

Рабочий протокол и отчет по лабораторной работе
№ 5.06
Изучение принципов работы квантовой
криптографии

Фадеев Артём

Апрель 2022

1 Цели и задачи

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

2 Задачи, решаемые во время выполнения работы

- Создание шифрующего ключа при помощи двух-базисной передачи данных

3 Объект исследования

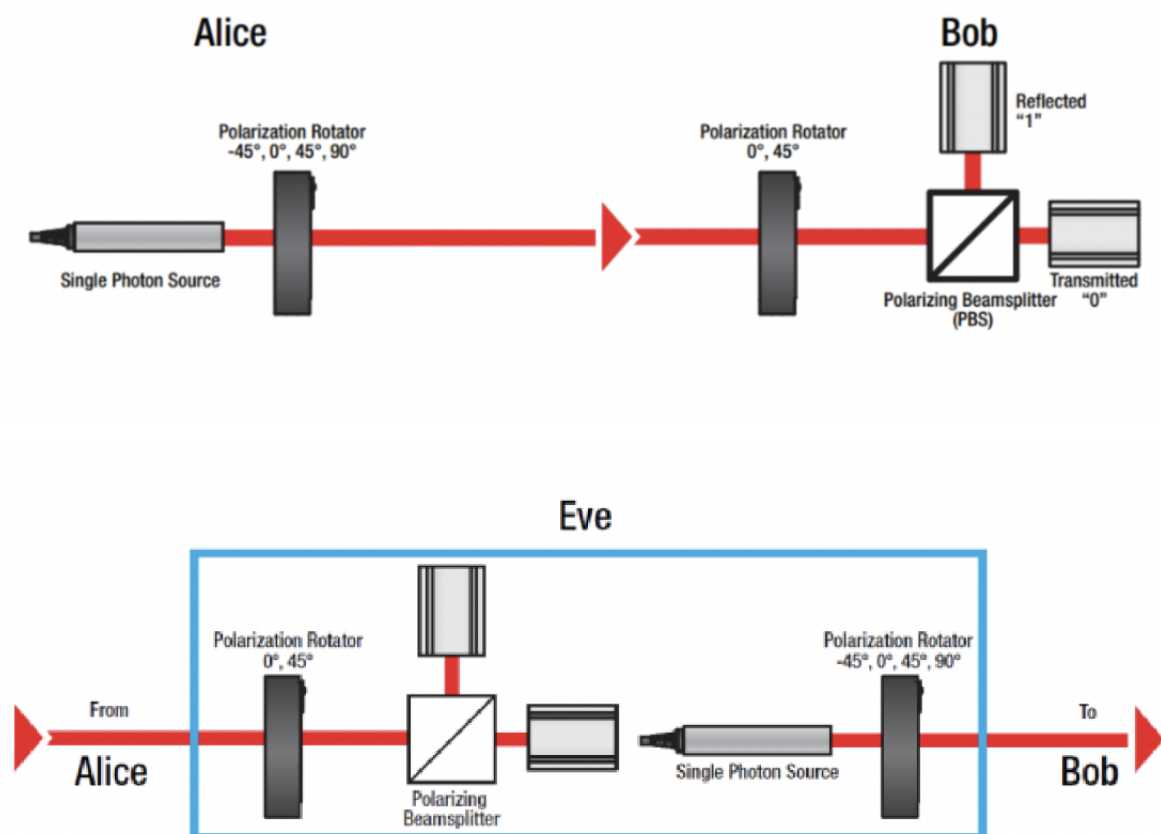
- Поляризация фотонов и её практическое применение

4 Рабочие формулы и исходные данные

- + базис
 - поляризация 0° - 0
 - поляризация 90° - 1
- X базис

- поляризация -45° - 0
- поляризация 45° - 1
- Значения букв в 2-чной СС

5 Схема установки



6 Результаты прямых и косвенных измерений и их обработки

n	Alice			Bob		
	basis	angle	bit	basis	angle	bit
1	+	90	1	x	45	1
2	+	0	0	+	0	0
3	x	-45	1	+		1
4	x	45	0	+		1
5	x		0	+		0
6	x		1	x		1
7	+		0	+		0
8	+		1	x		1
9	x		0	x		0
10	x		1	+		1
11	x		1	+		0
12	x		1	x		1
13	x		0	+		1
14	+		1	x		1
15	x		1	+		0
16	+		0	+		0
17	+		1	+		1
18	x		0	+		0
19	x		1	+		1
20	+		1	+		1
21	x		1	+		1
22	+		0	x		0
23	x		1	x		1
24	x		1	+		1
25	+		1	+		1
26	x		1	x		1
27	x		0	x		0
28	+		0	x		1
29	+		1	+		1
30	+		1	+		1
31	x		1	+		0
32	x		1	x		1
33	x		1	+		1
34	x		1	x		1
35	+		1	+		1
36	+		1	x		1
37	x		1	+		0
38	x		1	+		0
39	+		1	+		1
40	x		0	x		0
41	+		1	x		1
42	+		1	+		1
43	x		1	+		0
44	x		0	x		0
45	x		0	+		0
46	+		1	+		1
47	x		1	x		1
48	+		0	+		0
49	x		1	+		0
50	x		0	+		0
51	+		1	x		0
52	+		0	x		1

n	Alice		Eve		Bob	
	basis	bit	basis	bit	basis	bit
1	+	1	x	0	+	1
2	x	0	x	0	+	0
3	+	1	+	1	+	1
4	x	1	+	0	x	1
5	x	1	x	1	x	1
6	+	0	+	0	x	1
7	+	1	x	1	x	1
8	+	0	+	0	x	0
9	x	0	x	0	x	0
10	+	1	x	0	+	1
11	+	0	x	1	x	1
12	+	1	+	1	x	0
13	x	0	+	1	+	1
14	+	0	+	0	x	0
15	+	0	x	0	x	0
16	+	0	x	0	+	1
17	x	0	+	1	x	0
18	x	0	+	0	x	0
19	x	0	+	0	+	0
20	+	1	+	1	+	1
21	+	0	+	0	+	0
22	+	1	+	1	x	1
23	+	0	x	0	+	0
24	+	0	+	0	+	0
25	x	1	x	1	x	1
26	x	0	+	1	x	1
27	+	1	+	1	x	1
28	+	1	x	1	x	1
29	+	0	+	0	+	0
30	+	1	x	1	+	1
31	+	0	x	1	x	1
32	+	1	x	1	+	1
33	x	0	+	1	x	0
34	x	0	x	0	+	0
35	x	1	x	1	+	0
36	+	0	+	0	x	1
37	+	0	+	0	x	0
38	+	0	+	0	+	0
39	x	0	x	0	x	0
40	x	1	+	1	+	1
41	x	1	+	0	x	0
42	x	1	+	1	x	0
43	+	1	+	1	+	1
44	x	0	x	0	+	1
45	+	0	x	1	+	0
46	x	1	x	1	+	0
47	x	0	+	1	+	1
48	x	0	+	0	x	1
49	+	0	x	1	+	1
50	+	0	x	0	x	0
51	x	0	+	0	+	0
52	+	0	x	0	+	0

	O				O				P				S							
word	0	1	1	1	0	0	1	1	1	0	0	1	1	1	1	1	0	0	1	0
key	0	1	0	0	1	0	1	1	1	1	1	0	1	1	1	1	1	1	0	1
crypted	0	0	1	1	1	1	0	0	0	0	1	1	1	0	0	0	0	1	1	1
key	0	1	0	0	1	0	1	1	1	1	1	0	1	1	1	1	1	1	0	1
encrypted	0	1	1	1	0	0	1	1	1	0	0	1	1	1	1	1	1	0	0	1

7 Выводы и анализ работы

Мы используем фотон, как средство передачи информации.

С помощью полуволновых пластинок, которые определяют базис, и поляризационных разделительных кубов, которые отражают свет с вертикальной поляризацией и пропускают с горизонтальной, при отправлении фотона можем получить определенный результат, который может быть перехвачен.

Перехватчик – собранная Алиса и Боб, но в обратной последовательности.

Если Ева угадывает базис, то получает всю информацию Алисы незамеченно. При неудачной попытке на один из детекторов приходит неверный бит, и Ева отправит сигнал Бобу. При дальнейшей проверке базисов Алисы и Боба это будет заметно с вероятностью 25%. Тогда будет произведена замена ключа.