Zwiększanie losowości

Maciej Stankiewicz

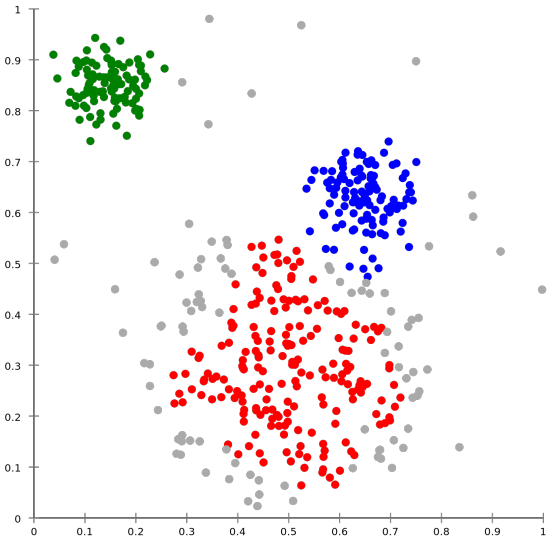
Wydział Matematyki, Fizyki i Informatyki UG
Krajowe Centrum Informatyki Kwantowej

XIII Matematyczne Warsztaty KaeNeMów
Hel, 20-22 maja 2016

Spis treści

Do czego potrzebujemy losowości?

Do czego potrzebujemy losowości?



Niezależność od urządzenia

W kryptografii często rozpatrujemy model “device independent” w którym nie ufamy urządzeniom i nie znamy ich struktury wewnętrznej “black box model”. Opieramy się jedynie na statystykach wyników otrzymywanych z urządzenia.

Niezależność od urządzenia

W kryptografii często rozpatrujemy model “device independent” w którym nie ufamy urządzeniom i nie znamy ich struktury wewnętrznej “black box model”. Opieramy się jedynie na statystykach wyników otrzymywanych z urządzenia.

Dobrą praktyką jest to by protokół był jawny!

Źródła "prawie" losowe [1]

Definicja (Źródło Santha-Vazirani)

ϵ-SV source jest dane przez rozkład prawdopodobieństwa $P(x_1, x_2, \ldots, x_n, \ldots)$ dla ciągów bitów, taki że

$$\frac{1}{2} - \epsilon \leqslant P(x_i | x_{i-1}, x_{i-2}, \ldots, x_1) \leqslant \frac{1}{2} + \epsilon \tag{1}$$

$$\frac{1}{2} - \epsilon \leqslant P(x_1) \leqslant \frac{1}{2} + \epsilon \tag{2}$$

Źródła "prawie" losowe [1]

Definicja (Źródło Santha-Vazirani)

ϵ-SV source jest dane przez rozkład prawdopodobieństwa $P(x_1, x_2, \ldots, x_n, \ldots)$ dla ciągów bitów, taki że

$$\frac{1}{2} - \epsilon \leqslant P(x_i | x_{i-1}, x_{i-2}, \ldots, x_1) \leqslant \frac{1}{2} + \epsilon \tag{1}$$

$$\frac{1}{2} - \epsilon \leqslant P(x_1) \leqslant \frac{1}{2} + \epsilon \tag{2}$$

Wniosek

- $\epsilon = 0$ - *źródło w pełni losowe*
- $\epsilon = \frac{1}{2}$ - *źródło deterministyczne*
- $\epsilon \in (0, \frac{1}{2})$ - *źródło częściowo losowe*

Klasyczne zwiększanie losowości [1]

Twierdzenie (Klasycznie zwiększanie losowości nie jest możliwe)

Dla każdej funkcji Ext : $\{0,1\}^n \to \{0,1\}$ *i każdego* ϵ *istnieje* ϵ*-SV source X takie, że Ext(X) jest losowe z błędem nie mniejszym niż* ϵ.

Klasyczne zwiększanie losowości [1]

Twierdzenie (Klasycznie zwiększanie losowości nie jest możliwe)

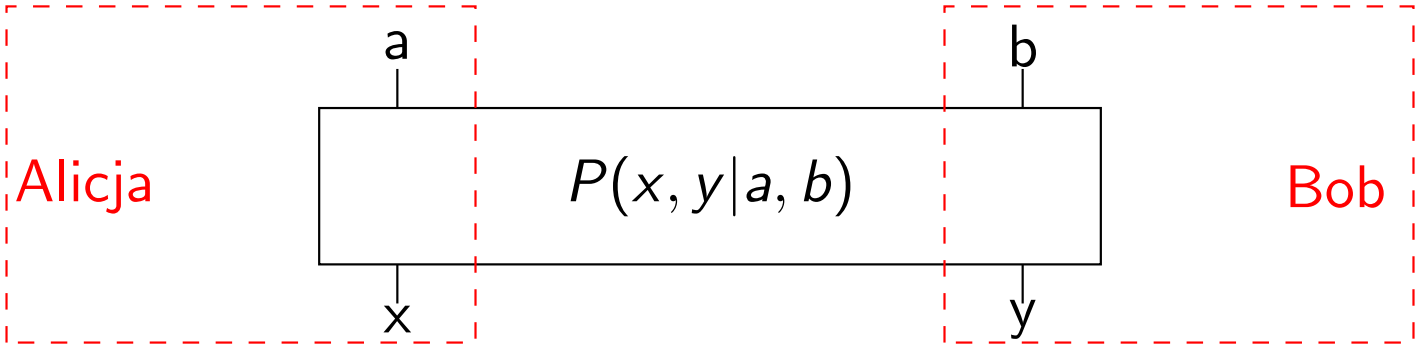
Dla każdej funkcji Ext : $\{0,1\}^n \to \{0,1\}$ *i każdego* ϵ *istnieje* ϵ*-SV source X takie, że Ext(X) jest losowe z błędem nie mniejszym niż* ϵ.

Warto przytoczyć fakt, że mając większą ilość niezależnych SV-source można klasycznie zwiększać losowość.

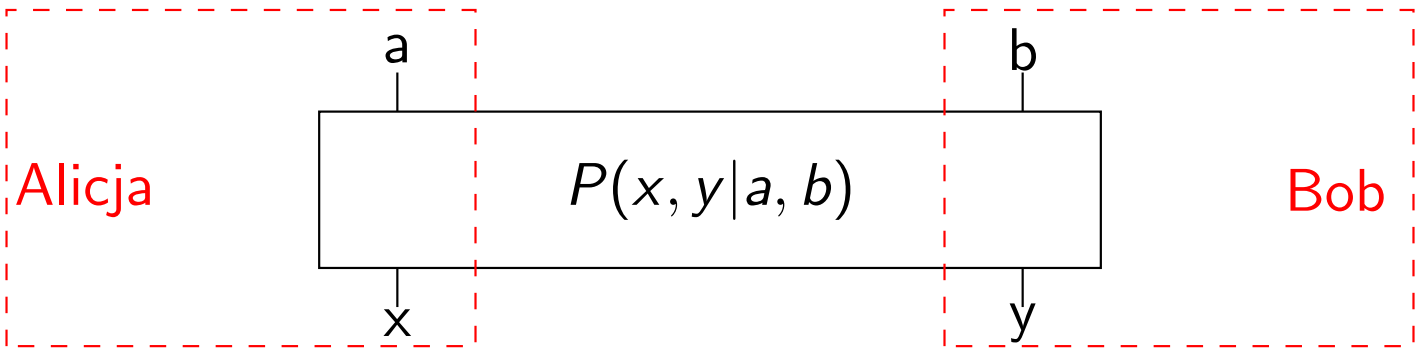
Kwanty

Czy efekty kwantowe mogą pomóc?

Pudełka



Pudełka



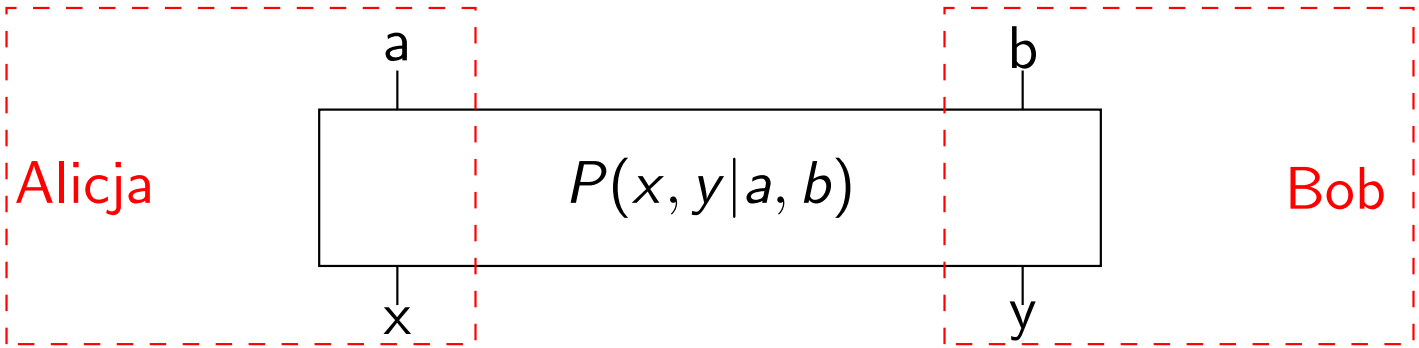
Definicja (Warunek lokalności)

Pudło jest lokalne jeśli

$$P(x, y|a, b) = \sum_{\lambda} P(x|a, \lambda)P(y|b, \lambda) \tag{3}$$

Gdzie λ opisuje pewną z góry ustaloną, dzieloną losowość.

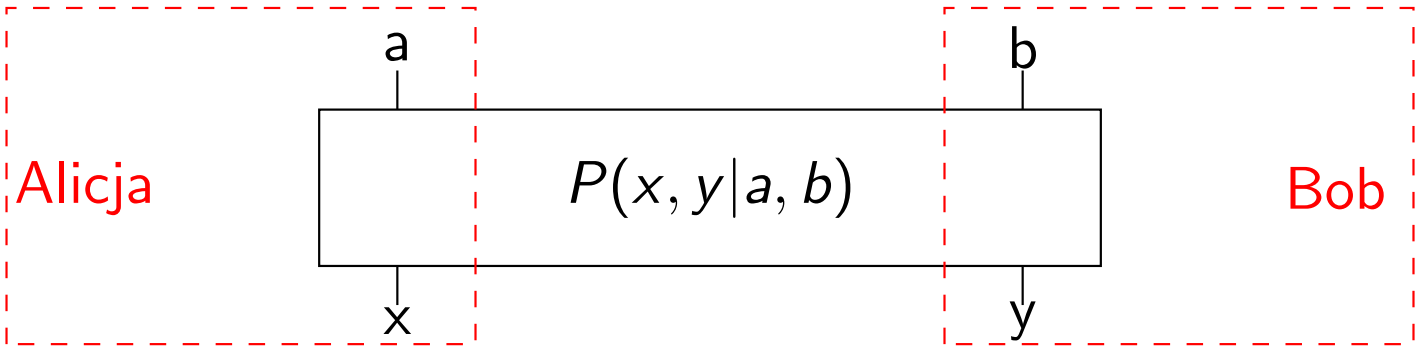
Pudełka



Definicja (Pudełka kwantowe)

Pudło jest kwantowe jeśli możemy je "zbudować" korzystając z efektów kwantowych ;)

Pudełka

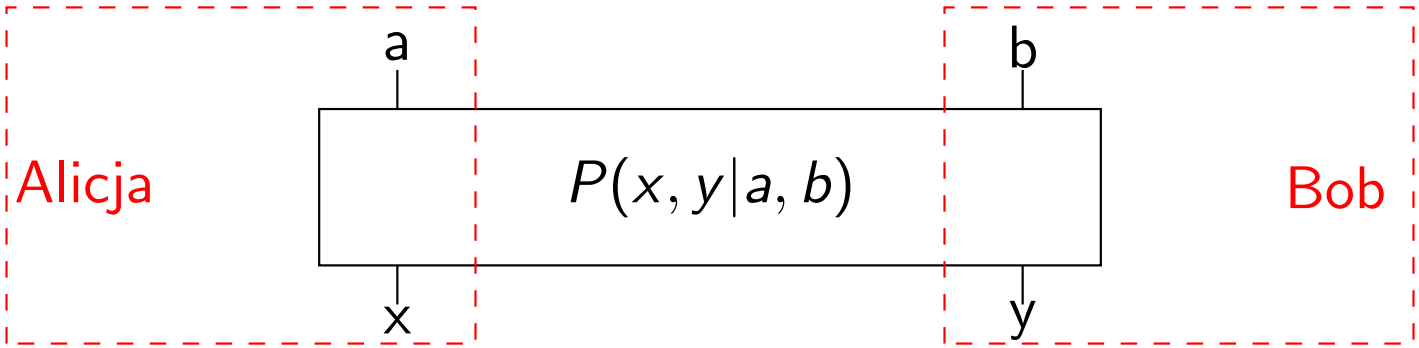


Definicja (Pudełka kwantowe)

Pudło jest kwantowe jeśli możemy je "zbudować" korzystając z efektów kwantowych ;)

Ważne jest to że potrafimy zbudować kwantowe pudła nielokalne.

Pudełka



Definicja (Warunek nie sygnalizacji)

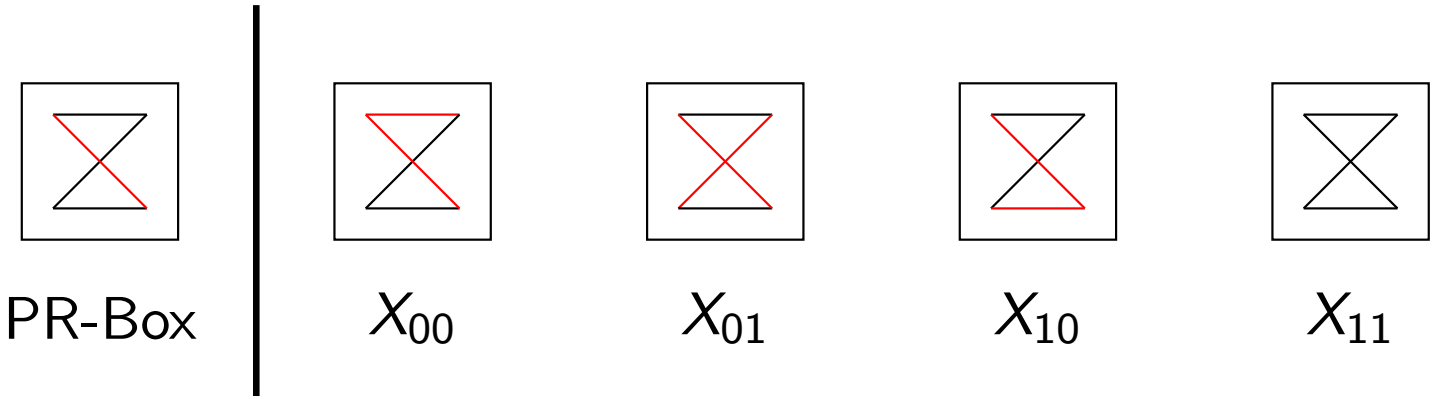
$$\begin{aligned} \underset{a,b,b',x}{\forall} \sum_y P(x, y|a, b) &= \sum_y P(x, y|a, b') \\ \underset{a,a',b,y}{\forall} \sum_x P(x, y|a, b) &= \sum_x P(x, y|a', b) \end{aligned} \tag{3}$$

Popescu - Rohrlich Box

Definicja (PR-Box)

$$P(x,y|a,b) = \begin{cases} \frac{1}{2} : x \oplus y = ab \\ 0 : \text{w.p.p.} \end{cases} \tag{4}$$

PR-Box i pudła lokalne



Podsumowanie

Podsumowanie

Problemy otwarte:

Korelacje pomiędzy SV i urządzeniem [3].

Poprawa ϵ.

Zmniejszenie liczby urządzeń.

Bibliografia I

[1] M. Santha and U. V. Vazirani.
Generating quasi-random sequences
from semi-random sources.
Journal of Computer and System Sciences, 33(1):75–87, 1986.

[2] .R. Colbeck and R. Renner.
Free randomness can be amplified.
Nature Physics, 8(6):450–453, 2012.

Bibliografia II

[3] H. Wojewodka, F. G. S. L. Brandao, A. Grudka, M. Horodecki, K. Horodecki, P. Horodecki, M. Pawlowski, and R. Ramanathan.
Amplifying the randomness of weak sources correlated with devices.
ArXiv e-prints, January 2016.

Inne tematy badań

Inne tematy badane w kwantowej teorii informacji:

- Kryptografia (szyfrowanie, podpis elektroniczny, wybory, bit commitment)
- Redukcja złożoności komunikacyjnej
- Komputery i algorytmy kwantowe
- Kwantowa korekcja błędów
- Badanie podstaw fizyki i wszechświata
- I wiele innych

Koniec

Dziękuję za uwagę