

Группа М32111 К работе допущен

Студент Денисенко Максим, Акберов Рустам Работа выполнена Преподаватель Шоев В.И Отчет принят

Рабочий протокол и отчет по лабораторной работе

№ 5.06

Изучение принципов работы квантовой криптографии

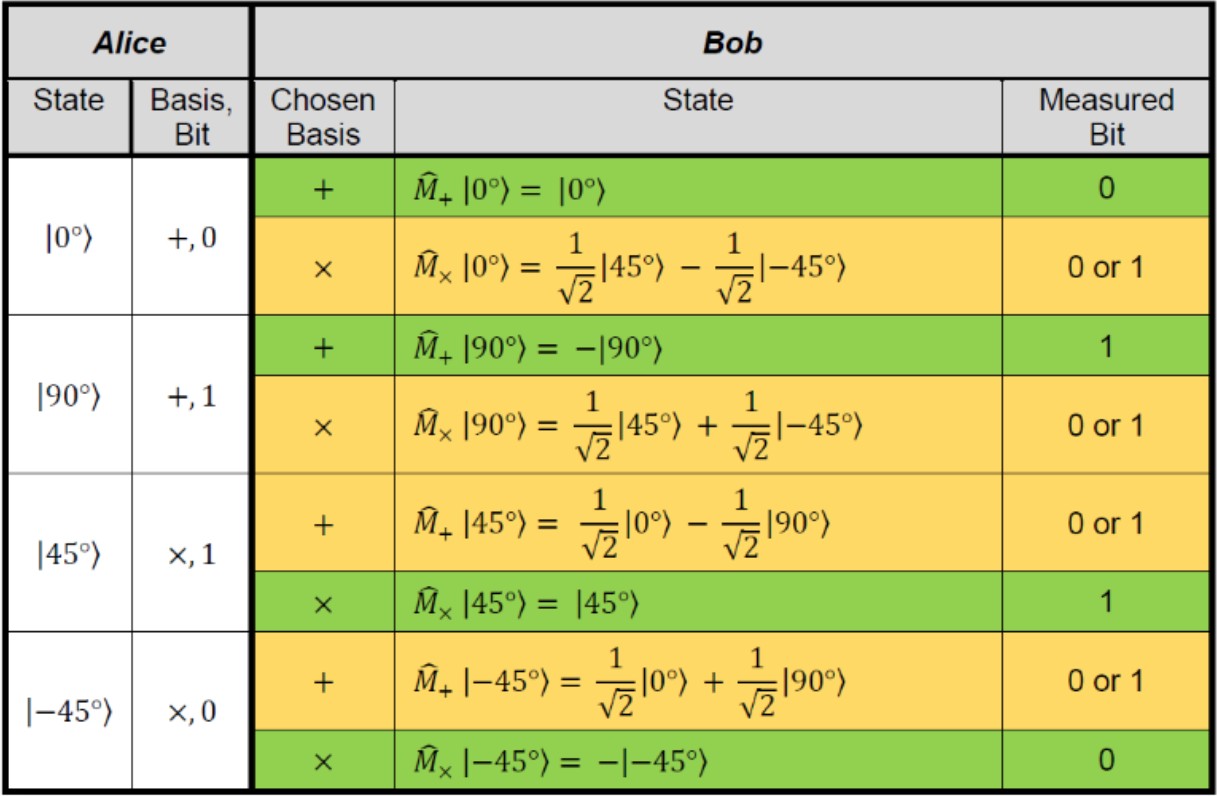
# Цель работы:

1. Изучение основных принципов квантовой связи
2. Создание зашифрованного сообщения
3. Обнаружение перехватчика

# Объект исследования:

Импульсный источник света.

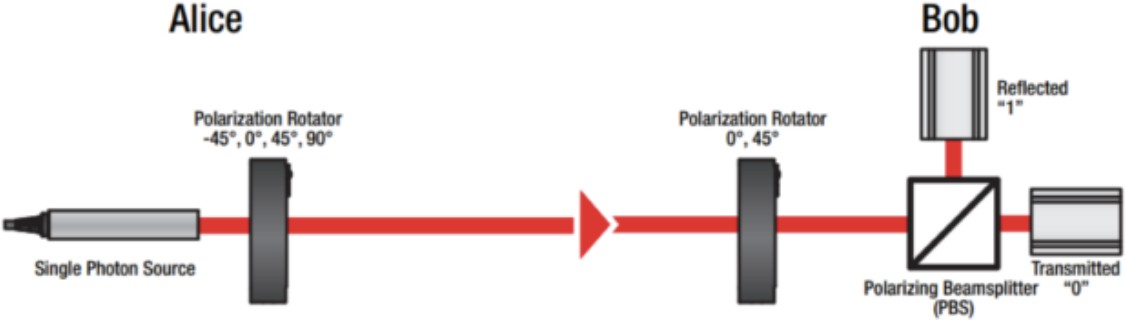
# Рабочие формулы и исходные данные:



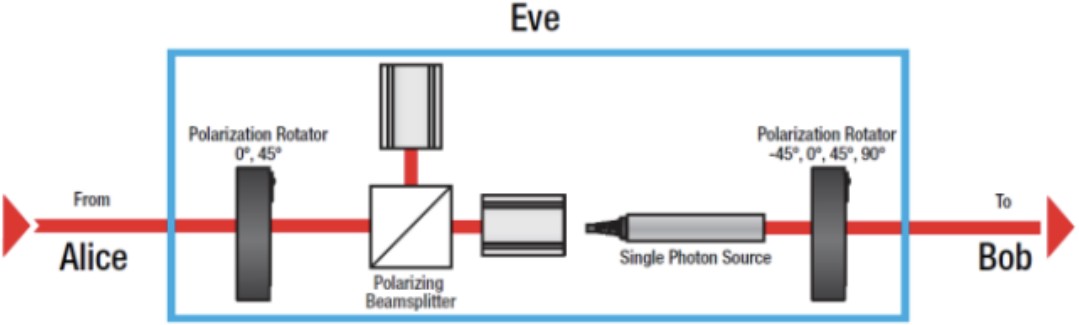
у Алисы и Боба совпадают базисы и значения битов можно использовать, как ключ – зеленый; Желтое – базисы не совпадают и измерение нужно отбросить

# Схема установки:

Установка состоит из 3 основных элементов: Алиса, Боб и Ева



В эксперименте с Алисой, Евой и Бобом:



# Необходимый материал:



**Расчет результатов косвенных измерений:**

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Alice | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 |
| Basis | + | x | x | x | + | x | + | + | x | + | + | + | + | x | + | x | x | x | + | x | x |
| Bit | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 0 | 1 | 1 | 0 | 0 | 1 | 0 | 0 | 1 | 1 | 1 | 0 |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Alice | 22 | 23 | 24 | 25 | 26 | 27 | 28 | 29 | 30 | 31 | 32 | 33 | 34 | 35 | 36 | 37 | 38 | 39 | 40 | 41 |
| Basis | + | + | + | x | x | + | x | x | x | + | x | + | + | x | + | + | + | + | x | + |
| Bit | 0 | 1 | 1 | 1 | 0 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 0 | 1 | 1 | 1 | 0 | 0 |

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Alice | 42 | 43 | 44 | 45 | 46 | 47 | 48 | 49 | 50 | 51 | 52 |
| Basis | x | x | x | + | x | x | + | + | + | x | x |
| Bit | 0 | 1 | 1 | 0 | 1 | 1 | 0 | 0 | 1 | 1 | 0 |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Bob | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 |
| Basis | x | x | x | + | + | x | + | + | x | + | x | x | + | x | + | + | x | x | + | x | x |
| Bit | 0 | 1 | 0 | 0 | 0 | 1 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 0 | 0 | 1 | 1 | 1 | 0 |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Bob | 22 | 23 | 24 | 25 | 26 | 27 | 28 | 29 | 30 | 31 | 32 | 33 | 34 | 35 | 36 | 37 | 38 | 39 | 40 | 41 |
| Basis | + | + | x | + | x | + | x | x | x | + | x | + | + | x | + | + | + | + | x | + |

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

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Bob | 42 | 43 | 44 | 45 | 46 | 47 | 48 | 49 | 50 | 51 | 52 |
| Basis | x | x | x | + | x | x | + | + | + | x | x |
| Bit | 0 | 1 | 1 | 0 | 1 | 1 | 0 | 0 | 1 | 1 | 0 |

Ключ: 1001 0100 0010 1110 0100

# Кодировка 4-х буквенного слова:

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Letter** | T | | | | | H | | | | | O | | | | | R | | | | |
| **Data Bit** | 1 | 0 | 0 | 1 | 1 | 0 | 0 | 1 | 1 | 1 | 0 | 1 | 1 | 1 | 0 | 1 | 0 | 0 | 0 | 1 |
| **Key Bit** | 1 | 0 | 0 | 1 | 0 | 1 | 0 | 0 | 0 | 0 | 1 | 0 | 1 | 1 | 1 | 0 | 0 | 1 | 0 | 0 |
| **Encrypt ed Bit** | 0 | 0 | 0 | 0 | 1 | 1 | 0 | 1 | 1 | 1 | 1 | 1 | 0 | 0 | 1 | 1 | 0 | 1 | 0 | 1 |

Передача зашифрованного сообщения Бобу:

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Encrypt ed Bit** | 0 | 0 | 0 | 0 | 1 | 1 | 0 | 1 | 1 | 1 | 1 | 1 | 0 | 0 | 1 | 1 | 0 | 1 | 0 | 1 |
| **Key Bit** | 1 | 0 | 0 | 1 | 0 | 1 | 0 | 0 | 0 | 0 | 1 | 0 | 1 | 1 | 1 | 0 | 0 | 1 | 0 | 0 |
| **Data Bit** | 1 | 0 | 0 | 1 | 1 | 0 | 0 | 1 | 1 | 1 | 0 | 1 | 1 | 1 | 0 | 1 | 0 | 0 | 0 | 1 |
| **Letter** | T | | | | | H | | | | | O | | | | | R | | | | |

# Введение в установку Евы и обнаружение перехватчика Алисой и Бобом:

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Alice | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 |
| Basis | + | x | x | x | + | x | + | + | x | + | + | + | + | x | + | x | x | x | + | x | x |
| Bit | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 0 | 1 | 1 | 0 | 0 | 1 | 0 | 0 | 1 | 1 | 1 | 0 |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Alice | 22 | 23 | 24 | 25 | 26 | 27 | 28 | 29 | 30 | 31 | 32 | 33 | 34 | 35 | 36 | 37 | 38 | 39 | 40 | 41 |
| Basis | + | + | + | x | x | + | x | x | x | + | x | + | + | x | + | + | + | + | x | + |
| Bit | 0 | 1 | 1 | 1 | 0 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 0 | 1 | 1 | 1 | 0 | 0 |

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Alice | 42 | 43 | 44 | 45 | 46 | 47 | 48 | 49 | 50 | 51 | 52 |
| Basis | x | x | x | + | x | x | + | + | + | x | x |
| Bit | 0 | 1 | 1 | 0 | 1 | 1 | 0 | 0 | 1 | 1 | 0 |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Eve | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 |
| Basis | x | x | x | + | x | + | + | + | + | + | + | x | x | + | x | + | x | x | x | x | x |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Eve | 22 | 23 | 24 | 25 | 26 | 27 | 28 | 29 | 30 | 31 | 32 | 33 | 34 | 35 | 36 | 37 | 38 | 39 | 40 | 41 | 42 |
| Basis | x | + | x | x | x | x | + | + | x | + | x | + | + | x | + | x | x | + | + | x | x |

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Eve | 43 | 44 | 45 | 46 | 47 | 48 | 49 | 50 | 51 | 52 |
| Basis | + | + | + | + | x | x | + | x | + | x |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Bob | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 |
| Basis | **x** | **x** | **x** | **+** | **+** | **x** | **+** | **+** | **x** | **+** | **x** | **x** | **+** | **x** | **+** | **+** | **x** | **x** | **+** | **x** | **x** |
| Bit | **1** | **1** | **0** | **0** | **1** | **0** | **0** | **1** | **0** | **0** | **0** | **0** | **1** | **0** | **1** | **1** | **0** | **1** | **0** | **1** | **0** |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Bob | 22 | 23 | 24 | 25 | 26 | 27 | 28 | 29 | 30 | 31 | 32 | 33 | 34 | 35 | 36 | 37 | 38 | 39 | 40 | 41 |
| Basis | **+** | **+** | **x** | **+** | **x** | **+** | **x** | **x** | **x** | **+** | **x** | **+** | **+** | **x** | **+** | **+** | **+** | **+** | **x** | **+** |
| Bit | **1** | **1** | **1** | **0** | **0** | **0** | **0** | **0** | **1** | **0** | **1** | **0** | **1** | **0** | **0** | **0** | **0** | **1** | **0** | **1** |

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Bob | 42 | 43 | 44 | 45 | 46 | 47 | 48 | 49 | 50 | 51 | 52 |
| Basis | **x** | **x** | **x** | **+** | **x** | **x** | **+** | **+** | **+** | **x** | **x** |
| Bit | **1** | **1** | **0** | **0** | **1** | **1** | **0** | **1** | **1** | **1** | **0** |

**Вывод:**

Базисы совпали в 45 случаях, но 12 битов переданы с ошибкой.

В ходе первого эксперимента Бобу было передано зашифрованное с помощью ранее созданного ключа сообщение в однобазисной системе. Боб получил и корректно его расшифровал.

В ходе второго эксперимента в установку был введен перехватчик Ева. В двухбазисной системе Алиса передала 52 бита в случайно выбранном базисе. Базисы Алисы и Боба совпали в 45 случаях, из них в 33 бита были переданы верно. То есть 26% битов были переданы с ошибкой, откуда следует присутствие перехватчика.