BB84

1) **Бездоганне кодування** $A \to B$

x_i – біти для передачі $\quad |\varphi_{00}\rangle = |0\rangle \quad |\varphi_{10}\rangle = |1\rangle$

y_i – вибір базису 0/1 або +/- $\quad |\varphi_{01}\rangle = |+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$

$|\varphi_{11}\rangle = |-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$

A

x_i	1	0	1	1	0	1	0	1	0	0	0	1	0	1	1	1	0	1	0	1
y_i	0	1	0	1	0	1	0	1	0	1	0	1	0	0	0	1	1	1	1	0
	φ_{10}	φ_{01}	φ_{10}	φ_{11}	φ_{00}	φ_{11}	φ_{00}	φ_{11}	φ_{00}	φ_{01}	φ_{00}	φ_{11}	φ_{00}	φ_{10}	φ_{10}	φ_{11}	φ_{01}	φ_{11}	φ_{01}	φ_{10}
	$\|1\rangle$	$\|+\rangle$	$\|1\rangle$	$\|-\rangle$	$\|0\rangle$	$\|-\rangle$	$\|0\rangle$	$\|-\rangle$	$\|0\rangle$	$\|+\rangle$	$\|0\rangle$	$\|-\rangle$	$\|0\rangle$	$\|+\rangle$	$\|1\rangle$	$\|-\rangle$	$\|+\rangle$	$\|-\rangle$	$\|+\rangle$	$\|1\rangle$
B y'_i	1	1	0	1	0	1	0	0	1	0	1	0	1	1	0	0	0	1	0	1
x'_i	1	0	1	1	0	1	0	1	0	1	1	0	1	0	1	1	1	1	0	0
Випадковий вибір																				
Базис Боба	0	1	0	1	0	1	0	1	0	1	0	1	0	0	0	1	1	1	1	0
Перевіряємо y_i, y'_i	1	1	0	1	0	1	0	0	1	0	1	0	1	1	0	0	0	1	0	1
Залишкові біти		0	1	1	0	1	0								1			1		

Перевіряємо половину

x_i	0	1	1 (перев)	0	1 (перевіряємо)	0	1	1 (перев)
x'_i	0	1	1	0	1	0	1	1

$\Rightarrow$ маємо вихідний ключ! 0 1 0 0 1

Як вимірюємо x_i при різних базисах?

$|-\rangle$ при 0/1 — $|-\rangle = \frac{|0\rangle - |1\rangle}{\sqrt{2}}$ (вимір 0 – $\frac{1}{2}$, 1 – $\frac{1}{2}$) $\quad$ $|1\rangle$ при +/- — $|1\rangle = \frac{|+\rangle - |-\rangle}{\sqrt{2}}$ = (вимір + – $\frac{1}{2}$, - – $\frac{1}{2}$)

$|+\rangle$ при 0/1 — $|+\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}}$ (вимір 0 – $\frac{1}{2}$, 1 – $\frac{1}{2}$)

$|0\rangle$ при +/- — $|0\rangle = \frac{|+\rangle + |-\rangle}{\sqrt{2}}$ (вимір + – $\frac{1}{2}$, - – $\frac{1}{2}$)

Будемо вимірювати випадково

φ_1 – початкове значення, φ_2 – після CNOT, φ_3 – отримує Боб

2) CNOT атака

A

x_i	0	1	0	1	1	0	0	1	0	1	0	0	0	1	1	0	0	1	0	0
y_i	1	1	0	1	0	1	0	0	0	1	0	1	1	1	0	0	1	0	1	1
	φ_{01}	φ_{11}	φ_{00}	φ_{11}	φ_{10}	φ_{01}	φ_{00}	φ_{10}	φ_{00}	φ_{11}	φ_{00}	φ_{01}	φ_{01}	φ_{11}	φ_{10}	φ_{00}	φ_{01}	φ_{10}	φ_{01}	φ_{01}
φ_i	|+>	|->	|0>	|->	|1>	|+>	|0>	|1>	|0>	|->	|0>	|+>	|+>	|->	|1>	|0>	|+>	|1>	|+>	|+>

Є

CNOT (φ_2)	|+>	|+>	|0>	|+>	|1>	|+>	|0>	|1>	|0>	|+>	|0>	|+>	|+>	|+>	|1>	|0>	|+>	|1>	|+>	|+>
Eav. Knowledge:	|+>	|->	|0>	|->	|1>	|+>	|0>	|1>	|0>	|->	|0>	|+>	|+>	|->	|1>	|0>	|+>	|1>	|+>	|+>
y'_i	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	1	0	1	0
x'_i	1	1	0	1	1	0	0	1	0	1	0	0	1	1	1	1	0	1	0	0

Б

φ_3	|+>	|+>	|0>	|+>	|1>	|+>	|0>	|1>	|0>	|+>	|0>	|+>	|+>	|+>	|1>	|0>	|+>	|1>	|+>	|+>
y''_i	1	1	1	0	0	1	1	0	0	1	0	1	1	0	0	0	1	0	1	0
x''_i	1	1	1	0	1	1	0	1	0	1	0	1	1	0	1	0	1	1	1	1

Збіги вибору базису

Аліса y_i	1	1	0	1	0	1	0	0	0	1	0	1	1	1	0	0	1	0	1	1
Боб y''_i	1	1	1	0	0	1	1	0	0	1	0	1	1	0	0	0	1	0	1	0
Єва y'_i	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	1	0	1	0

Перевірка помилок 7 шт

Аліса x_i	0	1			1	0			0	1	0									
Боб x''_i	1	1			1	1			0	1	0									
Єва x'_i	1	1			1	0			0	1	0									

?потенційний ключ?
А 0010010
Б 1110111
Є 0111010

Res • Вийшли 2 помилки, можна вважати, що А і Б розпізнали втручання зловмисника, чи ні, могли проігнорувати помилку

Як зловмисник вплив(ає)?

CNOT атака полягає у застосуванні CNOT$(\varphi \otimes |0_E\rangle)$

У випадку $|+\rangle$ зловмисник отримає $CNOT(|+\rangle_A |0_E\rangle) = \frac{|+\rangle_A |+\rangle_E + |-\rangle_A |-\rangle_E}{\sqrt{2}}$, що не помітне зловмиснику виміряти 1 кубіт і передати далі без змін

У випадку $|-\rangle$ отримаємо $CNOT(|-\rangle_A |0_E\rangle) = \frac{|+\rangle_A |-\rangle_E + |-\rangle_A |+\rangle_E}{\sqrt{2}}$, що не дасть однозначно передати далі Бобу

$CNOT(|1\rangle_A |0\rangle_E) = |1\rangle_A |1\rangle_E$

$CNOT(|0\rangle_A |0\rangle_E) = |0\rangle_A |0\rangle_E$

$CNOT(|+\rangle_A |0\rangle_E) = \frac{|+\rangle_A |+\rangle_E + |-\rangle_A |-\rangle_E}{\sqrt{2}}$

$CNOT(|-\rangle_A |0\rangle_E) = \frac{|+\rangle_A |-\rangle_E + |-\rangle_A |+\rangle_E}{\sqrt{2}}$

① $= \frac{1}{2}\left(|+\rangle_A (|+\rangle_E - |-\rangle_E) + |-\rangle_A (|-\rangle_E - |+\rangle_E)\right)$

② $= \frac{1}{2}\left(|+\rangle_A (|+\rangle_E + |-\rangle_E) + |-\rangle_A (|+\rangle_E + |-\rangle_E)\right)$

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

④ $= \frac{|0_A\rangle |0_E\rangle - |1_A\rangle |1_E\rangle}{\sqrt{2}}$

у базисі 0/1

① виміряємо 1

② виміряємо 0

③ $0 - \frac{1}{2},\ 1 - \frac{1}{2}$

④ $0 - \frac{1}{2}\ \ 1 - \frac{1}{2}$

у базисі +−

① $\frac{1}{2} - |+\rangle$, $\frac{1}{2} - |-\rangle$

② $\frac{1}{2} - |+\rangle$, $\frac{1}{2} - |-\rangle$

③ $\frac{1}{2} - |+\rangle$, $\frac{1}{2} - |-\rangle$

(+) знаємо який кубіт В

④ $\frac{1}{2} - |+\rangle$, $\frac{1}{2} - |-\rangle$

(+) Знаємо протилежне значення для В

↓ В

① $|1\rangle_E = \frac{|+\rangle_E - |-\rangle_E}{\sqrt{2}}$

② $|0\rangle = \frac{|+\rangle_E + |-\rangle_E}{\sqrt{2}}$

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

④ $\frac{|0_E\rangle - |1_E\rangle}{\sqrt{2}} = \frac{|-\rangle_E + |+\rangle_E}{\sqrt{2}}$

Тобто виходить ми виграємо
- лише у випадку вимір базису +/− кубіт $|+\rangle$
- та при базисі 0/1 при вимірі $|0\rangle$ або $|1\rangle$

Висновок

у базисі 0/1

① 1 ② 0 ③ $0 - \frac{1}{2},\ 1 - \frac{1}{2}$ 4) $0 - \frac{1}{2}\ \ 1 - \frac{1}{2}$

у базисі +/−

① $+ - \frac{1}{2},\ \frac{1}{2} - -$ ② $\frac{1}{2} - +,\ \frac{1}{2} - -$ ③ $\frac{1}{2} - +,\ \frac{1}{2} - -$ ④ $\frac{1}{2} - +,\ \frac{1}{2} - -$