Wykład 7

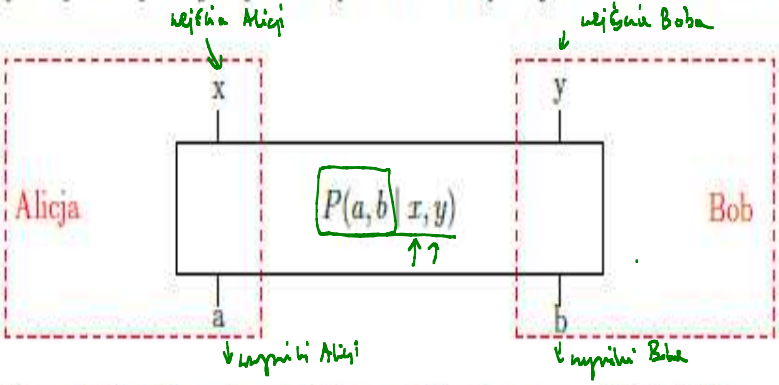
Kryptografia niezależna od urządzenia

W tym wykładzie omówimy tak zwaną kwantową kryptografię Device-Indepenent (niezależną od urządzenia). Stanowi ona rozwiązanie problemu gdy kwantowe urządzenia, które używamy w protokole nie sa zaufane i mogły być wytworzone lub zmodyfikowane przez Ewę.

1. Protokół DI jest uogólnieniem protokołu E91.

2. Bezpieczeństwo DI jest silniejsze niż kwantowe! Mechanika kwantowa jest wymagana tylko aby uczciwy producent mógł wyprodukować działające urządzenie do generowania klucza kryptograficznego (tak zwana honest implementation). Jednak bezpieczeństwo może być zapewnione nawet względem Ewy, która ma możliwości większe niż kwantowe (wystarczy, że Ewa spełnia zasady nie sygnalizowania [no-signalling]).

Rozważmy abstrakcyjne urządzenie współdzielone przez Alicję i Boba (w praktyce rozpatruje się też urządzenia dla większej ilości osób tak zwane multi



Rysunek 7.1: Kwantowe układy współdzielone przez Alicję i Boba. x oraz y oznaczają odpowiednio wejścia Alicji i Boba natomiast ax oraz b to ich wyjścia.

party cryptography). W urządzeniu tym zarówno Alicja jak i Bob mają do dyspozycji wejście i wyjście. Przyjmijmy oznaczenia $x \in \{0, \ldots, d_x - 1\}$ - wejście Alicji, $y \in \{0, \ldots, d_y - 1\}$ - wejście Boba, $a \in \{0, \ldots, d_a - 1\}$ - wyjście Alicji, $b \in \{0, \ldots, d_b - 1\}$ - wyjście Boba. Wtedy, działanie takiego urządzenia może być określone przez rozkład prawdopodobieństwa dany wzorem

$$P(a, b \mid x, y). \tag{7.1}$$

Aby powyższy zestaw był rozkładem prawdopodobieństwa muszą zostać spełnione warunki:

- Dla każdego x, y, a, b musi zachodzić $P(a, b \mid x, y) \geqslant 0$.
- Dla każdego x, y musi zachodzić $\sum_{a,b} P(a, b \mid x, y) = 1$.

ex: $\sum_{a,b=0}^{1} P(a\,b \mid 0\,0) = 1$

2 binarne wejścia
2 binarne wyjścia

Przejdźmy teraz do sytuacji gdy $d_x = d_y = d_a = d_b = 2$. Wtedy powyższy rozkład prawdopodobieństwa można zapisać jako macierz w następującej postaci

$$P(a, b \mid x, y) = \begin{bmatrix} P(00 \mid 00) & P(10 \mid 00) & P(00 \mid 10) & P(10 \mid 10) \\ P(01 \mid 00) & P(11 \mid 00) & P(01 \mid 10) & P(11 \mid 10) \\ P(00 \mid 01) & P(10 \mid 01) & P(00 \mid 11) & P(10 \mid 11) \\ P(01 \mid 01) & P(11 \mid 01) & P(01 \mid 11) & P(11 \mid 11) \end{bmatrix} \tag{7.2}$$

Zobaczmy 3 przykłady

$$\text{a)} \begin{bmatrix} 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}, \quad \text{b)} \begin{bmatrix} \frac{1}{2} & 0 & \frac{1}{2} & 0 \\ 0 & \frac{1}{2} & 0 & \frac{1}{2} \\ \frac{1}{2} & 0 & \frac{1}{2} & 0 \\ 0 & \frac{1}{2} & 0 & \frac{1}{2} \end{bmatrix}, \quad \text{c)} \begin{bmatrix} 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{bmatrix}. \tag{7.3}$$

$x=0$ $x=1$
statystyka
$P(b|y)$
powinna być mierzona od x

Interesujące układy powinny spełniać zasadę niesygnalizowania to znaczy pomiary po jednej stronie układu nie mogą zmieniać wyników po drugiej stronie. Formalnie zapiszemy to jako

Definicja 20 (Niesygnalizowanie). *Układ $P(a, b \mid x, y)$ nazywamy niesygnalizującym (NS) jeśli*

$$\forall_{b,x,x',y} \sum_a P(a, b \mid x, y) = \sum_a P(a, b \mid x', y) \tag{7.4}$$

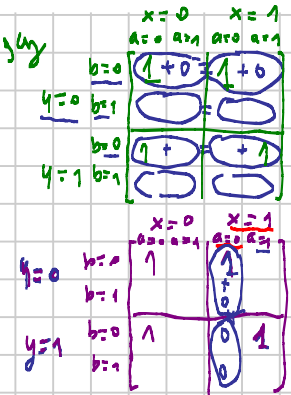
$A \not\to B$

oraz

$$\forall_{a,y,y'} \sum_b P(a, b \mid x, y) = \sum_b P(a, b \mid x, y') \tag{7.5}$$

$A \not\leftarrow B$

układ c) jest sygnalizujący od Boba do Alicji



$A \not\to B$

$x = 1$
$a = 0$
$B \to A$

Wniosek: Ten układ jest nieczasowy (niezgodny z OTW i STW)

Fizyczne można zapewnić, żeby układy nie sygnalizowały, rozdzielając podukłady na odpowiednio dużą odległość i wykonując pomiary tak szybko, żeby nawet informacja poruszająca się z prędkością światła w próżni ($c = 299792458$ m/s) nie mogła przekazać informacji o pomiarze między podukładami.

Definicja 21 (Lokalność). *Układ $P(a,b \mid x,y)$ nazywamy lokalnym ($\mathcal{L}$) jeśli*

$$P(a,b \mid x,y) = \sum_\lambda p_\lambda P^A_\lambda(a \mid x) P^B_\lambda(b \mid y) \tag{7.6}$$

gdzie dla każdego λ mamy $p_{\lambda \geqslant 0}$ oraz $\sum_\lambda p_\lambda = 1$.

Jeśli układu nie można przedstawić w powyższej postaci to mówimy, że jest nielokalny.

Definicja 22 (Układ kwantowy). *Układ $P(a,b \mid x,y)$ nazywamy kwantowym ($\mathcal{Q}$) jeśli*

$$P(a,b \mid x,y) = \mathrm{Tr}(\rho_{AB} M_{a|x} \otimes M_{b|y}) \tag{7.7}$$

gdzie ρ_{AB} jest stanem kwantowym dowolnego wymiaru współdzielonym przez Alicję i Boba a $M_{a|x}$ oraz $M_{b|y}$ to operatory pomiaru Alicji i Boba odpowiedni.

Można pokazać, że $\mathcal{L} \subsetneq \mathcal{Q} \subsetneq \mathcal{NS}$.

Twierdzenie 10 (Tsirelson 1980 [53]). *Dla dowolnego układu kwantowego zachodzi*

$$|CHSH(P(a,b \mid x,y))| \leqslant 2\sqrt{2}. \tag{7.8}$$

Dowód. Niech A_i, B_j, $i,j \in \{0,1\}$ będą obserwablami takimi, że $A_i^2 = I, B_j^2 = I$ o wartościach własnych ± 1. Zdefiniujmy H następująco

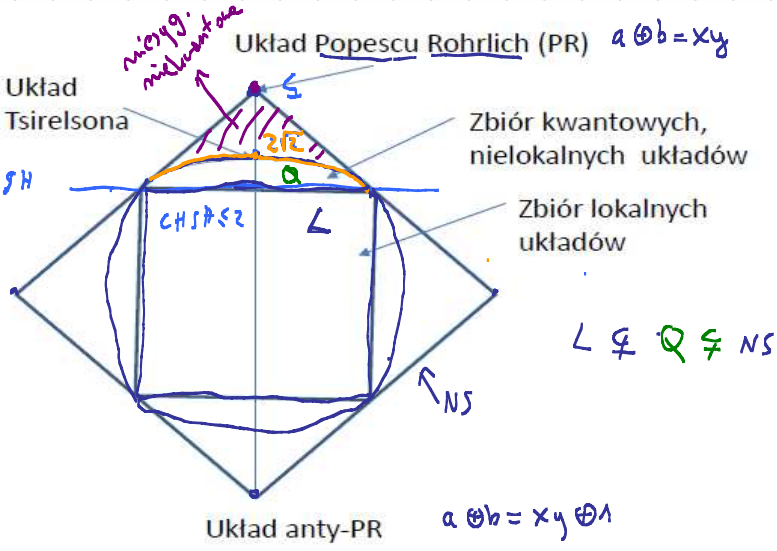
$$H := A_0 \otimes B_0 + A_0 \otimes B_1 + A_1 \otimes B_0 - A_1 \otimes B_1. \tag{7.9}$$

Ponieważ

$$\sup_{\rho = \sum_i p_i |\Psi_i\rangle\langle\Psi_i|} \mathrm{Tr}\,\rho H = \sup_{|\Psi\rangle} \mathrm{Tr}\,|\Psi\rangle\langle\Psi| H \tag{7.10}$$

wystarczy ograniczyć analizę do przypadku stanów czystych.

$$\begin{aligned} H^2 =& (A_0 \otimes (B_0 + B_1) + A_1 \otimes (B_0 - B_1))^2 \\ =& I \otimes ((B_0 + B_1)^2 + (B_1 - B_0)^2) \\ &+ [A_0 A_1 \otimes (B_0 + B_1)(B_0 - B_1)] + [A_1 A_0 \otimes (B_0 - B_1)(B_0 + B_1)] \\ =& I \otimes (B_0^2 + B_1^2 + B_0^2 + B_1^2) + A_0 A_1 \otimes B_0^2 + A_0 A_1 \otimes B_1 B_0 \\ &- A_0 A_1 \otimes B_0 B_1 - A_0 A_1 \otimes B_1^2 - A_1 A_0 \otimes B_0^2 + \\ &A_1 A_0 \otimes B_1 B_0 - A_1 A_0 \otimes B_0 B_1 - A_1 A_0 \otimes B_1^2 \\ =& 4I \otimes I + A_0 A_1 \otimes (-B_0 B_1 + B_1 B_0) + A_1 A_0 \otimes (B_0 B_1 - B_1 B_0) \\ =& 4I \otimes I + (A_0 A_1 - A_1 A_0)(B_1 B_0 - B_0 B_1) \leqslant 8I \end{aligned} \tag{7.11}$$



Rysunek 7.2: Poglądowa ilustracja przedstawiająca zależność zbiorów układów lokalnych, nielokalnych kwantowych i nielokalnych post-kwantowych dla układów o 2 wejściach binarnych i 2 binarnych wyjściach. Układ Tsirelsona to najbardziej nielokalny układ kwantowy. Spośród układów niesygnalizujących najbardziej nielokalny jest układ PR (Popescu-Rohrlich). Układ Anti-PR spełnia warunek $ab = x.y \oplus 1$, czyli przeciwne do warunku który spełnia układ PR.

Uwaga: jeśli norma zdefiniowana jako $\|X\|_\infty := \max_i |\lambda_i|$ spełnia $\|X\|_\infty \leqslant \alpha$ to $X \leqslant \alpha I$ gdyż $X - \alpha I \leqslant 0$. Ponadto dla dowolnych macierzy A, B zachodzi $\|AB\| \leqslant \|A\|\|B\|$ zatem $\|A_0A_1B_1B_0\|_\infty \leqslant \|A_0\|_\infty\|A_1\|_\infty\|B_1\|_\infty\|B_0\|_\infty \leqslant 1$, gdyż obserwable A_i, B_j są dychtomiczne tj. mają wartości własne ± 1. Analogicznie dla pozostałych trzech elementów sumy. Ponieważ $H^2 \leqslant 8I$ to $H \leqslant 2\sqrt{2}I$ zatem

$$\sup_{|\Psi\rangle} \langle\Psi| H |\Psi\rangle \leqslant 2\sqrt{2} \sup_{|\Psi\rangle} \langle\Psi|\Psi\rangle = 2\sqrt{2}. \tag{7.12}$$

□

Popescu i Rohrlich w 1994 [54] pokazali, że istnieją układy niesygnalizujące, niekwantowe. Od ich nazwisk jeden z nich jest nazywany układem PR i ma postać

$$P^{\mathrm{PR}}(a,b \mid x,y) := \begin{array}{|cc|cc|}\hline \frac{1}{2} & 0 & \frac{1}{2} & 0 \\ 0 & \frac{1}{2} & 0 & \frac{1}{2} \\ \hline \frac{1}{2} & 0 & 0 & \frac{1}{2} \\ 0 & \frac{1}{2} & \frac{1}{2} & 0 \\ \hline \end{array} \tag{7.13}$$

Łatwo sprawdzić, że

$$\mathrm{CHSH}(P^{\mathrm{PR}}(a,b \mid x,y)) = 4 \tag{7.14}$$

co jest wartością maksymalną tej nierówności dla rozkładów probabilistycznych.

Inną bardziej zwartą formą zapisu jest

$$P^{\mathrm{PR}}(a,b \mid x,y) = \begin{cases} \frac{1}{2}: & a \oplus b = xy \\ 0: & \text{w.p.p.} \end{cases}. \tag{7.15}$$

Zbiór układów niesygnalizujących tworzy wielościan w $\mathbb{R}^n$. W przypadku $d_x = d_y = d_a = d_b = 2$ (układ o binarnych wejściach i wyjściach) jest to ośmiowymiarowy wielościan w $\mathbb{R}^{16}$, który posiada 24 wierzchołki z czego 16 odpowiada deterministycznym rozkładom lokalnym danych wzorem

$$P^{\mathrm{L}}_{\alpha\beta\gamma\delta}(a,b \mid x,y) = \begin{cases} 1: & a = \alpha x \oplus \beta, b = \gamma y \oplus \gamma \\ 0: & \text{w.p.p.} \end{cases}, \tag{7.16}$$

gdzie $\alpha, \beta, \gamma \in \{0,1\}$ a pozostałe 8 to rozkłady typu PR dane wzorem

$$P^{\mathrm{PR}}_{\alpha\beta\gamma}(a,b \mid x,y) = \begin{cases} \frac{1}{2}: & a \oplus b = xy \oplus \alpha x \oplus \beta y \oplus \gamma \\ 0: & \text{w.p.p.} \end{cases}, \tag{7.17}$$

gdzie $\alpha, \beta, \gamma, \delta \in \{0,1\}$.

Jak możemy wykorzystać to w kontekście bezpieczeństwa?

Cel: Protokół, który jest możliwy do wykonania za pomocą kwantowych stanów, ale którego bezpieczeństwo nie zakłada, że urządzenia kwantowe do niego potrzebne wykonano poprawnie, lub nawet nie spełniają praw mechaniki kwantowej.

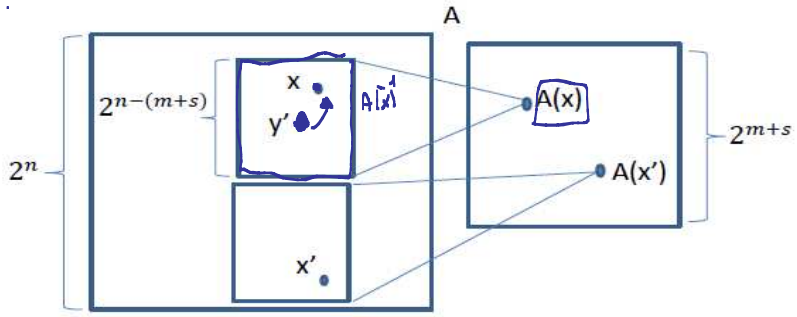
Dowód bezpieczeństwa ma korzystać tylko z zasady nie sygnalizowania i bazuje jedynie na statystykach wejścia i wyjścia. Taki protokół nazywamy niezależnym od urządzenia (Device-Independent ~~Quantum~~ Key Distribution)

Najważniejsze publikacje, które należy wymienić w tym kontekście to [55–59]

Przykład protokołów:

Protokół ~~„prawie"~~ DI (Hänggi, Renner i Wolf 2010 [60]):

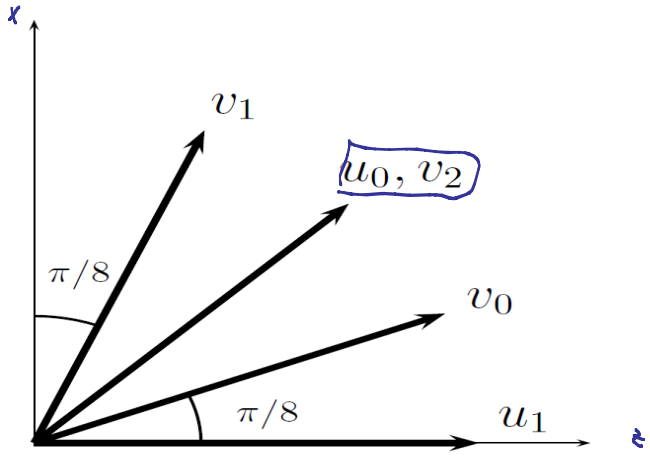
1. Alicja kreuje $n+k$ stanów $|\Psi_-\rangle_{AB} := 1/\sqrt{2}(|0\rangle|1\rangle - |1\rangle|0\rangle)$ i wysyła podukłady B do Boba.
2. Alicja losowo mierzą i-ty stan w bazie U_0 lub U_1 (Alicja) oraz V_0, ~~lub~~ V_1 (Bob).
3. Losowo wybierają wyniki pomiarów U_0V_0 (surowy klucz).
4. Dla k z pomiarów (losowy podzbiór) sprawdzają prawdopodobieństwo $a \oplus b \neq xy$ i jeśli jest zbyt wysokie to przerywają protokół.
5. Zwiększanie korelacji i bezpieczeństwa: Alicja losuje binarną macierz wymiaru $(m+s) \times n$ (taką, że dla każdego elementu macierzy A_{ij} $P(A_{ij}=0) = P(A_{ij}=1) = 1/2$). Alicja wysyła pierwsze m bitów ciągu As Bobowi (mnożenie macierzy jest wykonywane modulo 2). Klucz powstaje przez działanie macierzy na wektorze surowego klucza (działanie mod 2).



Rysunek 7.3: Losowa macierz binarna A jest używana do wykonania korekty błędu i zwiększania bezpieczeństwa w protokole RHW opisanym powyżej. s to długość wynikowego klucza, zaś m to wiadomość którą dowiaduje się Bob. Bob dekoduje ciąg Alicji wybierając najbliższy w odległości Hamminga ciąg binarny do tego który ma y_B, spośród tych r które spełniają $A(x) = A(r)$ (zaznaczone małym kwadratem wokół x). $m = h(\delta)$, gdzie δ to prawdopodobieństwo że ciągi Alicji i Boba różnią się, zaś $h(a) = -a\log_2 a - (1-a)\log_2(1-a)$ to tzw. binarana Entropia Shannona którą omówimy w późniejszym rodziale.

$\min_{y'} d_H(y_B, y') : A(x) = (y')$

$A(x) \rightarrow$ Bobu



U		0		1	
V	Y \ X	0	1	0	1
0	0	$\frac{1}{2} - \frac{\delta}{2}$	$\frac{\delta}{2}$	$\frac{3}{8} - \frac{\epsilon}{2}$	$\frac{1}{8} + \frac{\epsilon}{2}$
	1	$\frac{\delta}{2}$	$\frac{1}{2} - \frac{\delta}{2}$	$\frac{1}{8} + \frac{\epsilon}{2}$	$\frac{3}{8} - \frac{\epsilon}{2}$
1	0	$\frac{3}{8} - \frac{\epsilon}{2}$	$\frac{1}{8} + \frac{\epsilon}{2}$	$\frac{1}{8} + \frac{\epsilon}{2}$	$\frac{3}{8} - \frac{\epsilon}{2}$
	1	$\frac{1}{8} + \frac{\epsilon}{2}$	$\frac{3}{8} - \frac{\epsilon}{2}$	$\frac{3}{8} - \frac{\epsilon}{2}$	$\frac{1}{8} + \frac{\epsilon}{2}$

$$S = 1 - h(\delta) - \log_2(1+\epsilon)$$

Poniżej przedstawiam (vide E. Hänggi PhD thesis) układ Tsirelsona wraz z pomiarami, które go realizują na stanie $\frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$

Example 9. The system in Figure 2.8 is a quantum system. It can be obtained by measuring the state $|\psi^-\rangle = (|10\rangle - |01\rangle)/\sqrt{2}$ using the operator $E_u^x = |\Psi_u^x\rangle\langle\Psi_u^x|$ and $E_v^y = |\Phi_v^y\rangle\langle\Phi_v^y|$ as given below.

$$
\begin{aligned}
|\Psi_0^0\rangle &= \tfrac{1}{\sqrt{2}}(|0\rangle + |1\rangle) & |\Psi_0^1\rangle &= \tfrac{1}{\sqrt{2}}(|0\rangle - |1\rangle)\\
|\Psi_1^0\rangle &= |0\rangle & |\Psi_1^1\rangle &= |1\rangle\\
|\Phi_0^0\rangle &= \tfrac{\sqrt{2-\sqrt{2}}}{2}|0\rangle - \tfrac{\sqrt{2+\sqrt{2}}}{2}|1\rangle & |\Phi_0^1\rangle &= \tfrac{\sqrt{2+\sqrt{2}}}{2}|0\rangle + \tfrac{\sqrt{2-\sqrt{2}}}{2}|1\rangle\\
|\Phi_1^0\rangle &= \tfrac{\sqrt{2+\sqrt{2}}}{2}|0\rangle - \tfrac{\sqrt{2-\sqrt{2}}}{2}|1\rangle & |\Phi_1^1\rangle &= \tfrac{\sqrt{2-\sqrt{2}}}{2}|0\rangle + \tfrac{\sqrt{2+\sqrt{2}}}{2}|1\rangle .
\end{aligned}
$$

x \ y	0		1	
0	$\frac{2+\sqrt{2}}{8}$	$\frac{2-\sqrt{2}}{8}$	$\frac{2+\sqrt{2}}{8}$	$\frac{2-\sqrt{2}}{8}$
1	$\frac{2-\sqrt{2}}{8}$	$\frac{2+\sqrt{2}}{8}$	$\frac{2-\sqrt{2}}{8}$	$\frac{2+\sqrt{2}}{8}$
0	$\frac{2+\sqrt{2}}{8}$	$\frac{2-\sqrt{2}}{8}$	$\frac{2-\sqrt{2}}{8}$	$\frac{2+\sqrt{2}}{8}$
1	$\frac{2-\sqrt{2}}{8}$	$\frac{2+\sqrt{2}}{8}$	$\frac{2+\sqrt{2}}{8}$	$\frac{2-\sqrt{2}}{8}$

Figure 2.8: A quantum system.

7.2 Urządzenia i ataki

Definicja 25. *Urządzeniem (device) pozwala na generowanie dowolnej liczby układów. n użyć urządzenia jest opisane przez rozkład warunkowy*

$$P(a_1, \ldots, a_n, b_1, \ldots, b_n \mid x_1, \ldots, x_n, y_1, \ldots, y_n). \tag{7.24}$$

Urządzenie takie jest wielokrotnego użytku. Często przyjmujemy sensowne założenie, że urządzenie może sygnalizować w czasie w przód czyli x_i może wpływać na $a_{i+1}, \ldots a_n$. Zauważmy, że przedstawiony wcześniej protokół zakładał coś silniejszego czyli nie sygnalizowanie w obie strony (w czasie).

Ataki: Zainstalowanie w urządzeniu mechanizmu ponownego uwalnia pomiarów lub wyników z poprzedniej sesji możliwe mimo tego, że w pierwszej sesji (użyciu) urządzenie jest bezpieczne. Na przykład w kontakcie serwera z Alicją połączenie jest szyfrowane ale gdy później gdy Ewa połączy się z serwerem ten może ujawnić klucz użyty wcześniej przez Alicję.

inna postać nierówności CHSH:

(1) $E(A_i B_j) = P(A_i = B_j) - P(A_i \neq B_j) = P(A_i = B_j) - [1 - P(A_i = B_j)]$

$= 2P(A_i = B_j) - 1$

$-E(A_i B_j) = P(A_i \neq B_j) - P(A_i = B_j) = 2P(A_i \neq B_j) - 1$

zatem:

$CHSH = |E(A_0 B_0) + E(A_0 B_1) + E(A_1 B_0) - E(A_1 B_1)| =$

$= 2P(A_0 = B_0) - 1 + 2P(A_0 = B_1) - 1 + 2P(A_1 = B_0) - 1 + [2P(A_1 \neq B_1) - 1] =$

$2[P(A_0 = B_0) + P(A_0 = B_1) + P(A_1 = B_0) + P(A_1 \neq B_1)] - 4$

$2\left(\sum_{x,y=0}^{1} \sum_{a \oplus b = x \cdot y}^{1} P(a \oplus b = x \cdot y)\right) - 4$

$P(a \oplus b = x \cdot y)$ ← etykiety obserwabli A_x, B_y

gdy $CHSH = 2$,

$2CHSH' - 4 = 2 \Rightarrow CHSH' = 3$

gdy $CHSH = 2\sqrt{2}$ (maks kwantowy)

$2CHSH' - 4 = 2\sqrt{2} \Rightarrow CHSH' = \frac{2\sqrt{2} + 4}{2} = 2\sqrt{2} + 2$

gdy $CHSH = 4$, $2CHSH' - 4 = 4 \Rightarrow CHSH' = 4$.

$$CHSH' = \sum_{x,y,a,b} P(a \oplus b = xy)$$

Kolokwium z Podstaw Informatyki Kwantowej gr A

Zad1. Która z macierzy nie jest stanem i dlaczego ?

a) $\begin{pmatrix} 1/2 & i/3 \\ i/3 & 1/2 \end{pmatrix}$, b) $\begin{pmatrix} 1/6 & 3/6 \\ 3/6 & 5/6 \end{pmatrix}$, c) $\begin{pmatrix} 0 & \sqrt{2/5} \\ \sqrt{2/5} & 1/5 \end{pmatrix}$

d) $\begin{pmatrix} 1/2 & 0 & 0 & -1/2 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ -1/2 & 0 & 0 & 1/2 \end{pmatrix}$

Zad 2. Oblicz iloczyn skalarny:

a) $\langle u|v\rangle$

b) $(\langle u| \otimes \langle x|)(|v\rangle \otimes |y\rangle)$

Gdzie $|u\rangle = |-\rangle, |x\rangle = |+_i\rangle,$

$v = \sqrt{\frac{1}{3}}|0\rangle + \sqrt{\frac{2}{3}}|1\rangle$

$y = \sqrt{\frac{2}{3}}|0\rangle + \sqrt{\frac{1}{3}}|1\rangle$

Zad 3. Zapisz podany stan w notacji Diraca:

a) $\begin{pmatrix} 1/6 & 0 & 0 & 1/6 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 2/3 & 0 \\ 1/6 & 0 & 0 & 1/6 \end{pmatrix}$, b) $\begin{pmatrix} 1/4 & 1/6 \\ 1/6 & 3/4 \end{pmatrix}$

Zad 4. Podaj wynik mnożenia tensorowego stanów :

$\rho_A = \begin{pmatrix} 1/2 & -i/2 \\ i/2 & 1/2 \end{pmatrix}$ przez stan z zad 3.b (w tej kolejności)

Zad 5. Oblicz prawdopodobieństwo otrzymania stanu $|+\rangle$ w wyniku pomiaru w bazie $\{|+\rangle, |-\rangle\}$ stanu

$$|\psi\rangle = \sqrt{\frac{4}{5}}|0\rangle + \frac{1}{\sqrt{5}}|1\rangle$$

Zad 6. Alicja chce przesłać Bobowi angielskie słowo „AM". Zamień litery na ich kod binarny na 5 bitach (A=00000, B=00001,C=00010 itd.) i podaj jakie operacje i w jakiej kolejności musi wykonać ona odpowiedniej liczbie stanów $|\psi_+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ w protokole gęstego kodowania.

Zad 7 Oblicz wartość średnią obserwabli σ_x na stanie $|\psi >$z zad 5
Wsk. Jako ρ we wzorze na w.śr. wstaw projektor na ten stan.

Zad 8. Wykonaj kwantową teleportację stanu z zadania 5) za pomocą stanu $|\psi_+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$. Wskazówka: Przekształć stan:

$$(\sqrt{\frac{4}{5}}|0\rangle_C + \frac{1}{\sqrt{5}}|1\rangle_C) \otimes \frac{1}{\sqrt{2}}(|00\rangle_{AB} + |11\rangle_{AB})$$