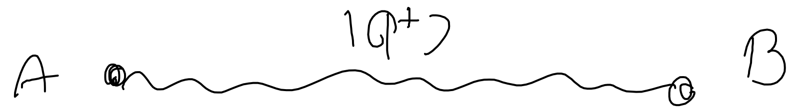
Entanglement based QKD

(Ekert 91)
E91



A wybiera pomiar w bazie $|0\rangle, |1\rangle$ lub $|+\rangle |-\rangle$ przygotowuje w B stan identyczny. Mamy ef. protokół BB84.

Aby mieć pewność że E nie ma wpływu wiedzy mamy sprawdzić łamanie nierówności Bella. (wybierając jeszcze pomiary w innych bazach)

Bardziej ilościowo trzeba by pokazać monogamię CHSH

$$|\langle C\rangle_{AB}| + |\langle C\rangle_{AC}| \leq 4$$

czyli gdy łamiemy w AB to mamy silniejsze korelacje między A B niż np. AC.

Destylacja splątania

Chcemy myśleć o splątaniu jako o zasobie

Np. $|\phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$

pozwala na teleportację 1 qubitu (przesyłając 2 cbity)

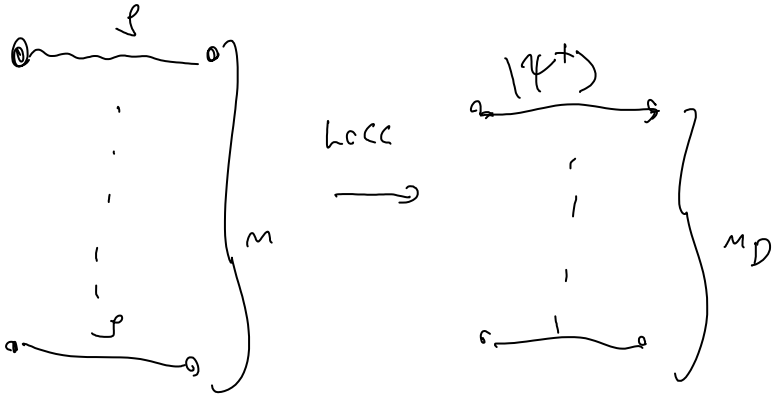
a pozwala na przesłanie 2 bitów info za pomocą 1 qubitu

(Dense coding)

Mamy ilość splątania w max-splątanym stanie 2 qubitów

1 ebit

Chcemy splątanie dla innych stanów wyrazić w ebitach.



Destylowalne splątanie:

$$E_D(\rho) = \sup \lim_{n\to\infty} \frac{n_D}{n}$$ w optymalnym protokole

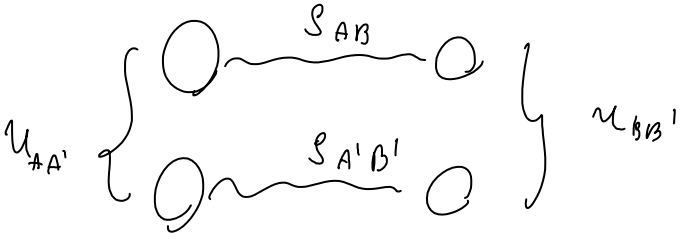
Fakt: Dla wszystkich stanów splątanych dwóch qubitów $E_D > 0$.

Przykład:

$$\rho_{AB} = p|\phi^+\rangle\langle\phi^+| + (1-p)|\psi^+\rangle\langle\psi^+|$$

Mamy wiele kopii i chcielibyśmy uzyskać obok siebie

Koniec mieć $\rho_{AB} \approx |\phi^+\rangle\langle\phi^+|$



$U_{AA'}\ |i\rangle \otimes |j\rangle = |i\rangle \otimes |i \oplus j \bmod 2\rangle$

$U_{BB'}$ - ~

$U_{AA'} \otimes U_{BB'}$ $|\Phi^+\rangle_{AB} \otimes |\Phi^+\rangle_{A'B'} = |\Phi^+\rangle|\Phi^+\rangle$

$|\Phi^+\rangle \otimes |\Psi^+\rangle = |\Phi^+\rangle|\Psi^+\rangle$

$|\Psi^+\rangle |\Phi^+\rangle = |\Psi^+\rangle|\Phi^+\rangle$

$|\Psi^+\rangle |\Psi^+\rangle = |\Psi^+\rangle|\Phi^+\rangle$

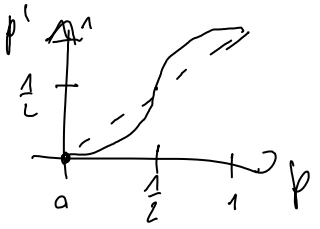
Mamy $A'B'$ i zostawiają te gdzie mają zgodne

$\rightarrow p^2 |\Phi^+\rangle\langle\Phi^+| + (1-p)^2 |\Psi^+\rangle\langle\Psi^+|$

normujemy

$\equiv p' |\Phi^+\rangle\langle\Phi^+| + (1-p') |\Psi^+\rangle\langle\Psi^+|$

$p' = \frac{p^2}{p^2 + (1-p)^2}$



Jeśli zaczniemy z $p > \frac{1}{2}$ mamy destylację i w końcu $\rightarrow |\Phi^+\rangle\langle\Phi^+|$.

Podobnie dla $|\Psi^+\rangle$. Tylko jak $p = \frac{1}{2}$ destylacja nie zwiększa, ale wtedy stan separowalny !

Na destylacje splatania można patrzec jak na kwantowa wersje privacy amplification. (troche mocniejsze bo mamy two-way disitllation co może nie mieć opdowiednika w standardowym BB84 + classical postprocessing)

No-cloning i inne twierdzenia

. 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 pozwoli się do ....

Kluczowa kwestia bo jeśli się da ....

a) BB84 nie jest bezpieczne !

b) Możliwe jest rozróżnianie nieortogonalnych stanów kwantowych

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

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

Ale jeśli można je przepisać przez maszynę:

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

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

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

c) Pozwoliłoby to w szczególności na komunikację ponad świetlną:

A ∘ $|\psi\rangle$ ∘ B

A decyduje czy mierzy w bazie: B ma

⊕ (bit 0) — $|\leftrightarrow\rangle$ lub $|\updownarrow\rangle$

czy

⊗ (bit 1) — $|\nearrow\rangle$ lub $|\searrow\rangle$

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

<u>Tw. Klonowanie nieortogonalnych stanów kwantowych jest niemożliwe</u>

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

Zatem że istnieje operacja zgodna z mech kwantowej (op. unitarna) klonująca klonowalne obie stany. 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:

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

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

$\neq 0$

sprzeczność

Ufff.... Klonować się nie da.

Pamiętamy że w teleportacji nieznane stany były mieszane. Czyli wszystko OK.