Splątanie kwantowe i jego zastosowania

Wojciech Bruzda

wykład dla studentów Politechniki Warszawskiej
semestr zimowy 2025/2026

https://chaos.if.uj.edu.pl/∼wojtek/teaching

w.bruzda@cft.edu.pl

wersja: 20251126

wykład #03A/15

one-time pad (XOR)

Franklin Miller (1882) $\longrightarrow$ 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 WLAZŁ NA PAGÓREK, ABY ZOBACZYĆ JESZCZE WIĘKSZĄ GÓRĘ
```

kod ASCII[1]: $a_j =$ 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: $\texttt{4D} \oplus \texttt{7A} = \texttt{37} \iff 01001101 \oplus 01111010 = 00110111$

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

```
7^HZ« \x88\x10Öª©\x05ölØ¨...
```

[1] polskie 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:

$$|\psi_j\rangle \overset{\star}{=} \begin{cases} |0\rangle & : \quad \texttt{Z} \quad \longleftrightarrow \quad b_j = 0 \\ |1\rangle & : \quad \texttt{Z} \quad \longleftrightarrow \quad b_j = 1 \\ |+\rangle & : \quad \texttt{X} \quad \longleftrightarrow \quad b_j = 0 \\ |-\rangle & : \quad \texttt{X} \quad \longleftrightarrow \quad b_j = 1 \end{cases}$$

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

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 funkcjonalność[2]...

[2] komercyjny użytek (2025)

?

najskuteczniejsza metoda szyfrowania danych?

$\Longrightarrow$ **socjotechnika i otwarty tekst!** (najciemniej pod latarnią...)

uważny czytelnik odnajdzie "ukryty" przekaz znajdujący gdzieś się na slajdach :)