УНИВЕРСИТЕТ ИТМО

Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики

УЧЕБНЫЙ ЦЕНТР ОБЩЕЙ ФИЗИКИ ФТФ

Группа: M32021 **К работе допущен:** _____

Студент: Корнилов Н. В. **Работа выполнена:** _____

Преподаватель: Тимофеева Э. О. **Отчёт 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:

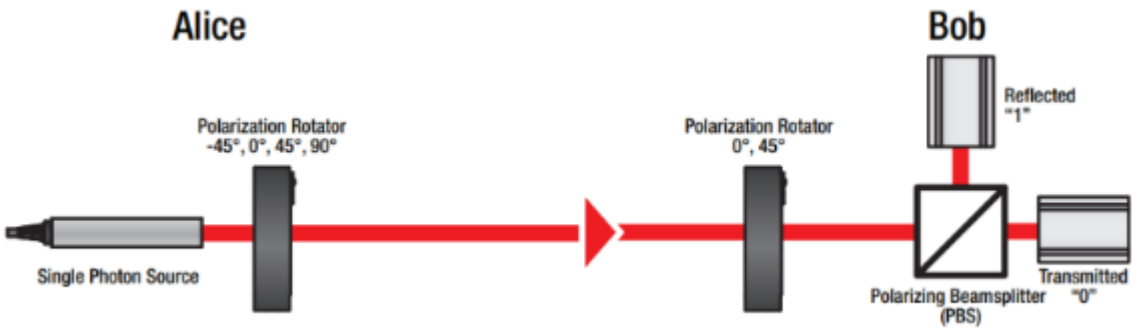
Alice		***Bob***		
State	Basis, Bit	Chosen Basis	State	Measured Bit
$\|0°\rangle$	$+, 0$	$+$	$\hat{M}_+ \|0°\rangle = \|0°\rangle$	0
		$\times$	$\hat{M}_\times \|0°\rangle = \frac{1}{\sqrt{2}}\|45°\rangle - \frac{1}{\sqrt{2}}\|-45°\rangle$	0 or 1
$\|90°\rangle$	$+, 1$	$+$	$\hat{M}_+ \|90°\rangle = -\|90°\rangle$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

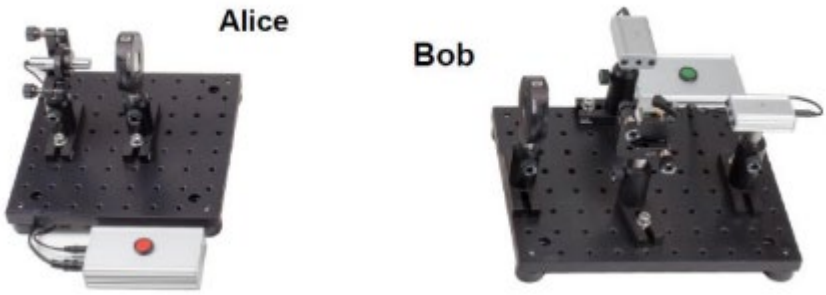
4. Оборудование:
    - Установка состоит из 3 основных элементов: Алиса, Боб и Ева. Алиса – оптическая плита, блок управления с источником излучения, полуволновая пластинка с маркировкой “ – 45˚ 0˚ 45˚ 90˚”. Боб - оптическая плита, светоделительный куб, два детектора сигнала, полуволновая пластинка с маркировкой "0˚ 45˚”. Ева - оптическая плита, блок управления с источником излучения, полуволновая пластинка с маркировкой “ – 45˚ 0˚ 45˚ 90˚”, светоделительный куб, два детектора сигнала, полуволновая пластинка с маркировкой "0˚ 45˚”.
    - **Полуволновая пластинка**

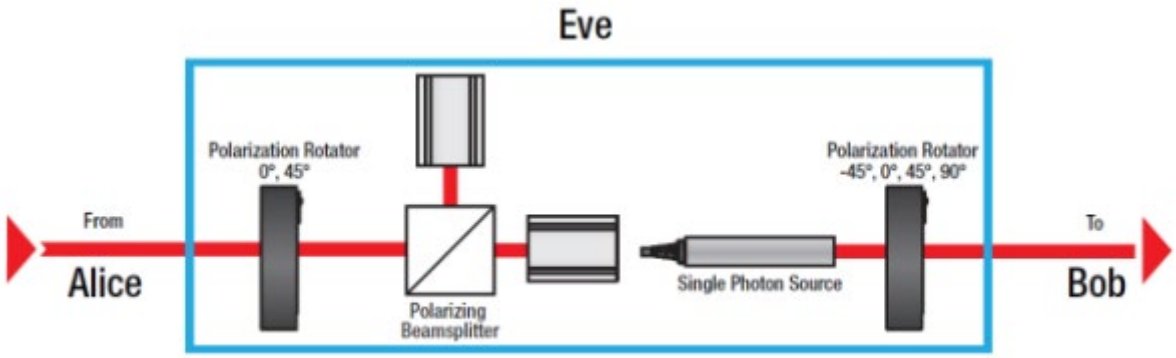
    - **Блок управления источником излучения**

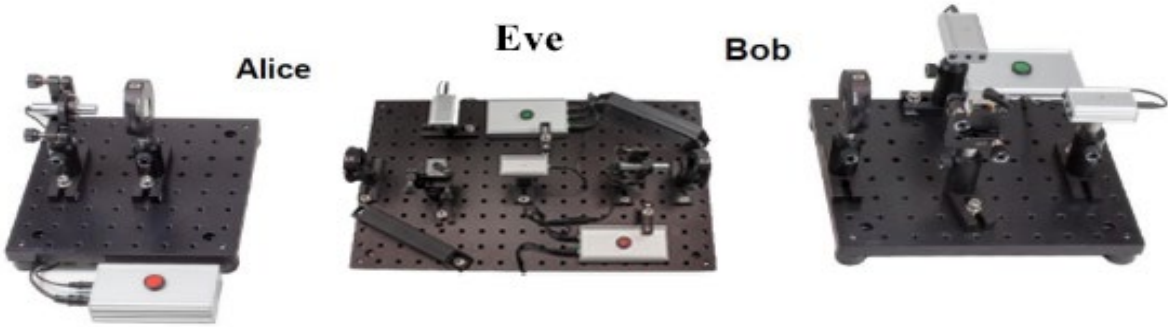
    - **Детектор сигнала**

5. Схема установки:









6. Результаты прямых измерений и их обработки (таблицы, примеры расчётов):

Создание секретного ключа

Сгенерируем случайные наборы базисов для Алисы и Боба, а также случайный набор битов для Алисы. Длина набора – 52 бита.

Для Алисы получим такую таблицу:

№	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
Базис	X	+	+	X	X	+	X	X	+	+	+	+	X	X	X	+	+	+	+	X	X	+	+	X	+	X
Бит	0	0	1	0	1	0	1	1	0	1	1	1	1	0	0	1	1	1	0	0	1	0	1	1	0	0
№	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50	51	52
Базис	X	X	X	+	+	X	X	+	X	X	X	X	+	X	+	X	+	X	X	X	+	X	+	+	X	X
Бит	1	1	0	0	1	1	1	0	0	0	0	0	0	0	0	0	0	0	1	1	1	0	1	0	1	1

Передадим сообщение с Алисы на Боба

Получим для Боба вот такую таблицу:

№	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
Базис	X	X	X	X	+	+	X	X	X	X	+	+	+	+	+	X	X	+	+	+	+	X	X	X	+	X
Бит	0	0	0	0	1	0	1	1	0	0	1	1	1	1	0	1	0	1	0	0	1	0	1	1	0	0
№	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50	51	52
Базис	+	X	X	+	X	X	+	X	X	+	X	X	X	X	+	+	+	X	+	+	+	X	X	+	X	X
Бит	0	1	0	0	0	1	0	1	0	0	0	0	1	0	0	0	0	0	1	1	1	0	0	0	1	1

Выберем те сообщения, где базис совпал и получим секретный ключ длиной 28 бит

0001 1111 0100 1001 0000 0001 0011

Кодирование слова

В качестве слова для сообщения возьмем: TCSG - 10011 00010 10010 00110

Используем первые 20 из 28 бит нашего секретного ключа

Слово	T					C					S					G				
Исходное	1	0	0	1	1	0	0	0	1	0	1	0	0	1	0	0	0	1	1	0
Ключ	0	0	0	1	1	1	1	1	0	1	0	0	1	0	0	1	0	0	0	0
Зашифрованное	1	0	0	0	0	1	1	1	1	1	1	0	1	1	0	1	0	1	1	0

Для передачи сообщения используем базис +

Алиса передает сообщение:

№	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
Базис	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+
Бит	1	0	0	0	0	1	1	1	1	1	1	0	1	1	0	1	0	1	1	0

Боб получает сообщение:

№	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
Базис	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+
Бит	1	0	0	0	0	1	1	1	1	1	1	0	1	1	0	1	0	1	1	0

Расшифровка сообщения

Полученное	1	0	0	0	0	1	1	1	1	1	1	0	1	1	0	1	0	1	1	0
Ключ	0	0	0	1	1	1	1	1	0	1	0	0	1	0	0	1	0	0	0	0
Расшифрованное	1	0	0	1	1	0	0	0	1	0	1	0	0	1	0	0	0	1	1	0
Слово	T					C					S					G				

Введение в установку Евы и обнаружение перехватчика Алисой и Бобом

Переданное Алисой сообщение

№	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
Базис	+	+	X	+	X	+	X	+	X	+	+	+	X	X	X	X	+	X	X	+	X	+	X	+	+	+
Бит	0	0	0	0	1	0	1	1	1	1	1	0	0	0	1	0	0	1	1	0	1	1	1	1	0	0
№	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50	51	52
Базис	+	+	+	+	X	+	+	X	+	X	X	+	X	+	+	+	+	X	X	X	X	X	+	+	X	+
Бит	1	0	1	1	0	1	0	1	1	1	1	0	1	1	0	1	1	1	0	1	0	1	0	0	0	0

Евой

№	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
Базис	+	+	+	X	X	X	X	X	X	+	X	X	X	X	+	+	+	X	+	X	+	+	+	X	+	+
Бит	0	0	1	1	1	1	1	0	1	1	0	1	0	0	1	0	0	1	1	1	1	1	1	0	0	0
№	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50	51	52
Базис	X	X	+	X	+	+	X	+	+	+	X	+	X	+	+	+	X	X	+	X	X	+	X	+	+	+
Бит	0	1	1	0	0	1	0	0	1	0	1	0	1	1	0	1	1	1	0	1	0	1	1	0	0	0

Полученное Бобом

№	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
Базис	X	+	+	+	X	+	X	+	X	+	+	+	+	X	X	+	+	X	X	X	X	X	X	X	X	+
Бит	0	0	1	0	1	0	1	0	1	1	0	0	0	0	0	0	0	1	0	1	0	0	0	0	0	0
№	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50	51	52
Базис	X	+	+	+	+	+	X	X	+	+	X	+	X	X	X	X	+	X	+	+	+	+	X	+	+	+
Бит	0	0	1	0	0	1	0	1	1	0	1	0	1	1	1	1	1	1	0	0	1	1	1	0	0	0

Помеченные цветом значения соответствую битам, базисы которых совпали у Алисы и Боба. При этом зеленый цвет означает, что также совпали и полученные биты, а оранжевый – биты не совпали.

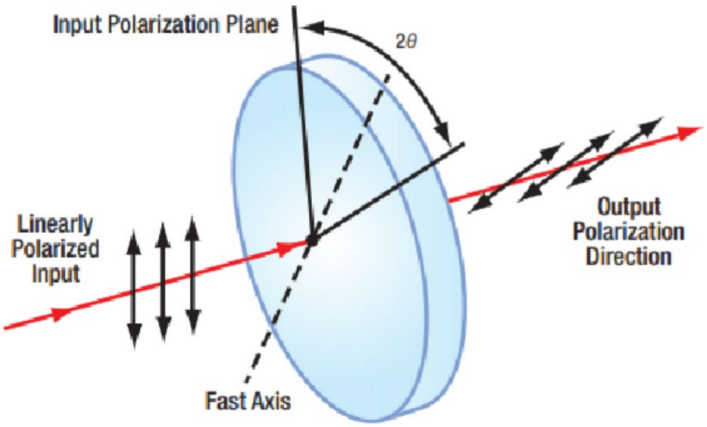
Итоговые секретные ключи:

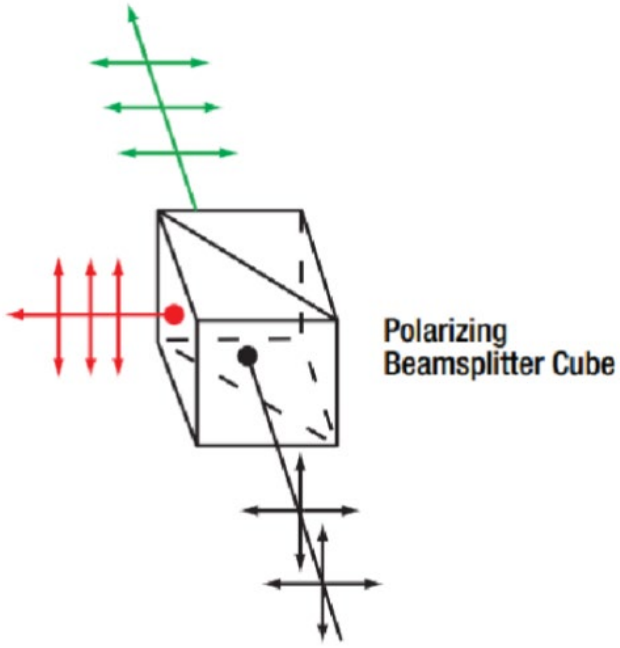
У Алисы: 00101111100101111001111111011100

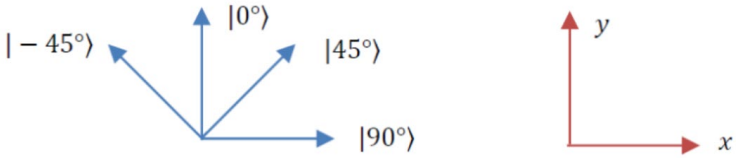
У Боба: 00101011000001000001011111011100

7 из 31 (23%) переданных битов не совпадают, что позволяет определить, что в передачу сообщения была внедрена Ева.

7. Графики







8. Выводы и анализ результатов работы

В первой части эксперимента мы смогли понять основные принципы работы квантовой связи и алгоритма случайного распределения квантового ключа BB84 и с помощью их создать секретный ключ.

Во второй части работы при помощи этого ключа нам удалось успешно зашифровать, передать, а затем расшифровать полученное сообщение.

В третьей части работы, при создании секретного ключа шифрования, мы смогли заметить, что в процесс была внедрена Ева, что следует из анализа полученных нами данных.

9. Ответы на контрольные вопросы:
    a. **В чем заключается метод одноразового ключа?**
    Метод одноразового ключа, также известный как шифр с одноразовым блокнотом, является криптографическим алгоритмом, который предлагает теоретически идеальную безопасность при соблюдении определенных условий. Принцип заключается в использовании случайного ключа, который имеет ту же длину, что и сообщение, которое нужно зашифровать или расшифровать. Ключ используется только однажды и затем уничтожается. Для шифрования и расшифрования используется применение операции XOR над сообщением и ключом.
    b. **Каковы правила данного метода шифрования?**
        1. Генерация ключа: Создайте случайный ключ, который имеет ту же длину, что и сообщение, которое нужно зашифровать. Ключ должен быть настоящим случайным числом, а не генерироваться алгоритмически.
        2. Секретность ключа: Убедитесь, что ключ абсолютно секретен и известен только отправителю и получателю.
        3. Шифрование: Отправитель комбинирует свое сообщение с ключом с использованием операции XOR на битовом уровне. Полученный результат является зашифрованным сообщением.
        4. Передача: Зашифрованное сообщение передается получателю по каналу связи. Поскольку ключ и сообщение имеют одинаковую длину, а ключ случаен, зашифрованное сообщение будет выглядеть как случайный набор данных.
        5. Расшифровка: Получатель комбинирует зашифрованное сообщение с тем же ключом снова с использованием операции XOR. Это приводит к восстановлению исходного текста сообщения.
        6. Одноразовое использование ключа: Ключ должен использоваться только однажды и затем уничтожаться. Повторное использование ключа может привести к уязвимостям и возможности раскрытия информации.
    c. **Чем одно-базисная система отличается от двух-базисной?**
    В одно-базисной системе используется только один базис для кодирования и измерения квантовых состояний. Такая система позволяет Еве угадать нужный базис и незаметно получить доступ к передаваем данным.
    В двух-базисной системе используются два ортогональных базиса для кодирования и измерения квантовых состояний (0 и 90, -45 и 45). Благодаря такой системе, в случае внедрения Евы у Алисы и Боба есть возможность это определить из-за появления несовпадений битов при одинаковых базисах.
    d. **Для чего в установке используется полуволновая пластинка?**
    Полуволновая пластинка – это оптический элемент, который используется для изменения поляризации света. В лабораторной работе полуволновые пластинки используются для подготовки и кодирования квантовых состояний в различных поляризационных базисах.
    e. **Как производится выполнение протокола шифрования?**

Шифрование в лабораторной выполняется при помощи применения операции побитовой операции XOR над секретным одноразовым ключом и сообщением. Дешифрование является аналогичной операцией.

f. **Как можно обнаружить перехватчика сообщения (Еву)?**
Обнаружить перехватчика можно при появлении случайных ошибок в алгоритме генерации секретного ключа между Алисой и Бобом. Согласно теории, порядка 25% из переданных битов между Алисой и Бобом, в одном базисе, будут иметь разные значения.

g. **Как выбираются Алисой базис и бит при создании ключа шифрования?**
Для обеспечения высокой надежности шифрования базис и биты при создании ключа должны выбираться АБСОЛЮТНО случайно. Для генерации таких чисел могут использоваться такие источники как физические шумы, такие, как детекторы событий ионизирующей радиации, дробовой шум в резисторе или космическое излучение.

h. **Каковы правила бинарного сложения?**

$$0 + 0 = 0$$

$$1 + 0 = 1$$

$$0 + 1 = 1$$

$$1 + 1 = 0$$