Университет ИТМО

Физико-технический мегафакультет
Физический факультет

Группа: М32041 К работе допущен

Студенты: Никитин, Игнатьев, Курепин Работа выполнена

Преподаватель: Лабунцов Виктор Отчет принят

Рабочий протокол и отчет по лабораторной работе №5.06

КВАНТОВАЯ КРИПТОГРАФИЯ

1. Цель работы

   - Изучение основных принципов квантовой связи
   - Создание зашифрованного сообщения
   - Обнаружение перехватчика

2. Объект Исследования

   Импульсный источник света

3. Рабочие формулы и исходные данные

Alice		***Bob***		
State	Basis, Bit	Chosen Basis	State	Measured Bit
$\|0°\rangle$	+, 0	+	$\hat{M}_+ \|0°\rangle = \|0°\rangle$	0
		×	$\hat{M}_\times \|0°\rangle = \frac{1}{\sqrt{2}}\|45°\rangle - \frac{1}{\sqrt{2}}\|-45°\rangle$	0 or 1
$\|90°\rangle$	+, 1	+	$\hat{M}_+ \|90°\rangle = -\|90°\rangle$	1
		×	$\hat{M}_\times \|90°\rangle = \frac{1}{\sqrt{2}}\|45°\rangle + \frac{1}{\sqrt{2}}\|-45°\rangle$	0 or 1
$\|45°\rangle$	×, 1	+	$\hat{M}_+ \|45°\rangle = \frac{1}{\sqrt{2}}\|0°\rangle - \frac{1}{\sqrt{2}}\|90°\rangle$	0 or 1
		×	$\hat{M}_\times \|45°\rangle = \|45°\rangle$	1
$\|-45°\rangle$	×, 0	+	$\hat{M}_+ \|-45°\rangle = \frac{1}{\sqrt{2}}\|0°\rangle + \frac{1}{\sqrt{2}}\|90°\rangle$	0 or 1
		×	$\hat{M}_\times \|-45°\rangle = -\|-45°\rangle$	0

4. Оборудование

Экспериментальная установка: Алиса, Боб, Ева – представляют из себя три отдельные оптические плиты со следующими элементами. Алиса – лазер с блоком управления, полуволновая пластинка. Боб – полуволновая пластинка, светоделительный куб, два сенсора с блоком управления. Ева – полуволновая пластинка, светоделительный куб, два сенсора и лазер с полуволновой пластинкой

5. Схема установки

6. Результаты прямых измерений и их обработки (*таблицы, примеры расчетов*).

Зашифрованное слово: KIND – 01010 01000 01101 00011

Letter	K					I					N					D				
Data Bit	0	1	0	1	0	0	1	0	0	0	0	1	1	0	1	0	0	0	1	1
Key Bit	1	0	0	1	0	1	0	0	1	0	0	1	1	1	0	1	1	1	0	0
Encrypted Bit	1	1	0	0	0	1	1	0	1	0	0	0	0	1	1	1	1	1	1	1

	Алиса		Боб		
№	Базис	Бит	Базис	Бит	совпадение
1	+	1	x	1	нет
2	x	0	x	0	0
3	x	0	x	0	0
4	+	0	x	1	нет
5	+	0	+	1	нет
6	x	0	x	0	0

7	x	1	+	1	нет
8	+	1	x	0	нет
9	+	1	x	1	нет
10	+	1	x	0	нет
11	+	0	x	1	нет
12	x	1	x	1	1
13	+	1	x	1	нет
14	+	1	+	1	1
15	x	1	+	1	нет
16	x	0	x	0	0
17	+	1	x	0	нет
18	x	1	x	1	1
19	+	0	+	0	0
20	x	0	+	1	нет
21	+	1	+	1	1
22	x	0	x	0	0
23	+	1	x	1	нет
24	x	1	+	1	нет
25	x	1	+	0	нет
26	+	1	x	0	нет
27	+	0	+	0	0
28	+	0	x	0	нет
29	x	1	x	1	1
30	+	0	+	0	0
31	x	1	+	0	нет
32	x	0	+	0	нет
33	x	0	+	1	нет
34	x	1	x	1	1
35	+	0	x	1	нет
36	+	0	+	0	0
37	+	0	+	0	0
38	x	1	+	1	нет
39	x	0	x	0	0
40	+	0	x	0	нет
41	+	1	+	1	1
42	+	0	+	0	0
43	x	1	x	1	1
44	+	1	+	1	1
45	x	0	+	0	нет
46	x	0	+	1	нет
47	x	1	x	1	1
48	x	0	x	0	0
49	x	1	x	1	1
50	+	0	+	0	0
51	+	0	x	1	нет
52	x	1	+	0	нет

	Алиса		Ева		Боб		
№	Базис	Бит	Базис	Бит	Базис	Бит	совпадение
1	x	0	+	1	x	0	0
2	+	1	x	0	+	1	1
3	+	1	x	0	x	0	нет
4	+	0	+	0	x	1	нет
5	x	0	x	0	+	1	нет
6	x	0	+	0	x	1	нет
7	x	1	x	1	x	1	1
8	+	1	x	0	x	0	нет
9	x	0	x	0	x	0	0
10	+	0	+	0	x	1	нет
11	+	1	+	1	+	1	1
12	+	0	+	0	+	0	0
13	x	1	+	1	x	1	1
14	x	1	+	0	+	0	нет
15	+	0	x	0	x	0	нет
16	x	0	x	0	+	1	нет
17	x	0	+	0	+	0	нет
18	+	1	x	0	+	1	1
19	x	1	+	0	x	1	1
20	x	0	+	1	+	1	нет
21	x	0	+	0	x	1	нет
22	+	0	x	0	x	0	нет
23	x	1	+	0	+	1	нет
24	+	1	x	0	+	0	нет
25	+	0	x	0	+	1	нет
26	x	0	x	0	+	0	нет
27	+	1	x	0	+	0	нет
28	+	1	x	0	+	0	нет
29	x	0	+	0	+	0	нет
30	+	1	+	1	+	1	1
31	x	0	x	0	+	1	нет
32	+	1	+	1	+	1	1
33	+	1	+	1	x	1	нет
34	x	0	+	1	x	0	0
35	+	0	x	0	x	0	нет
36	+	1	+	1	+	1	1
37	+	1	+	1	x	1	нет
38	+	1	+	1	x	0	нет
39	+	0	+	0	x	1	нет
40	+	1	x	0	+	0	нет
41	+	0	+	0	x	0	нет
42	x	1	x	1	+	0	нет
43	x	1	x	1	x	1	1
44	+	1	x	0	x	0	нет

45	x	1	x	1	x	1	1
46	x	1	x	1	+	0	нет
47	+	0	+	0	+	0	0
48	+	0	+	0	x	1	нет
49	x	1	+	0	+	0	нет
50	+	0	+	0	+	0	0
51	+	0	x	0	+	1	нет
52	x	1	+	1	x	0	нет

7. Расчет результатов косвенных измерений (*таблицы, примеры расчетов*).

%Ошибок: =1 - (52 - СЧЁТЕСЛИ(C42:BB42; "нет"))/52 = 67,31%

11. Окончательные результаты.

%Ошибок = 67,31%

12. Выводы и анализ результатов работы.

В первом пункте лабораторной мы закодировали ключ и успешно передали его с помощью методов квантовой криптографии. Во втором пункте мы успешно перехватили сигнал Алисы с помощью Евы и передали его Бобу. Процент ошибок составил намного больше 25%, что явно указало на присутствие перехватчика.