

Kwantowa kryptografia i związane splątanie

Wydział Fizyki i Matematyki
Stosowanej,
Politechnika Gdańska

K. M. P. Horodeccy, J. Oppenheim,

Wydział Matematyki,
Fizyki i Informatyki
Uniwersytet Gdański

Instytut Fizyki
Teoretycznej i
Astrofizyki,
Uniwersytet Gdański

Wydział Matematyki
Stosowanej i Fizyki
Teoretycznej
Uniwersytet Cambridge

W ramach projektów: RESQ, QUPRODIS
Kierownictwo - R. Horodecki

Quant-ph/0309110 (przesłane do Phys. Rev. Lett.)

Kwantowa teoria informacji

KUBIT (kwantowy bit)

- układ fizyczny dwustanowy
- np. cząstka o spinie 1/2
- ~ 2-wymiarowa przestrzeń Hilberta

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

EBIT (entangled bit)

- układ fizyczny złożony (dwa podukłady: A i B)

~ il. tensorowy przestrzeni Hilberta: $H'' = H \otimes H$

- np. „stan kota Schroedingera” - **singlet**

$$\Psi_{AB}^+ = \frac{1}{\sqrt{2}} [|0\rangle_A \otimes |0\rangle_B + |1\rangle_A \otimes |1\rangle_B]$$

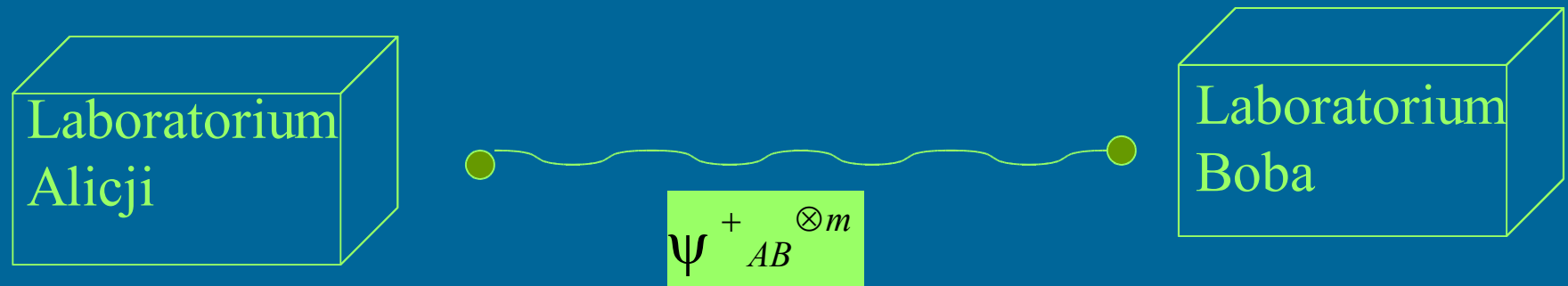
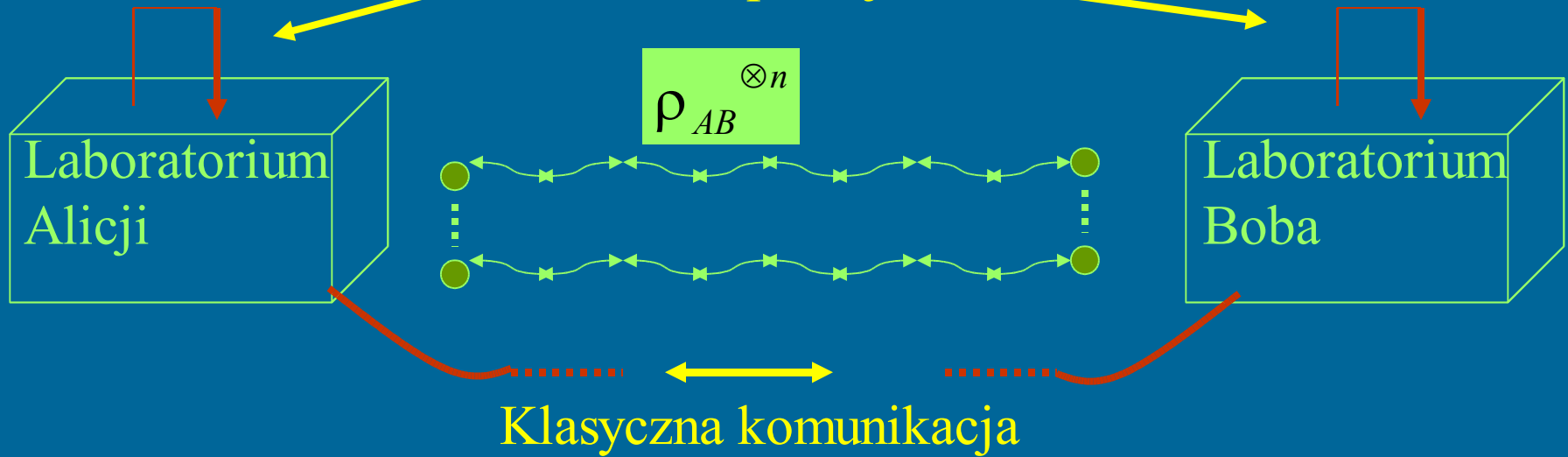
STAN MIESZANY

- ρ jest mieszanką stanów $\Psi^{(i)}$ zgodnie z rozkładem $\{p_i\}$

$$\rho = \sum_i p_i |\Psi^{(i)}\rangle\langle\Psi^{(i)}|$$

Przetwarzanie stanów dwuukładowych

Lokalne operacje



[Bennett et.al. '96]

Pojęcie splątania

Stan kwantowy ρ jest **splątany**, jeżeli nie można go przedstawić w postaci mieszanki stanów produktowych :

$$\rho \neq \sum_i p_i \rho_A^{(i)} \otimes \rho_B^{(i)}$$

w sytuacji przeciwnej, stan nazywamy **separowalnym**

Miara splątania - dowolna funkcja macierzy gęstości,

która nie wzrasta ze względu na LOKK

Przykład: 1) operacyjna miara splątania :

Splątanie destylacji $E_D(\rho)$: maksymalna liczba *singletów* (w przeliczeniu na parę) do jakiej można sprowadzić dany stan ρ za pomocą operacji LOKK

2) „matematyczna” miara splątania :

Względna entropia splątania : $E_R(\rho) = \inf_{\sigma \in SEP} S(\rho \parallel \sigma)$

Stany o związanym splątaniu

Def. Stany o **związanym splątaniu** (bound entangled) to stany splątane, niedestylowalne.

Def. Stany PPT (positive partial transpose) :

$$[I_A \otimes T_B](\rho_{AB}) \geq 0$$

Splątane stany PPT są niedestylowalne : $E_D(\rho) = 0$

- Do wytworzenia ρ potrzeba ebitów
 - Po utworzeniu ρ , nie można otrzymać z ρ żadnego ebitu
- [MPR. Horodeccy '98]

Stany o związanym splątaniu są „czarnymi dziurami” teorii splątania

[B.Terhal et al. Physics Today '03]

Klucz klasyczny i kwantowy

Klasyczny klucz kryptograficzny:

zmienna losowa $(X,Y)_K$ o rozkładzie :

$$P(X = 0, Y = 0) = P(X = 1, Y = 1) = \frac{1}{2}$$

oraz jeśli Z - zmienna podsłuchującego : $P(X,Y,Z) = P(X,Y)P(Z)$

Szyfr Vernama

Kwantowy klucz kryptograficzny:

stan kwantowy ρ :

$$\rho = \frac{1}{2} [|00\rangle\langle 00| + |11\rangle\langle 11|]_{AB} \otimes \rho_E$$

Obserwacja : jeżeli Alicja i Bob mają klucz kwantowy,
to mają także klucz klasyczny.

Związki kryptografii ze splątaniem

1) Protokół Ekerta z 1991

2) Tajne skorelowane bity (klucz klasyczny) to zasób o własnościach analogicznych do splątania.

Monotoniczność
ze względu na LOPK



Monotoniczność ze względu
na LOKK

A i B mają klas. klucz



A i B posiadają singlet

Nikt nie podsłuchuje



Nikt nie jest dokorelowany
kwantowo.

3) Dowody bezpieczeństwa protokołów BB84 [Shor, Preskil '00] i B92 [Tamaki et al. '03].

Ewa nie potrafi odróżnić protokołów BB84 oraz B92
od pewnych protokołów destylacji splątania !

Kwantowe zwiększanie bezpieczeństwa (quantum privacy amplification)

$$\rho_{AB}^{\otimes n}$$

Stan skorelowany
z Ewą

Destylacja (quantum
privacy amplification)

$$\Psi_{AB}^{\otimes m}$$

Odkorelowany od
Ewy kwantowo (jako
stan czysty)

Pomiar w
bazie
standardowej
 $|0\rangle, |1\rangle$

$$\frac{1}{2} [|00\rangle\langle 00|_{AB} + |11\rangle\langle 11|_{AB}]$$

Też odkorelowany od
Ewy kwantowo, gdyż
nie było komunikacji A z B.

Problem teoretycznej kryptografii kwantowej

Dany jest stan czysty Ψ_{ABE} , którego podukłady mają odpowiednio Alicja, Bob i Ewa.

Czy Alicja i Bob mogą uzyskać kwantowy klucz tj.

stan $\frac{1}{2} [|00\rangle\langle 00|_{AB} + |11\rangle\langle 11|_{AB}] \otimes \rho_E$?

(Zakładamy, że Alicja i Bob pracują na N kopiach stanu Ψ_{ABE})

Fakt : Jeżeli podukład AB stanu Ψ_{ABE} jest destylowalny,

Alicja i Bob dostaną klucz po wydestylowaniu singletu (QPA)

Hipoteza : „Ze stanu Ψ_{ABE} można dostać kwantowy

klucz TYLKO WTEDY, gdy jego podukład AB
jest destylowalny” [folklor ostatnich lat]

Weryfikacja hipotezy :

Twierdzenie : Hipoteza [folklor] jest nieprawdziwa.
Istnieją stany o związanym splątaniu, z których można
otrzymać kwantowy klucz.

Idea dowodu :

- 1) wyprowadzenie ogólnej postaci stanów, które mają idealny klucz (stany bezpieczne)
- 2) stany bezpieczne można przybliżać pewnymi stanami PPT: $\sigma(d, l, p)$
- 3) stany $\sigma(d, l, p)$ są splątane, gdyż można z nich dostać klucz .

[KMP. Horodeccy, J.Oppenheim '03]

Efekt parowania „czarnych dziur” - stanów ze związanym splątaniem.
: dają klucz kryptograficzny

Stany bezpieczne (private states)

Twierdzenie: Jedyne dwuukładowe stany, które po pomiarze w bazie standardowej $\{|00\rangle, |01\rangle, \dots, |d-1, d-1\rangle\}$ dają kwantowy klucz są postaci:

$$\gamma = U |\Psi_+\rangle\langle\Psi_+|_{AB} \otimes \rho_{A'B'} U^\dagger$$

U - transformacja unitarna kontrolowana bazą standardową:

$$U = \sum_{i,j=0}^{d-1} |ij\rangle\langle ij|_{AB} \otimes U_{A'B'}^{(ij)}$$

Stan $\rho_{A'B'}$ **jest dowolny**, Alicja posiada część AA' stanu γ ,
Bob BB', **Ewa posiada dopełnienie stanu** γ do stanu czystego:

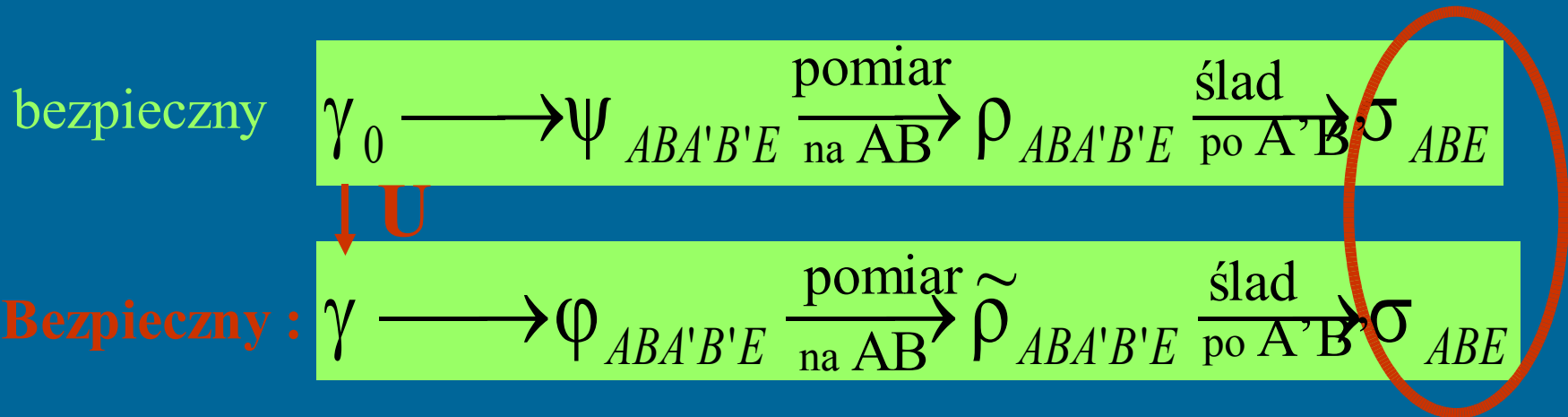
$$\text{Tr}_E |\Psi_{ABA'B'E}\rangle\langle\Psi_{ABA'B'E}| = \gamma$$

Stan $|\Psi_+\rangle\langle\Psi_+|_{AB}$ **jest dowolnym stanem maksymalnie splątany**

(\Leftarrow) Stany postaci γ są bezpieczne

Fakt: stan $\gamma_0 = |\psi_+\rangle\langle\psi_+|_{AB} \otimes \rho_{A'B'}$ jest bezpieczny.

Twierdzenie : Transformacja kontrolna U , kontrolowana bazą B , nie zmienia bezpieczeństwa stanu w tej bazie.



(\Rightarrow) Każdy stan 100% bezpieczny jest postaci γ

$$\psi_{ABA'B'E} = \frac{1}{\sqrt{2}} \left[\underline{|00\rangle}_{AB} \otimes \psi_{A'B'E}^{(00)} + \underline{|11\rangle}_{AB} \otimes \psi_{A'B'E}^{(11)} \right]$$

$$\underline{\psi_{A'B'E}^{(00)}} = \sum_i |i\rangle_{A'B'} X |i\rangle_E$$

$$X = U_0 \rho_X U_0^{-1}$$

$$\underline{\rho_E^{(00)}} = U_0 \rho U_0^{-1}$$

$$\underline{\psi_{A'B'E}^{(11)}} = \sum_i |i\rangle_{A'B'} Y |i\rangle_E$$

$$Y = \tilde{U}_0 \rho_Y \tilde{U}_0^{-1}$$

$$\underline{\rho_E^{(11)}} =$$

Postać ostateczna :

$$\frac{1}{2} \begin{matrix} 00 & 01 & 10 & 11 \\ 00 & 01 & 10 & 11 \end{matrix} \begin{bmatrix} U_1 \rho U_1^{-1} & 0 & 0 \parallel U_1 \rho \tilde{U}_1^{-1} \parallel & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ U_1^{-1} \rho \tilde{U}_1 & 0 & 0 & \tilde{U}_1 \rho \tilde{U}_1^{-1} \end{bmatrix}$$

Parametr
bezpieczeństwa !

$$= \gamma_{ABA'B'}$$

Qed.

Klucz kwantowy = stany bezpieczne

Twierdzenie : Alicja i Bob mogą wydestylować m bitów klucza kwantowego, $\Leftarrow \Rightarrow$ gdy mogą wydestylować stan bezpieczny z którego po pomiarze na układzie AB można otrzymać m bitów kwantowego klucza

Dowód :

(\Leftarrow) wynika z definicji stanu bezpiecznego.

(\Rightarrow) każdy protokół kwantowy można zaimplementować zamykając układ :

śląd częściowy = oddanie podukładu Ewie

pomiar = czysta ancilla + transformacja unitarna + „wewnętrzne wyśladowanie układu ancilli.

Q.E.D

Przykłady stanów bezpiecznych :

Stany bezpieczne typu „singlet z flagami”

$$p\psi_{AB}^{+} \otimes \rho_{A'B'}^{(1)} + (1-p)\psi_{AB}^{-} \otimes \rho_{A'B'}^{(2)}$$

Stany „flagowe” spełniają:

$$\rho_{A'B'}^{(1)} \perp \rho_{A'B'}^{(2)}$$

Przykładowe stany „flagowe” - Stany kryjące (hiding states) :

$$\tau_2 = \rho_S^{\otimes l}$$

oraz

$$\tau_1 = \left[\frac{1}{2}(\rho_S + \rho_A) \right]^{\otimes l}$$

Stany Wernera :
symetryczny i
antysymetryczny

przy $l \longrightarrow \infty$ oraz $d \longrightarrow \infty$ stają się :

- 1) globalnie ortogonalne
- 2) nierozróżnialne przy pomocy LOKK,

Stany PPT, którymi można przybliżać stany bezpieczne

$$\sigma(d, l, p) = \begin{bmatrix} \frac{p}{2}(\tau_1 + \tau_2) & 0 & 0 & \frac{p}{2}(\tau_1 - \tau_2) \\ 0 & (\frac{1}{2} - p)\tau_2 & 0 & 0 \\ 0 & 0 & (\frac{1}{2} - p)\tau_2 & 0 \\ \frac{p}{2}(\tau_1 - \tau_2) & 0 & 0 & \frac{p}{2}(\tau_1 + \tau_2) \end{bmatrix}$$

Idea : ukrywamy splątanie:

- 1) stany flagowe kryjące \longrightarrow nie możemy rozróżnić singletów
- 2) stany flagowe są separowalne \longrightarrow nie wnoszą splątania

Ponadto : pbit mieszamy z szumem aby zapewnić PPT-owość.

Dobieramy odpowiednie d oraz l dla pewnych p .

Protokół wydobywania klucza z $\sigma(d,l,p)$

1) Ustalamy dokładność protokołu $\varepsilon > 0$

2) Uproszczony **protokół rekurencji** daje przy $p > \frac{1}{4}$ zwiększanie parametru bezpieczeństwa:

Wyniki
przeciwnie
Obie pary
usuwamy



Wyniki zgodne



Liczba par N tak duża aby : $\| [\frac{p}{2}(\tau_1 - \tau_2)]^{\otimes n} \| \approx \frac{1}{2} - \varepsilon$

3) Alicja wykonuje pomiar w bazie obliczeniowej

4) Dla dużych N stan po „rekurencji” i pomiarze spełnia warunek protokołu „haszującego” [Devetak, Winter ‘03] :

$$I_q(A : B) - I_q(A : E) > 0$$

Czy stany $\sigma(d,1,p)$ są splątane ?

Def. Operacyjna miara klucza kwantowego:

Klucz destylacji $K_D(\rho)$: maksymalna ilość klucza (w przeliczeniu na parę) do jakiej można sprowadzić dany stan ρ za pomocą operacji LOPK

Twierdzenie: $K_D(\rho) \leq E_R^\infty(\rho)$, gdzie $E_R^\infty(\rho) = \lim_{n \rightarrow \infty} \frac{E_R(\rho^{\otimes n})}{n}$

Idea dowodu :

1) Z monotoniczności względnej entropii ze względu na LOKK :

$$E_R(\rho^{\otimes n}) \geq E_R(\gamma'_m)$$

Prawie bezpieczny stan

2) Pokazujemy

$$E_R(\gamma'_m) \geq m$$

Przykład zastosowania : Stany antysymetryczne Wernera:

Koszt splątania =1, Klucz destylacji $\longrightarrow 0$, gdyż

$$E_R = \log\left(\frac{d+2}{d}\right)$$

Podsumowanie

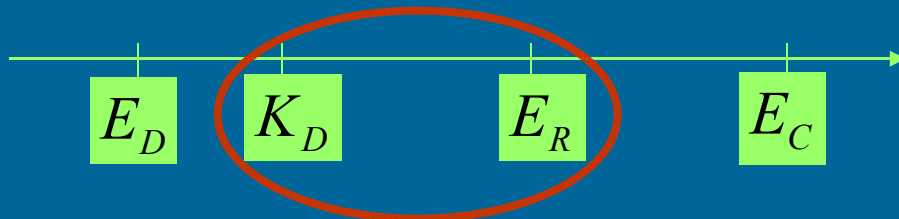
1. Wyprowadzenie ogólnej klasy stanów zawierających w pełni bezpieczny klucz (STANY BEZPIECZNE)
2. Kwantowy klucz kryptograficzny = \singlety
Kwantowy klucz kryptograficzny = stany bezpieczne, które można aproksymować stanami PPT
3. Pierwsza próba zrozumienia związanego splątania.
Zawierają „związany” singlet.
4. Klucz destylacji jest operacyjną miarą splątania.
5. Klucz destylacji jest ograniczony z góry przez względną entropię splątania.

PROBLEMY OTWARTE :

I Związki z kryptografią praktyczną :

Czy jest możliwe odróżnienie stanów PPT bezpiecznych od stanów separowalnych w sposób wydajny ?

II Relacje klucza destylacji do innych miar splątania



Czy zachodzi : $K_D = E_R$?

III Splątanie = kwantowy klucz kryptograficzny ?

KONIEC.