:

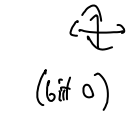
$|\psi\rangle \longrightarrow |\psi\rangle^{\otimes N}$

$|\varphi\rangle \longrightarrow |\varphi\rangle^{\otimes N}$

to $p_e^{(N)} = \frac{1}{2}\left(1 - \sqrt{1 - \underbrace{|\langle\psi|\varphi\rangle^{\otimes N}|^2}_{|\langle\psi|\varphi\rangle|^{2N}}}\right) \xrightarrow{N\to\infty} 0$!

c) Przeczytaliśmy to w szczególności na komunikacje ponad światłem:

A decyduje czy mamy w bicie:



B ma

$|\leftrightarrow\rangle$ lub $|\updownarrow\rangle$

$|\nearrow\rangle$ lub $|\searrow\rangle$

Ale B może teraz skalować swój stan i dokładnie stwierdzić co dostał. Więc będzie wiedział dokładnie w jakiej bazie znajduje A !

Tw. Klonowanie nieortogonalnych stanów kwantowych jest niemożliwe

Dowód (Nie wprost) Niech $|\psi\rangle, |\varphi\rangle$, $0 < |\langle\psi|\varphi\rangle| < 1$

Zatem że istnieje operacja zgodna z mech. kwantową (cp. unitarna) kopiująca klonowanych obu stanów. Matematycznie:

"czysta kartka" — maszyna klonująca

$$|\psi\rangle \otimes |0\rangle \otimes |A\rangle \xrightarrow{U} |\psi\rangle \otimes |\psi\rangle \otimes |A_\psi\rangle$$

$$|\varphi\rangle \otimes |0\rangle \otimes |A\rangle \longrightarrow |\varphi\rangle \otimes |\varphi\rangle \otimes |A_\varphi\rangle$$

2 unitarności:

$$\langle\psi|\varphi\rangle \underbrace{\langle 0|0\rangle}_{1} \langle A|A\rangle = \langle\psi|\varphi\rangle \langle\psi|\varphi\rangle \langle A_\psi|A_\varphi\rangle$$

$$\underbrace{\langle\varphi|\psi\rangle}_{\neq 0} \cdot \Big(1 - \underbrace{\langle\psi|\varphi\rangle \langle A_\psi|A_\varphi\rangle}_{<1}\Big) = 0$$

sprzeczność ▨

Ull.... Klonować się nie da.