**Министерство науки и высшего образования Российской Федерации**

**Федеральное государственное автономное образовательное учреждение высшего образования**

**«Национальный исследовательский университет ИТМО»**

Факультет информационных технологий и программирования

Лабораторная работа № 5.06

*Изучение принципов квантовой криптографии.*

**Выполнили студенты группы № М3311**

Сорокина Н.

Пестриков М.

Санкт-Петербург

2024

1) Цели работы:

1. Изучение основных принципов квантовой связи

2. Создание зашифрованного сообщения

3. Обнаружение перехватчика

2) Задачи:

1. Изучить протокол квантовой передачи данных, включая выбор базиса и бита, проверку на перехват и формирование финального ключа шифрования.

2. Экспериментально провести передачу данных.

3. Научиться обнаруживать попытки перехвата.

3) Объект исследования:

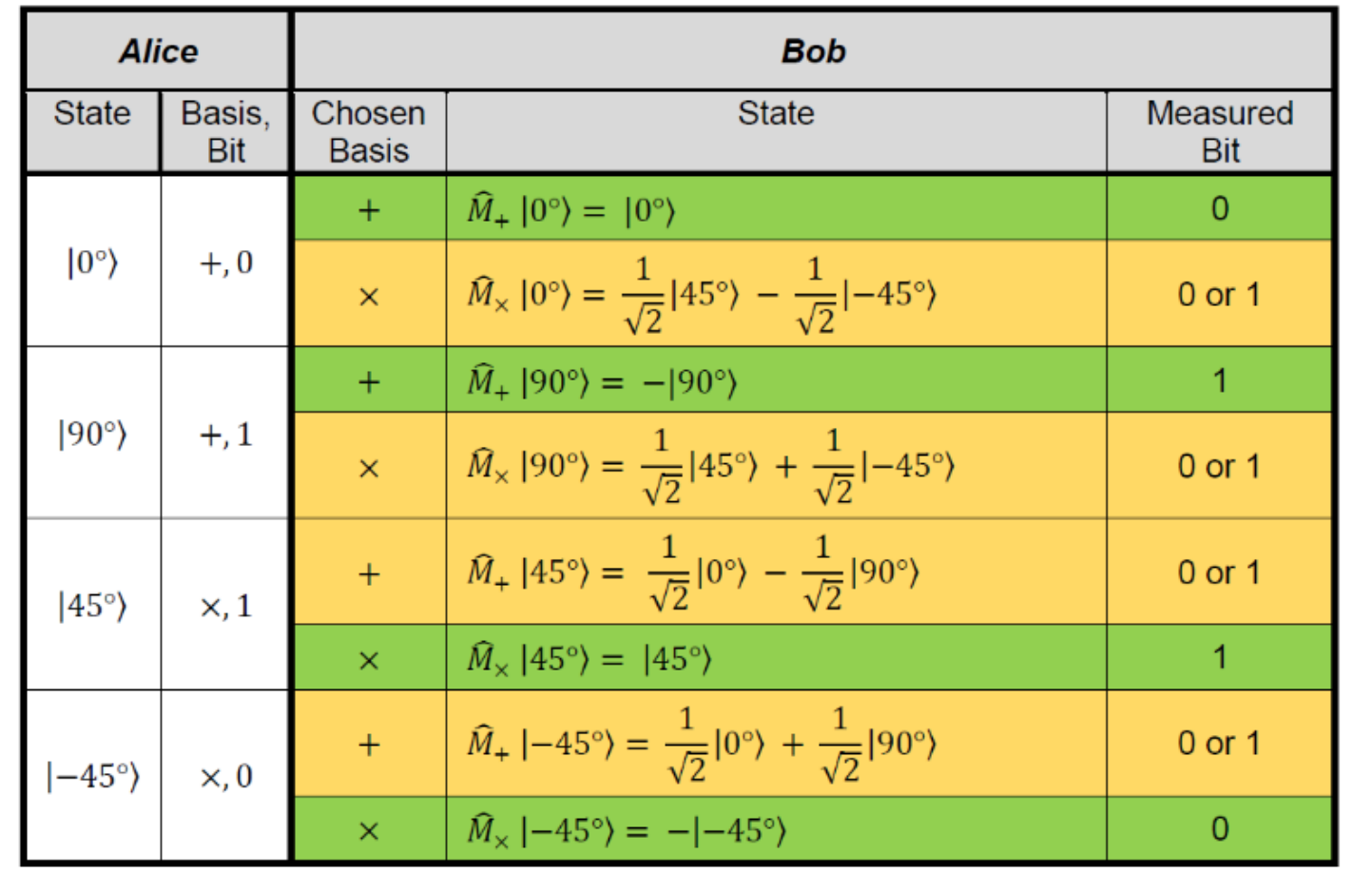
Импульсный источник света

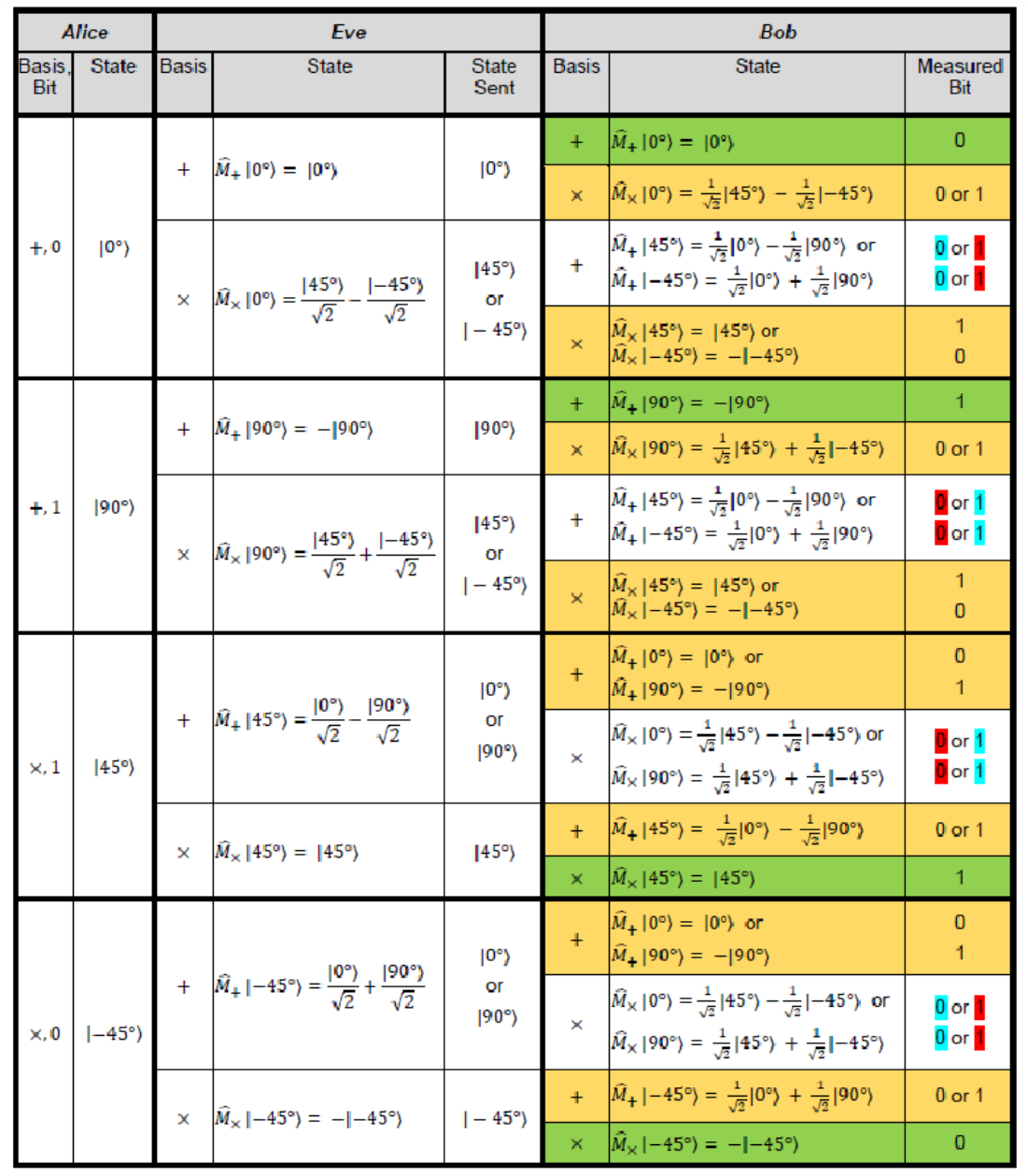
4) Метод исследования:

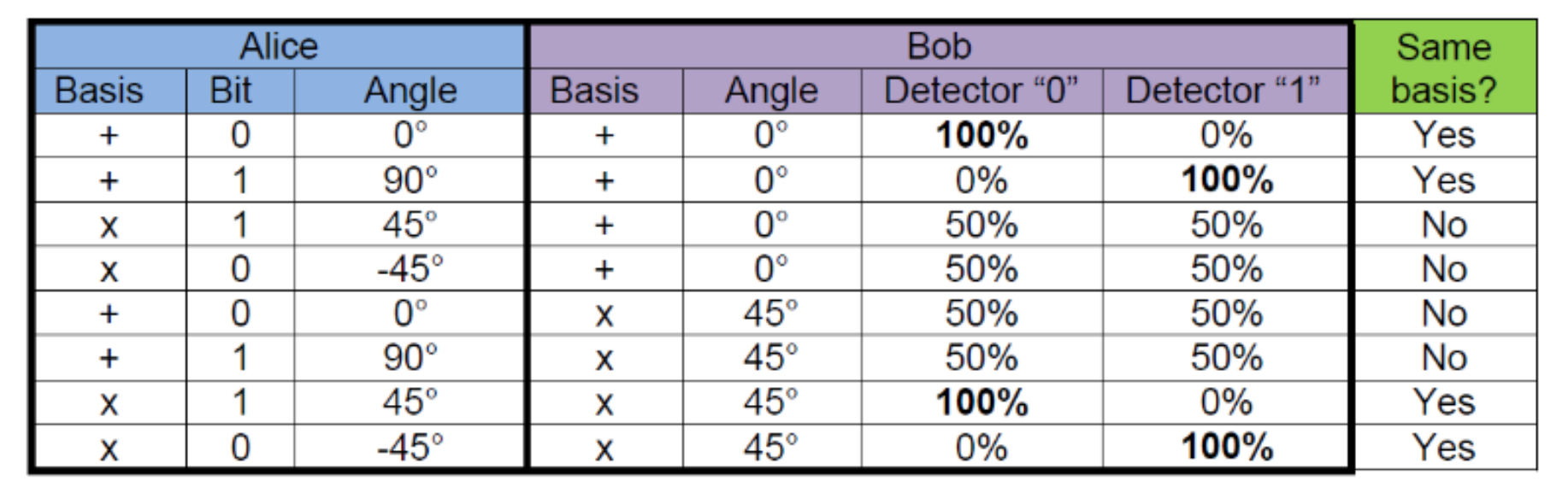
Проведение эксперимента

5) Теория:

Боб - поляризационный светоделительный куб - отражает свет с вертикальной поляризацией и пропускает горизонтальную. Если Алиса отправляет на светоделительный куб горизонтальную поляризацию света, фотон пройдет через куб насквозь = "0". Если поляризация будет повернута пластинкой на 90, фотон отразится = "1". Базис - набор из двух возможных состоянии поляризации отправленного фотона. Базисы – "0 90" и "-45 45".







6) Установка:

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" - источник единичных фотонов и поляризатор.

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**



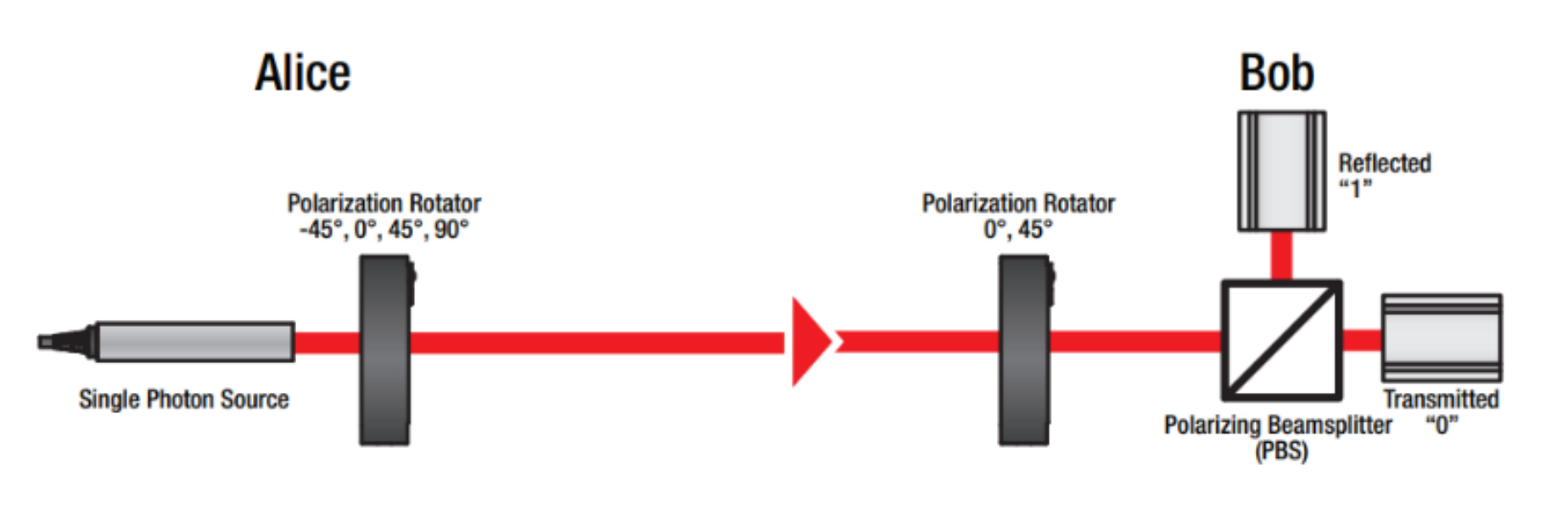
**Блок управления источником излучения**

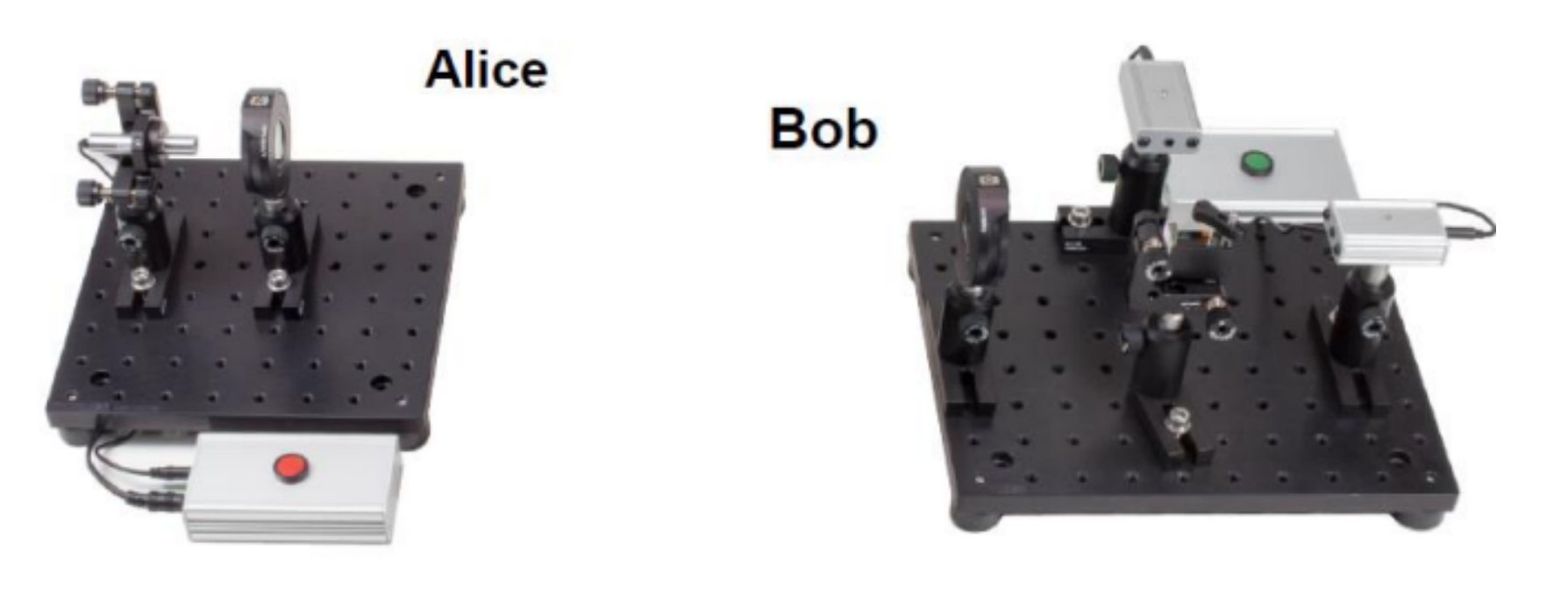


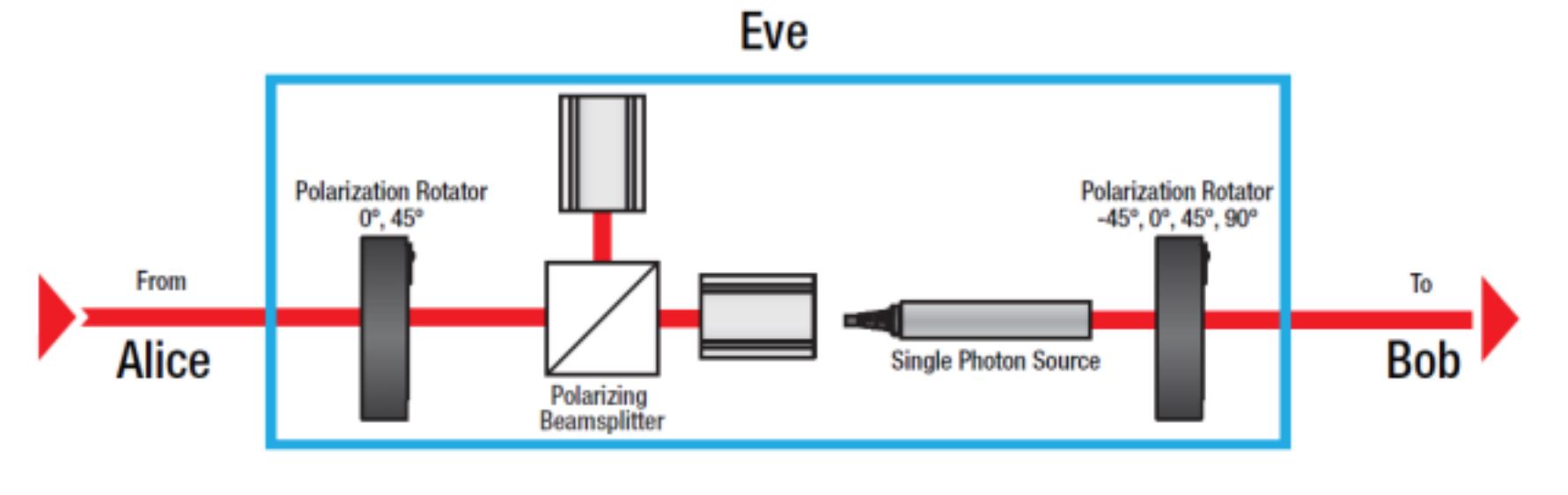
**Детектор сигнала**

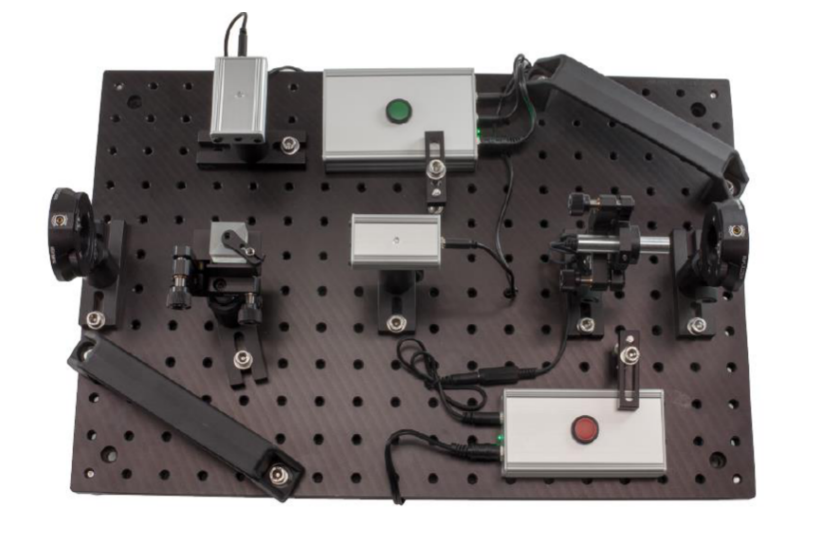


7) Схема установки:









8) Ход работы:

**Создание секретного ключа**

Возьмем случайные наборы базисов для Алисы и Боба, сгенерируем случайный набор битов, передаваемый с Алисы. Передаем сообщение с Алисы до Боба, ключом будут совпавшие биты.

**Алиса**

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| № | 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 | 1 | 1 | 0 | 0 | 1 | 1 | 0 | 0 | 1 | 1 | 1 | 1 | 0 | 0 | 0 | 1 | 1 | 0 | 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 | + | + | x | x | + | x | + | + | x | x |
| Бит | 1 | 1 | 0 | 0 | 1 | 1 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 1 | 1 | 1 | 0 | 1 | 0 | 1 | 1 |

**Боб**

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| № | 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 | 1 | 0 | 0 | 0 | 1 | 1 | 1 | 0 | 1 | 1 | 0 | 0 | 0 | 1 | 1 | 1 | 0 | 0 | 1 | 1 | 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 |

**Ключ 24 бит**

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 0 | 1 | 1 | 0 | 1 | 1 | 0 | 0 | 1 | 1 | 1 | 1 | 0 | 0 | 1 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 0 |

**Кодирование слова**

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| слово | P | | | | | Q | | | | | R | | | | | S | | | | |
| исходное | 0 | 1 | 1 | 1 | 1 | 1 | 0 | 0 | 0 | 0 | 1 | 0 | 0 | 0 | 1 | 1 | 0 | 0 | 1 | 0 |
| ключ | 0 | 1 | 1 | 0 | 1 | 1 | 0 | 0 | 1 | 1 | 1 | 1 | 0 | 0 | 1 | 0 | 0 | 1 | 0 | 0 |
| зашифрованное | 0 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 1 | 1 | 0 | 1 | 0 | 0 | 0 | 1 | 0 | 1 | 1 | 0 |

Передаем сообщение с Алисы до Боба с базисом +. Получаем те же значения битов.

Расшифровка

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| зашифрованное | 0 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 1 | 1 | 0 | 1 | 0 | 0 | 0 | 1 | 0 | 1 | 1 | 0 |
| ключ | 0 | 1 | 1 | 0 | 1 | 1 | 0 | 0 | 1 | 1 | 1 | 1 | 0 | 0 | 1 | 0 | 0 | 1 | 0 | 0 |
| исходное | 0 | 1 | 1 | 1 | 1 | 1 | 0 | 0 | 0 | 0 | 1 | 0 | 0 | 0 | 1 | 1 | 0 | 0 | 1 | 0 |
| слово | P | | | | | Q | | | | | R | | | | | S | | | | |

**Вводим в установку Еву, обнаружение перехватчика**

Алиса передает сообщение с случайным базисом, Ева его перехватывает, также выбирает случайный базис и с тем же базисом передает сообщение Бобу. Боб выбирает случайный базис и получает сообщение. После полной передачи Алиса и Боб открыто обмениваются информацией об использованных базисах, но не сообщают сами биты. Биты, для которых базисы были одинаковые сохраняются, остальные отбрасываются.

Если Ева пыталась перехватить сообщение, то из-за случайного выбора базиса около 50% её выборов будут неверными. При неверном выборе Ева изменяет состояние фотона и Боб получит неверный бит в тех случаях, когда его базис совпадает с базисом Алисы, но не с базисом Евы.

\*1 - совпавшие базисы и одинаковые значения

\*2 - совпавшие базисы, но разные значения

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | Алиса | | Ева | | Боб | |  | | |
| № | базис | бит | базис | бит | базис | бит | совпадение | \*1 | \*2 |
| 1 | x | 0 | x | 0 | + | 1 | 0 | 0 | 0 |
| 2 | + | 0 | + | 0 | + | 0 | 1 | 1 | 0 |
| 3 | x | 1 | x | 1 | + | 1 | 0 | 0 | 0 |
| 4 | x | 1 | x | 1 | + | 0 | 0 | 0 | 0 |
| 5 | x | 1 | x | 1 | + | 0 | 0 | 0 | 0 |
| 6 | + | 1 | + | 1 | + | 1 | 1 | 1 | 0 |
| 7 | x | 0 | x | 1 | x | 0 | 1 | 1 | 0 |
| 8 | + | 0 | + | 0 | x | 0 | 0 | 0 | 0 |
| 9 | + | 1 | + | 1 | x | 1 | 0 | 0 | 0 |
| 10 | + | 0 | + | 1 | + | 1 | 1 | 0 | 1 |
| 11 | x | 1 | x | 1 | + | 1 | 0 | 0 | 0 |
| 12 | x | 0 | x | 1 | + | 0 | 0 | 0 | 0 |
| 13 | x | 0 | x | 0 | + | 0 | 0 | 0 | 0 |
| 14 | x | 0 | x | 0 | x | 0 | 1 | 1 | 0 |
| 15 | + | 1 | + | 1 | x | 0 | 0 | 0 | 0 |
| 16 | + | 1 | + | 0 | x | 0 | 0 | 0 | 0 |
| 17 | + | 0 | + | 0 | + | 0 | 1 | 1 | 0 |
| 18 | x | 1 | x | 1 | x | 1 | 1 | 1 | 0 |
| 19 | + | 1 | + | 1 | x | 0 | 0 | 0 | 0 |
| 20 | x | 0 | x | 1 | x | 1 | 1 | 0 | 1 |
| 21 | + | 1 | + | 1 | x | 0 | 0 | 0 | 0 |
| 22 | + | 1 | + | 1 | x | 0 | 0 | 0 | 0 |
| 23 | x | 0 | x | 1 | x | 0 | 1 | 1 | 0 |
| 24 | x | 1 | x | 0 | x | 0 | 1 | 0 | 1 |
| 25 | + | 0 | + | 0 | x | 0 | 0 | 0 | 0 |
| 26 | + | 0 | + | 0 | + | 0 | 1 | 1 | 0 |
| 27 | + | 1 | x | 0 | x | 0 | 0 | 0 | 0 |
| 28 | + | 0 | x | 1 | + | 0 | 1 | 1 | 0 |
| 29 | + | 1 | + | 1 | + | 1 | 1 | 1 | 0 |
| 30 | + | 1 | x | 0 | x | 1 | 0 | 0 | 0 |
| 31 | x | 0 | + | 0 | + | 0 | 0 | 0 | 0 |
| 32 | + | 1 | + | 1 | + | 1 | 1 | 1 | 0 |
| 33 | + | 0 | x | 0 | x | 0 | 0 | 0 | 0 |
| 34 | x | 1 | + | 1 | x | 1 | 1 | 1 | 0 |
| 35 | + | 1 | + | 1 | + | 1 | 1 | 1 | 0 |
| 36 | x | 1 | + | 0 | + | 0 | 0 | 0 | 0 |
| 37 | x | 1 | x | 1 | x | 1 | 1 | 1 | 0 |
| 38 | x | 0 | + | 1 | x | 1 | 1 | 0 | 1 |
| 39 | x | 1 | x | 1 | x | 1 | 1 | 1 | 0 |
| 40 | + | 1 | + | 1 | x | 1 | 0 | 0 | 0 |
| 41 | + | 0 | + | 0 | x | 1 | 0 | 0 | 0 |
| 42 | x | 1 | + | 1 | + | 0 | 0 | 0 | 0 |
| 43 | + | 1 | x | 1 | + | 0 | 1 | 0 | 1 |
| 44 | x | 1 | x | 1 | x | 1 | 1 | 1 | 0 |
| 45 | x | 0 | + | 0 | + | 0 | 0 | 0 | 0 |
| 46 | + | 1 | + | 1 | + | 1 | 1 | 1 | 0 |
| 47 | x | 0 | x | 0 | + | 1 | 0 | 0 | 0 |
| 48 | x | 1 | + | 1 | + | 1 | 0 | 0 | 0 |
| 49 | + | 0 | x | 1 | x | 1 | 0 | 0 | 0 |
| 50 | x | 1 | + | 0 | + | 0 | 0 | 0 | 0 |
| 51 | x | 0 | + | 0 | + | 0 | 0 | 0 | 0 |
| 52 | + | 0 | + | 0 | + | 0 | 1 | 1 | 0 |

Совпадений базисов между Алисой и Бобом – 23

Из них совпадений битов – 18

Ошибок – 5

Следовательно ошибок – 22%, что указывает на вмешательство Евы

p.s. процент ошибок не стремится к 50 из-за естественного интеллекта, участвовавшего в «случайном» выборе базисов.

9) Выводы:

В первой части эксперимента был создан секретный ключ длиной 24 бит. Для этого Алиса и Боб обменялись информацией о базисах, отбросили несовпадающие измерения и сформировали ключ из оставшихся битов.

Во второй части сообщение длиной 4 буквы было зашифровано с использованием полученного ключа и передано Бобу по открытому каналу. Сообщение успешно расшифровано Бобом, подтверждая работоспособность метода при отсутствии перехватчика.

В третьей части, после введения в установку Евы, были зафиксированы ошибки в переданных данных. Анализ этих ошибок позволил обнаружить вмешательство перехватчика, что подтвердило эффективность квантовой криптографии для защиты информации.