

Splątanie kwantowe i jego zastosowania

Wojciech Bruzda



wykład dla studentów Politechniki Warszawskiej
semestr zimowy 2025/2026

<https://wojtek.cft.edu.pl/teaching>

w.bruzda@cft.edu.pl

wykład #03A/15

one-time pad (XOR)

Franklin Miller (1882) $\rightarrow$ Gilbert Vernam (1917)

klasyczne szyfrowanie informacji za pomocą klucza, który jest

- jednorazowy
- dostarczony nadawcy i odbiorcy niezależnym kanałem komunikacyjnym

one-time pad (XOR) – przykład

tekst do zaszyfrowania:

MAŁY NIEDŹWIADEK WLAŻŁ NA PAGÓREK, ABY ZOBACZYĆ JESZCZE WIĘKSZĄ GÓRĘ

kod ASCII¹: $a_j =$ 4D, 41, 9C, 59, 20, 4E, 49, 45, 44, A0, 57, 49, 41, 44, 45, 4B, ...
klucz: $k_j =$ 7A, 1F, D4, 03, 8B, 6E, C1, 55, 92, 0A, FE, 4C, B7, 28, 9D, E3, ...
 $a_j \oplus k_j \equiv e_j =$ 37, 5E, 48, 5A, AB, 20, 88, 10, D6, AA, A9, 05, F6, 6C, D8, A8, ...

na przykład: $4D \oplus 7A = 37 \iff 01001101 \oplus 01111010 = 00110111$

tekst po zaszyfrowaniu jest z reguły binarny i nie da się go łatwo wyświetlić:

7^HZ« \x88\x10Öª©\x05ö1Ø"...

¹polskie znaki diakrytyczne zapisane przy użyciu strony kodowej [Mazovia CP790](#) (0x...)

protokół BB84

Charles Bennett, Gilles Brassard (1984)

1. (A) posiada generyczny qubit $|\psi\rangle = \tau_0|0\rangle + \tau_1|1\rangle$, który mierzy (PVM) w losowo wybranej bazie: X (baza Hadamarda) lub Z (baza obliczeniowa)
2. w wyniku pomiaru (A) otrzymuje:

$$|\psi_j\rangle \stackrel{*}{=} \begin{cases} |0\rangle & : & \text{Z} & \longleftrightarrow & b_j = 0 \\ |1\rangle & : & \text{Z} & \longleftrightarrow & b_j = 1 \\ |+\rangle & : & \text{X} & \longleftrightarrow & b_j = 0 \\ |-\rangle & : & \text{X} & \longleftrightarrow & b_j = 1 \end{cases}$$

oraz ciąg bitów $b_j \in \{0, 1\}$ będących wynikami pomiarów

3. (A) transmituje qubity $|\psi_j\rangle$ do (B) przy użyciu kanału kwantowego

protokół BB84

4. (B) $\forall_j$ wybiera w sposób losowy bazę X lub Z i mierzy qubit $|\psi_j\rangle$ otrzymując:

stan $ \psi_j\rangle$	$\overbrace{\text{wylosowana baza}}^{\equiv \text{obserwabla}}$	prawdopodobieństwo	stan po pomiarze
$ 0\rangle$	Z	$p_0 = 1$	$ 0\rangle$
$ 1\rangle$	Z	$p_1 = 1$	$ 1\rangle$
$\begin{Bmatrix} 0\rangle \\ 1\rangle \end{Bmatrix}$	X	$\begin{Bmatrix} p_+ = 1/2 \\ p_- = 1/2 \end{Bmatrix}$	losowo: $\begin{Bmatrix} +\rangle \\ -\rangle \end{Bmatrix}$
$\begin{Bmatrix} +\rangle \\ -\rangle \end{Bmatrix}$	Z	$\begin{Bmatrix} p_0 = 1/2 \\ p_1 = 1/2 \end{Bmatrix}$	losowo: $\begin{Bmatrix} 0\rangle \\ 1\rangle \end{Bmatrix}$
$ +\rangle$	X	$p_+ = 1$	$ +\rangle$
$ -\rangle$	X	$p_- = 1$	$ -\rangle$

stan po pomiarze zawsze jest wektorem własnym obserwabli $\longleftrightarrow$ bazy w której dokonywany jest pomiar

a odpowiednie wartości własne są przemapowane na identyfikatory pomiaru: $\{0, 1\}$ oraz $\{+, -\}$

protokół BB84 – przykładowa sekwencja 16 pomiarów

Ⓐ	X $ +\rangle$	X $ +\rangle$	Z $ 0\rangle$	Z $ 0\rangle$	Z $ 1\rangle$	Z $ 0\rangle$	Z $ 1\rangle$	X $ +\rangle$	X $ -\rangle$	X $ -\rangle$	Z $ 0\rangle$	X $ -\rangle$	X $ +\rangle$	Z $ 1\rangle$	Z $ 0\rangle$	Z $ 0\rangle$
Ⓑ	X $ +\rangle$	X $ +\rangle$	Z $ 0\rangle$	X $ -\rangle$	X $ +\rangle$	Z $ 0\rangle$	Z $ 1\rangle$	Z $ 0\rangle$	Z $ 0\rangle$	X $ -\rangle$	X $ +\rangle$	X $ -\rangle$	X $ +\rangle$	Z $ 1\rangle$	X $ -\rangle$	Z $ 0\rangle$

5. Ⓐ oraz Ⓑ publicznie ujawniają swoje bazy (nie wyniki!) i odrzucają te pomiary, gdzie bazy są niezgodne

Ⓐ	X $ +\rangle$	X $ +\rangle$	Z $ 0\rangle$			Z $ 0\rangle$	Z $ 1\rangle$			X $ -\rangle$		X $ -\rangle$	X $ +\rangle$	Z $ 1\rangle$		Z $ 0\rangle$
Ⓑ	X $ +\rangle$	X $ +\rangle$	Z $ 0\rangle$			Z $ 0\rangle$	Z $ 1\rangle$			X $ -\rangle$		X $ -\rangle$	X $ +\rangle$	Z $ 1\rangle$		Z $ 0\rangle$

6. według przyporządkowania ★ Ⓐ oraz Ⓑ teoretycznie uzyskują ciąg bitów

$$b = (0, 0, 0, 0, 1, 1, 1, 0, 1, 0)$$

protokół BB84

- dopuszcza modyfikacje i procedury wzmacniające losowość
- umożliwia wykrycie podsłuchu/wycieku danych

ale

- potrzeba stosowania kanałów kwantowych o wysokiej jakości transmisji
- absolutna gwarancja bezpieczeństwa vs. praktycznie niska funkcjonalność²...

²komercyjny użytek (2025)

?

najskuteczniejsza metoda szyfrowania danych?

⇒ **socjotechnika i otwarty tekst!** (najciemniej pod latarnią...)

ważny czytelnik odnajdzie “ukryty” przekaz znajdujący gdzieś się na slajdach :)