

Лабораторная работа № 5.06

ИЗУЧЕНИЕ ПРИНЦИПОВ РАБОТЫ КВАНТОВОЙ КРИПТОГРАФИИ

Содержание

Введение	2
Одноразовый ключ	2
Однобазисная система	4
Двухбазисная схема	5
Перехватчик	8
Понятие случайного события	8
Пример проведения эксперимента	9
Математическое описание	10
Выполнение протокола шифрования	14
Протокол шифрования в присутствии Евы	18
Экспериментальная установка	21
Порядок выполнения работы	26
Контрольные вопросы	28
Приложение	29

Цели работы

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

Введение

“Криптография предназначена для шифрования данных, таким образом, что исходное сообщение изменяется до неузнаваемости и становится читаемым только для отправителя и адресата. Читаемость достигается использованием заранее выбранной кодировки, с помощью которой оно было изменено”. Классические механизмы криптографии имеют тот недостаток, что со временем могут быть взломаны. Однако, эта фундаментальная проблема может быть решена использованием квантовой физики. Основное правило квантовой физики говорит о том, что измерение состояния фотона или частицы необратимо изменяет это состояние. Этот принцип, наряду с качественной методикой генерации случайных чисел, позволит создать действительно случайный код, известный только отправителю и получателю информации.

Одноразовый ключ

Этот метод криптографии дает 100% гарантию безопасности при условии, что необходимые условия удовлетворяются. Сам метод является классической техникой, однако квантовая физика дает возможность реализации условий, при которых он срабатывает. Представим себе сообщение, закодированное последовательностью нулей и единиц таким образом, что каждая буква это набор из четырех символов. Например, словес TEST ниже:


Word	T				E				S				T							
																				
Binary word	1	0	0	1	1	0	0	1	0	0	1	0	0	1	0	1	0	0	1	1

Рис. 1

Если мы введем ключ шифрования, также представляющий из себя последовательность нулей и единиц, и назначим правило соответствие в виде:

$$0 + 0 = 0,$$

$$1 + 0 = 1,$$

$$0 + 1 = 1,$$

$$1 + 1 = 0.$$

То добавив данный код к исходному сообщению, мы получим зашифрованное сообщение в виде

Word	T					E					S					T				
Binary word	1	0	0	1	1	0	0	1	0	0	1	0	0	1	0	1	0	0	1	1
+																				
Key (random)	1	1	0	1	0	1	0	0	0	1	1	0	1	0	0	1	1	1	0	1
Encrypted message	0	1	0	0	1	1	0	1	0	1	0	0	1	1	0	0	1	1	1	0

Рис. 2

Для перехватившего сообщение человека, зашифрованная последовательность при переводе нулей и единиц в буквы даст полную бессмыслицу. Только получатель, знающий шифр, суммет раскодировать исходное сообщение:

Encrypted message	0	1	0	0	1	1	0	1	0	1	0	0	1	1	0	0	1	1	1	0
+																				
Key (as above)	1	1	0	1	0	1	0	0	0	1	1	0	1	0	0	1	1	1	0	1
Binary word	1	0	0	1	1	0	0	1	0	0	1	0	0	1	0	1	0	0	1	1
Word	T					E					S					T				

Рис. 3

Правила данного метода шифрования следующие:

- Длина ключа должна быть не меньше длины исходного сообщения
- Ключ может быть использован только единожды
- Ключ должен быть полностью случайным
- Ключ должен быть известен только получателю и адресату

Однобазисная система.

Пластинка $\lambda/2$ и однобазисная передача данных

Для лучшего понимания того, что буде приведено ниже (двух-базисный механизм), рассмотрим сперва однобазисный механизм передачи данных. Мы используем поляризацию фотона как средство передачи информации. Фотон с горизонтальной поляризацией будем интерпретировать как 0, с вертикальной как 1. Экспериментальная установка для реализации подобного механизма будет выглядеть следующим образом:

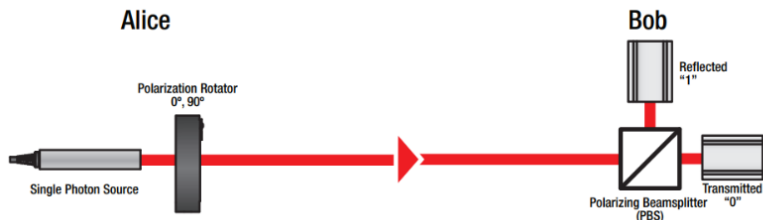


Рис. 4

Традиционно отправителя сообщения принято обозначать именем Алиса, получателя – Боб. Перехватчика сообщения обычно называют Евой (от английского eavesdropping - подслушивание).

Отправителем Алисой в данном случае является источник единичных фотонов и полуволновая пластинка. Полуволновая пластинка, как известно, поворачивает вектор поляризации на удво-

енный угол относительно угла между оптической осью пластинки и исходным вектором поляризации падающего света. Принцип работы полу-волновой пластинки приведен на рисунке ниже. Прием-

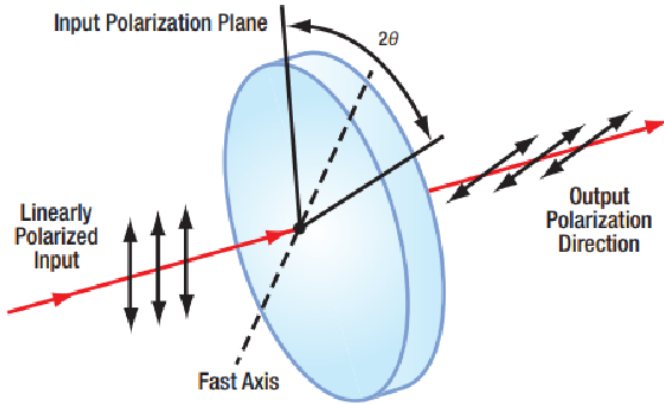


Рис. 5

ник “Боб” представляет из себя поляризационный светоделительный куб и два фотоприемника. Куб отражает свет с вертикальной поляризацией и пропускает горизонтальную, как показано на рисунке: Если Алиса отправляет на светоделительный куб горизонтальную поляризацию света, фотон пройдет через куб насквозь, этому событию мы положим значения “0”. Если поляризация будет повернута пластинкой на 90° , фотон отразится. Этому событию мы приписываем значение “1”. Базисом мы называем набор из двух возможных состояний поляризации отправленного фотона, одному из которых приписано значение 0, другому 1.

Двухбазисная схема

Описанный выше однобазисный метод достаточен для передачи данных между Алисой и Бобом, однако, недостаточно защищен от перехвата. Для выполнения этой задачи вводится двух-базисная схема. Крое набора из поляризаций $(0^\circ, 90^\circ)$ – который мы будем

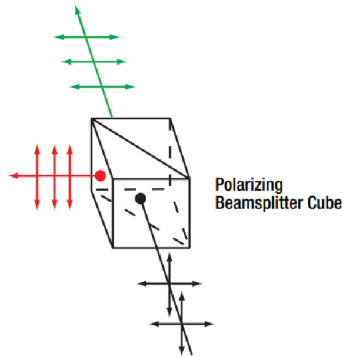


Рис. 6

обозначать как $+$, добавим еще один $(+45^\circ, -45^\circ)$, соответственно, обозначение будет буква X . Для реализации подобного двух- базисного варианта установка будет выглядеть как: Теперь для генера-

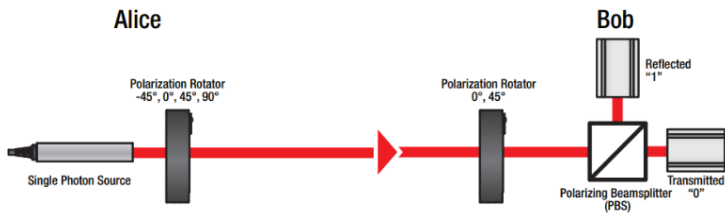


Рис. 7

ции ключа, Алисе требуется сделать следующее: случайным образом выбрать базис (X или $+$) и внутри базиса присвоить значения 1 и 0 также случайным образом, например:

- **$+$ базис:**
 - поляризация $0^\circ - 0$
 - поляризация $90^\circ - 1$

• **X базис:**

- поляризация -45° – 0
- поляризация 45° – 1

В свою очередь Боб устанавливает анализатор таким образом, чтобы тестировать + и X базисы. Соответственно, ему нужны положения 0° и 45° . В случае, когда Алиса отправляет фотон в базисе +, а Боб принимает в то же базисе, результат однозначен. Это же относится и к X базису. Но что произойдет, если они не совпадают? В этой ситуации, на светоделительный куб Боба будет направлен свет поляризованный под 45° . В случае протяженного пучка, половина будет отражена, половина пройдет. Для ситуации с единичным фотоном, с вероятностью 50% он будет либо отражен, либо пройдет насквозь.

Рассмотрим различные варианты обмена сигналами между Алисой и Бобом: Только в случае совпадения базисов, Бобу возможно

Alice			Bob				Same basis?
Basis	Bit	Angle	Basis	Angle	Detector "0"	Detector "1"	
+	0	0°	+	0°	100%	0%	Yes
+	1	90°	+	0°	0%	100%	Yes
x	1	45°	+	0°	50%	50%	No
x	0	-45°	+	0°	50%	50%	No
+	0	0°	x	45°	50%	50%	No
+	1	90°	x	45°	50%	50%	No
x	1	45°	x	45°	100%	0%	Yes
x	0	-45°	x	45°	0%	100%	Yes

Рис. 8

получить однозначно различимый результат. Однако, установить соответствие битов 0 и 1 и базисов Бобу возможно только в одном случае — если после обмена сигналами Алиса по открытому каналу связи сообщит Бобу, какой базис использовался. Теперь, после проведения измерений, и Алиса и Боб знают один и тот же ключ и Алиса может передать Бобу зашифрованное сообщение, которое тот сможет распознать.

Перехватчик

Рассмотрим ситуацию, когда между Алисой и Бобом внедряется перехватчик информации — Ева. Перехватчик собран аналогично Алисе и Бобу, только в обратной последовательности: Ева получает

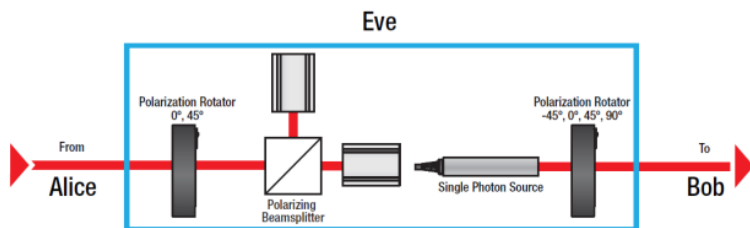


Рис. 9

информацию от Алисы, анализирует, и отправляет Бобу такой же сигнал. Возможны два варианта развития событий:

Ева угадывает правильный базис: Все, как описано выше для обмена сигналами между Алисой и Бобом

Ева не угадывает правильный базис: На один из детекторов приходит неправильный бит информации, поэтому, Ева не сможет это определить, и отправит Бобу сигнал в случайном базисе. При дальнейшей сверке базисов между Алисой и Бобом это будет заметно – с вероятностью в 25% даже в случае правильного базиса биты информации будут не совпадать, таким образом станет очевидно, что на линии передачи информации находится перехватчик, искажающий сигнал.

Понятие случайного события

Выбор ключа должен происходить исключительно случайным образом. Цифровая компьютерная генерация случайных чисел не является 100% защищенной. Квантовая физика является в этом случае более надежным инструментом – фотон, попадающий на светоделительный куб, равновероятно отразится и пройдет насквозь. Традиционно, отраженному фотону приписывают бит “0”, прошед-

шему — “1”. В ситуации волновой оптики, когда излучение падает на светоделительный куб, распределений регистраций на фотодетекторах так же абсолютно случайно.

Пример проведения эксперимента

1. **Передача ключа.** Алиса случайным образом выбирает базис(+/х) и бит (1 и 0) в этом базисе. Боб наугад выбирает базис. Установки настраиваются соответствующим образом, и посылается лазерный импульс. Боб выбирает значение полученного бита (0 или 1). Повторите достаточное количество раз (>10)
2. **Отбраковка некорректных базисов.** Алиса и Боб выполняют обмен сигналами, и после этого обмениваются базисами для каждого случая. Биты в случае совпадающих базисов сохраняются, остальные удаляются. Сохраненные биты становятся тайным ключом шифрования
3. **Проверка подслушивания.** Алиса и Боб открыто сравнивают биты сохраненные после п.2. В случае наличия ошибок, возможно присутствие шпиона (Ева) и ключ удаляется. Если же шпион не обнаружен и ошибок нет, протестированные биты удаляются и оставшиеся становятся финальным ключом шифрования.
4. **Шифрование.** Используя созданный финальный ключ, Алиса может зашифровать сообщение для Боба
5. **Передача сообщения.** Алиса отправляет зашифрованный сигнал Бобу по открытым каналам
6. **Расшифровка сообщения.** С помощью ключа, Боб расшифровывает сообщение

Отличие квантовой криптографии и данного эксперимента заключается в том, что подлинная безопасность может быть обеспечена только с помощью использования единичных квантов. Бит

информации может быть передан только единичным фотоном для невозможности копирования или измерения состояния без изменений. При использовании источника света наподобие лазера, Ева не может быть обнаружена. Все, что нужно Еве – это отвести часть светового потока для анализа и незаметно для Боба воспроизвести скопированный сигнал. В работе используется импульсный источник света, и хотя это не целиком квантовая криптография, принцип воспроизводится достаточно точно.

Математическое описание

Описание состояний поляризации будет удобно вести в форме bra-ket введенной Дираком. Возможные варианты $(0, 90, +45, -45)$ записываются в матричной форме как: $|0\rangle, |90\rangle, | +45\rangle, | -45\rangle$

Для системы координат:

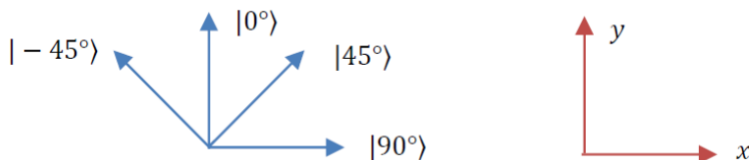


Рис. 10

Данные обозначения представляют собой матрицы (x, y) наподобие

$$|0^\circ\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \quad |90^\circ\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

Мы будем часто использовать правило скалярного перемножения матриц,

$$\langle 90^\circ | 0^\circ \rangle = (1 \ 0) \cdot \begin{pmatrix} 0 \\ 1 \end{pmatrix} = 0$$

И тот факт, что квадрат такого произведения для двух матриц состояния поляризации даст вероятность того, что фотон с вектором поляризации ориентированным на 0° пройдет через анализатор на

90° . Другие состояния поляризации можно выразить через комбинации этих матриц как:

$$|45^\circ\rangle = \alpha \cdot |0^\circ\rangle + \beta \cdot |90^\circ\rangle.$$

Чтобы получить значения α и β заметим, что скалярная сумма должна быть нормализована, в виде:

$$\begin{aligned} 1 = |\langle 45^\circ | 45^\circ \rangle|^2 &= \alpha^* \alpha \underbrace{\langle 0^\circ | 0^\circ \rangle}_{=1} + \alpha^* \beta \underbrace{\langle 0^\circ | 90^\circ \rangle}_{=0} + \\ &+ \alpha \beta^* \underbrace{\langle 90^\circ | 0^\circ \rangle}_{=0} + \beta^* \beta \underbrace{\langle 90^\circ | 90^\circ \rangle}_{=1} = |\alpha|^2 + |\beta|^2. \end{aligned}$$

Из соображений симметрии, $\alpha = \beta = \frac{1}{\sqrt{2}}$. Таким образом, все четыре состояния поляризации фотонов могут быть выражены как комбинации в различных базисах:

$$\begin{aligned} | + 45^\circ \rangle &= \frac{1}{\sqrt{2}} |0^\circ\rangle + \frac{1}{\sqrt{2}} |90^\circ\rangle, \\ | - 45^\circ \rangle &= \frac{1}{\sqrt{2}} |0^\circ\rangle - \frac{1}{\sqrt{2}} |90^\circ\rangle, \\ |0^\circ\rangle &= \frac{1}{\sqrt{2}} | + 45^\circ \rangle + \frac{1}{\sqrt{2}} | - 45^\circ \rangle, \\ |90^\circ\rangle &= \frac{1}{\sqrt{2}} | + 45^\circ \rangle - \frac{1}{\sqrt{2}} | - 45^\circ \rangle. \end{aligned}$$

Также это разложение может быть записано в векторном представлении: $|\pm 45^\circ\rangle = (1/\sqrt{2}, \pm 1/\sqrt{2})^T$

В таком случае вероятность, что фотон с поляризацией 0° пройдет через анализатор ориентированный под 45° будет вычисляться как:

$$|\langle 45^\circ | 0^\circ \rangle|^2 = \left| \frac{1}{\sqrt{2}} \underbrace{\langle 45^\circ | 45^\circ \rangle}_{=1} + \frac{1}{\sqrt{2}} \underbrace{\langle 45^\circ | - 45^\circ \rangle}_{=0} \right|^2 = \frac{1}{2}.$$

Что означает, что данная вероятность равна 50%. В реальном эксперименте, Алиса и Боб могут только выбрать базис, и наблюдать, какой детектор регистрирует событие. Но как это выразить математически?

Введем операторы \widehat{M}_+ , \widehat{M}_X для описания измерений, сделанных в соответствующем базисе как:

$$\begin{aligned}\widehat{M}_+ &= |0\rangle\langle 0| - |90\rangle\langle 90|, \\ \widehat{M}_X &= |45\rangle\langle 45| - |-45\rangle\langle -45|.\end{aligned}$$

Пусть оператор в $+$ базисе действует на вертикальную и горизонтальную поляризацию:

$$\begin{aligned}\widehat{M}_+|0\rangle &= |0\rangle\langle 0|0\rangle - |90\rangle\langle 90|0\rangle = |0\rangle - |90\rangle \cdot 0 = |0\rangle, \\ \widehat{M}_+|90\rangle &= |0\rangle\langle 0|90\rangle - |90\rangle\langle 90|90\rangle = |0\rangle \cdot 0 - |90\rangle = -|90\rangle.\end{aligned}$$

Обратим внимание, что сами \widehat{M}_+ и \widehat{M}_X – поддающиеся измерению величины, в то время как собственные вектора $|0\rangle$ и $|90\rangle$ это всего лишь возможные состояния системы. Собственные значения $+1$ и -1 означают возможные результаты измерений. $+1$ обозначает фотон, прошедший насквозь, -1 – отраженный фотон. Диагональная поляризация фотона, измеренная в диагональном базисе будет выглядеть как:

$$\begin{aligned}\widehat{M}_X|+45\rangle &= | +45\rangle\langle +45| +45\rangle - | -45\rangle\langle -45| +45\rangle = |45\rangle, \\ \widehat{M}_X|-45\rangle &= | +45\rangle\langle +45| -45\rangle - | -45\rangle\langle -45| -45\rangle = -|-45\rangle.\end{aligned}$$

Значение -1 в данном случае означает пропускание. Это определяется тем, что для базиса X мы не поворачиваем светоделительный куб под 45° но вращаем поляризацию падающего пучка полуволновой пластинкой. Но что будет происходить при падении 45° фотона на 0° Пластинку $\lambda/2$ в базисе $+$? Как было показано

выше, с вероятностью 50% фотон либо отразится либо пройдет насквозь. Точное вычисление даст суперпозицию состояний $|0\rangle$ и $|90\rangle$ следующим образом:

$$\begin{aligned}\widehat{M}_+|+45\rangle &= |0\rangle\langle 0|\left[\frac{1}{\sqrt{2}}|0^\circ\rangle + \frac{1}{\sqrt{2}}|90^\circ\rangle\right] - |90\rangle\langle 90|\left[\frac{1}{\sqrt{2}}|0^\circ\rangle + \right. \\ &+ \left.\frac{1}{\sqrt{2}}|90^\circ\rangle\right] = \frac{1}{\sqrt{2}}|0\rangle\langle 0|0\rangle + \frac{1}{\sqrt{2}}|0\rangle\langle 0|90\rangle - \frac{1}{\sqrt{2}}|90\rangle\langle 90|0\rangle - \\ &- \frac{1}{\sqrt{2}}|90\rangle\langle 90|90\rangle = \frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|90\rangle,\end{aligned}$$

$$\widehat{M}_+|-45\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|90\rangle.$$

Аналогично, измеряя в X базисе вертикальную и горизонтальные поляризации фотона, мы имеем

$$\begin{aligned}\widehat{M}_X|0\rangle &= \frac{1}{\sqrt{2}}|45\rangle - \frac{1}{\sqrt{2}}|-45\rangle, \\ \widehat{M}_X|45\rangle &= \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|-45\rangle.\end{aligned}$$

Теперь, зная, как меняется состояние фотонов мы можем математически описать измерения, которые делают Алиса, Боб и Ева, как это описано выше. Для начала рассмотрим ситуацию, когда Ева отсутствует в эксперименте. Зеленым выделены ситуации, когда у Алисы и Боба совпадают базисы, и значения битов можно использовать как ключ. Желтое – базисы не совпадают, и измерение нужно отбросить. Теперь рассмотрим ситуацию, когда в системе внедрена Ева:

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

Рис. 11

Выполнение протокола шифрования (Алиса + Боб)

1. Алиса случайным образом выбирает базисы и биты, Боб случайным образом выбирает базисы.

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

Bob																		
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
Basis	+	x	x	x	+	+	+	x	+	x	x	+	+	x	+	+	+	x
Bit																		

Рис. 13

2. Алиса посылает сигналы, Боб записывает результаты своих

Alice		Eve			Bob		
Basis Bit	State	Basis	State	State Sent	Basis	State	Measured Bit
+, 0	$ 0^\circ\rangle$	+	$\hat{M}_+ 0^\circ\rangle = 0^\circ\rangle$	$ 0^\circ\rangle$	+	$\hat{M}_+ 0^\circ\rangle = 0^\circ\rangle$	0
					\times	$\hat{M}_\times 0^\circ\rangle = \frac{1}{\sqrt{2}} 45^\circ\rangle - \frac{1}{\sqrt{2}} -45^\circ\rangle$	0 or 1
		\times	$\hat{M}_\times 0^\circ\rangle = \frac{ 45^\circ\rangle}{\sqrt{2}} - \frac{ -45^\circ\rangle}{\sqrt{2}}$	$ 45^\circ\rangle$ or $ - 45^\circ\rangle$	+	$\hat{M}_+ 45^\circ\rangle = \frac{1}{\sqrt{2}} 0^\circ\rangle - \frac{1}{\sqrt{2}} 90^\circ\rangle$ or $\hat{M}_+ -45^\circ\rangle = \frac{1}{\sqrt{2}} 0^\circ\rangle + \frac{1}{\sqrt{2}} 90^\circ\rangle$	0 or 1
					\times	$\hat{M}_\times 45^\circ\rangle = 45^\circ\rangle$ or $\hat{M}_\times -45^\circ\rangle = - -45^\circ\rangle$	1 0
+, 1	$ 90^\circ\rangle$	+	$\hat{M}_+ 90^\circ\rangle = - 90^\circ\rangle$	$ 90^\circ\rangle$	+	$\hat{M}_+ 90^\circ\rangle = - 90^\circ\rangle$	1
					\times	$\hat{M}_\times 90^\circ\rangle = \frac{1}{\sqrt{2}} 45^\circ\rangle + \frac{1}{\sqrt{2}} -45^\circ\rangle$	0 or 1
		\times	$\hat{M}_\times 90^\circ\rangle = \frac{ 45^\circ\rangle}{\sqrt{2}} + \frac{ -45^\circ\rangle}{\sqrt{2}}$	$ 45^\circ\rangle$ or $ - 45^\circ\rangle$	+	$\hat{M}_+ 45^\circ\rangle = \frac{1}{\sqrt{2}} 0^\circ\rangle - \frac{1}{\sqrt{2}} 90^\circ\rangle$ or $\hat{M}_+ -45^\circ\rangle = \frac{1}{\sqrt{2}} 0^\circ\rangle + \frac{1}{\sqrt{2}} 90^\circ\rangle$	0 or 1 0 or 1
					\times	$\hat{M}_\times 45^\circ\rangle = 45^\circ\rangle$ or $\hat{M}_\times -45^\circ\rangle = - -45^\circ\rangle$	1 0
$\times, 1$	$ 45^\circ\rangle$	+	$\hat{M}_+ 45^\circ\rangle = \frac{ 0^\circ\rangle}{\sqrt{2}} - \frac{ 90^\circ\rangle}{\sqrt{2}}$	$ 0^\circ\rangle$ or $ 90^\circ\rangle$	+	$\hat{M}_+ 0^\circ\rangle = 0^\circ\rangle$ or $\hat{M}_+ 90^\circ\rangle = - 90^\circ\rangle$	0 1
					\times	$\hat{M}_\times 0^\circ\rangle = \frac{1}{\sqrt{2}} 45^\circ\rangle - \frac{1}{\sqrt{2}} -45^\circ\rangle$ or $\hat{M}_\times 90^\circ\rangle = \frac{1}{\sqrt{2}} 45^\circ\rangle + \frac{1}{\sqrt{2}} -45^\circ\rangle$	0 or 1 0 or 1
		\times	$\hat{M}_\times 45^\circ\rangle = 45^\circ\rangle$	$ 45^\circ\rangle$	+	$\hat{M}_+ 45^\circ\rangle = \frac{1}{\sqrt{2}} 0^\circ\rangle - \frac{1}{\sqrt{2}} 90^\circ\rangle$	0 or 1
					\times	$\hat{M}_\times 45^\circ\rangle = 45^\circ\rangle$	1
$\times, 0$	$ - 45^\circ\rangle$	+	$\hat{M}_+ -45^\circ\rangle = \frac{ 0^\circ\rangle}{\sqrt{2}} + \frac{ 90^\circ\rangle}{\sqrt{2}}$	$ 0^\circ\rangle$ or $ 90^\circ\rangle$	+	$\hat{M}_+ 0^\circ\rangle = 0^\circ\rangle$ or $\hat{M}_+ 90^\circ\rangle = - 90^\circ\rangle$	0 1
					\times	$\hat{M}_\times 0^\circ\rangle = \frac{1}{\sqrt{2}} 45^\circ\rangle - \frac{1}{\sqrt{2}} -45^\circ\rangle$ or $\hat{M}_\times 90^\circ\rangle = \frac{1}{\sqrt{2}} 45^\circ\rangle + \frac{1}{\sqrt{2}} -45^\circ\rangle$	0 or 1 0 or 1
		\times	$\hat{M}_\times -45^\circ\rangle = - -45^\circ\rangle$	$ - 45^\circ\rangle$	+	$\hat{M}_+ -45^\circ\rangle = \frac{1}{\sqrt{2}} 0^\circ\rangle + \frac{1}{\sqrt{2}} 90^\circ\rangle$	0 or 1
					\times	$\hat{M}_\times -45^\circ\rangle = - -45^\circ\rangle$	0

Рис. 12

измерений

Bob

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
Basis	+	x	x	x	+	+	+	x	+	x	x	+	+	x	+	+	+	x
Bit	1	0	1	1	1	0	0	1	1	1	0	1	0	1	0	0	0	1

Рис. 14

3. Алиса и Боб сравнивают свои базисы (я выбрала +, я выбрал -)

Alice

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
Basis	x	x	+	x	+	+	+	x	x	+	x	x	x	+	+	x	+	x
Bit	1	0	0	1	1	0	0	1	1	1	0	1	0	0	0	1	0	1

Bob

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
Basis	+	x	x	x	+	+	+	x	+	x	x	+	+	x	+	+	+	x
Bit	1	0	1	1	1	0	0	1	1	1	0	1	0	1	0	0	0	1

Рис. 15

4. Итоговый ключ, подобранный из совпавших битов, выглядит как:

0110010001

5. Алиса шифрует две буквы с помощью сгенерированного кода. Используются буквы *Q* и *M* английского алфавита:

Letter	Q					M				
Data Bit	1	0	0	0	0	0	1	1	0	0
Key Bit	0	1	1	0	0	1	0	0	0	1
Encrypted Bit	1	1	1	0	0	1	1	1	0	1

Рис. 16

6. Далее, Алиса отправляет зашифрованные буквы в + базисе. 0° обозначает бит 0, 90° обозначает бит 1. Боб принимает сигналы в + базисе, таким образом, что отраженный свет – бит 1, прошедший – 0.

Received Bit	1	1	1	0	0	1	1	1	0	1
--------------	---	---	---	---	---	---	---	---	---	---

Рис. 17

Теперь, используя полученный ранее код, Боб может расшифровать сообщение:

Received Bit	1	1	1	0	0	1	1	1	0	1
Key Bit	0	1	1	0	0	1	0	0	0	1
Data Bit	1	0	0	0	0	0	1	1	0	0
Letter	Q					M				

Рис. 18

Протокол шифрования в присутствии Евы

При наличии перехватчика (Евы) все происходит по схеме, описанной выше, но с тем отличием, что Ева перехватывает сигнал Алисы. Ее присутствие обнаруживается сравнением битов:

1. Алиса наугад выбирает базисы и биты, Боб и Ева также случайным образом выбирают базисы

Alice

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
Basis	X	X	+	X	+	+	+	X	X	+	X	X	X	+	+	X	+	X
Bit	1	0	0	1	1	0	0	1	1	1	0	1	0	0	0	1	0	1

Bob

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
Basis	+	X	X	X	+	+	+	X	+	X	X	+	+	X	+	+	+	X
Bit																		

Eve

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
Basis	X	X	+	+	X	+	+	+	X	X	X	X	+	X	+	X	+	+

Рис. 19

2. Алиса отправляет биты информации в выбранном базисе, Боб принимает и записывает. Однако, в этой ситуации между ними находится Алиса, которая выбирает наугад базисы (+ или X). Если базис Евы совпадет с Алисой, Бобу будет передан корректный бит. Если нет – случайный (0 или 1):

Eve

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
Basis	x	x	+	+	x	+	+	+	x	x	x	x	+	x	+	x	+	+
Bit	1	0	0	0	1	0	0	1	1	0	0	1	1	1	0	1	0	1

Bob

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
Basis	+	x	x	x	+	+	+	x	+	x	x	+	+	x	+	+	+	x
Bit	1	0	1	1	0	0	0	0	1	0	0	0	1	1	0	0	0	0

Рис. 20

В следующих таблицах мы видим выделенные зеленым “случайные” биты при передаче сигнала, сначала между Алисой и Евой и далее между Евой и Бобом

Eve

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
Basis	x	x	+	+	x	+	+	+	x	x	x	x	+	x	+	x	+	+
Bit	1	0	0	0	1	0	0	1	1	0	0	1	1	1	0	1	0	1

Bob

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
Basis	+	x	x	x	+	+	+	x	+	x	x	+	+	x	+	+	+	x
Bit	1	0	1	1	0	0	0	0	1	0	0	0	1	1	0	0	0	0

Рис. 21

Теперь Алиса и Боб сравнивают результаты измерений, сообщив друг-другу использованные базисы:

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

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

Рис. 22

Финальное равнение количества правильных битов, для совпавших базисов:

Alice:	0	1	1	0	0	1	0	0	0	1
Bob:	0	1	0	0	0	0	0	0	0	0

Рис. 23

Итак, мы видим, что 3 из 10 переданных битов переданы с ошибкой. Это дает нам $> 25\%$ ошибки, что указывает на присутствие в системе перехватчика – Евы.

Экспериментальная установка

Установка состоит из 3 основных элементов: Алиса, Боб и Ева. Каждый элемент требует аккуратной юстировки и бережного отношения. Ниже описаны элементы экспериментальной установки, с которыми придется столкнуться в процессе юстировки и проведения лабораторных измерений.

1. Полуволновая пластинка

В работе используются четыре полуволновые пластинки с вращающейся оправой. Две с маркировкой “ 0° 45° ” и две с маркировкой “ -45° 0° 45° 90° ”



Рис. 24

2. Блок управления источником излучения

Блок управления лазером поддерживает два режима, переключающиеся с помощью красной кнопки на верхней поверхности блока: режим постоянного излучения и импульсный. Режимы с импульсного в постоянный переключаются зажатием кнопки на 2 секунды. Последующее быстрое однократное нажатие вернет лазер обратно в импульсный режим.



Рис. 25

3. Детекторы сигнала

Блок детекторов снабжен двумя выходами на отдельные сенсоры ("0" и "1"). Зеленая кнопка наверху переключает режимы "настройки" и "измерений". В режиме **настройки** светодиод на торце блока горит **желтым** цветом. При падении на оба сенсора излучения одинаковой интенсивности, оба светодиода на верхней плоскости сенсоров горят синим цветом одновременно. В режиме **измерений**, при горящем на торце **зеленом** светодиоде, когда на оба сенсора направлено излучение одинаковой интенсивности, загорается синим только один из светодиодов, расположенных над сенсорами, случайным образом. Это эмуляция события, при котором единичный фотон с 50% вероятностью либо отражается, либо проходит насквозь светоделительного куба.



Рис. 26

4. Светоделительные кубы

Юстировка

Ознакомьтесь с экспериментальной установкой: 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.

1. До начала выполнения работы, необходимо отъюстировать лазер и полуволновую пластинку. **Выполняется по указанию преподавателя или инженера**
2. Юстировка Алисы и Боба
 - (a) Алиса и Боб должны быть расположены параллельно друг-другу так, чтобы оставить свободное место для введения Евы в эксперимент. Это расстояние должно быть не менее 60 см
 - (b) Установите Алису (лазер и полуволновая пластинка) на плите. Пластинка расположена в центре плиты, направленная поверхностью с метками (0, 45, -45, 90) к лазеру. Лазер должен находиться в режиме постоянного излучения (зажмите красную кнопку на 2 секунды).
 - (c) На другой плите (Боб) полуволновая пластинка с маркировками 0 и 45 расположена с краю, маркировками в сторону Алисы.
 - (d) Расположите светоделительный куб за пластинкой. Установите сенсоры так, чтобы отраженный и прошедший лучи попадали точно в отверстия приемников. Расстояния между кубом и сенсорами должно быть примерно одинаковым в соответствии с рисунком:

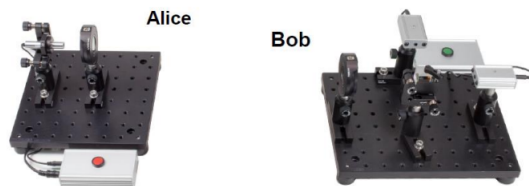


Рис. 27. Алиса и Боб

3. Ева анализирует сигнал Алисы, и передает его Бобу, поэтому конструктивно это оптические сетапы Боба и Алисы, собранные последовательно на одной плите.



Рис. 28. Ева

Точная настройка перед началом измерений

1. Зажмите красную кнопку на 3-4 секунды, чтобы ввести лазер в режим юстировки. Добиться попадания излучения на каждый из детекторов. При необходимости можно скорректировать положение детекторов. **Другие элементы установки рекомендуется не трогать.**
2. Установите сенсоры в режим настройки (горит желтый светодиод на торце блока)
3. Установите обе Пластинки $\lambda/2$ на "0" и нажмите красную кнопку.
4. Должен загореться синим тот сенсор, на который попадает излучение. Если это не произошло, проверьте что: сенсор перпендикулярен лучу, луч попадает точно в отверстие сенсора.
5. Установите полуволновую пластинку Алисы на "90" градусов. Теперь должен сработать сенсор, установленный по ходу луча отраженного от светоделительного куба. Всего до выполнения эксперимента необходимо выполнить 8 тестов, в соответствие с таблицей 1.

Таблица 1: Калибровка схемы Алиса-Боб: 100% – детектор горит синим. 50% и 50% – горят оба детектора, 0% – детектор не горит.

Алиса			Боб			
Базис	Бит	Угол	Базис	Угол	"0"	"1"
+	0	0°	+	0°	100%	0%
+	1	90°	+	0°	0%	100%
x	1	45°	+	0°	50%	50%
x	0	−45°	+	0°	50%	50%
+	0	0°	x	45°	50%	50%
+	1	90°	x	45°	50%	50%
x	1	45°	x	45°	100%	0%
x	0	−45°	x	45°	0%	100%

Важно!!! Выполнив все тесты, установите электронику сенсора в режим **измерений** (зеленый светодиод). Все тесты должны пройти в соответствие с таблицей приведенной выше, в противном случае эксперимент даст некорректные результаты.

Порядок выполнения работы

Создания ключа длиной минимум 20 бит

1. Сгенерируйте случайным образом набор базисов и битов у Алисы и набор базисов у Боба независимо друг от друга. Это можно сделать заранее. Протокол измерений должен содержать 52 бита.
2. Расположите модули Алиса и Боб, друг напротив друга, на расстоянии, достаточном для последующего введения между ними Евы, выполнив инструкции раздела “точная настройка”.
3. Когда точная настройка выполнена переведите блок детекторов в режим "измерений" (зеленый индикатор на торце). Алиса передает сигналы, Боб записывает полученные биты (отраженный сигнал – 1, пропущенный насквозь – 0). Так как требует создать итоговый ключ 20 битов длины, рекомендуется использовать тестовую последовательность как минимум в 52 бита. Если Алиса выбирает базис $+$, тогда 0° это 0, 90° это 1. Если Алиса выбирает базис X , тогда -45° это 1, 45° это 0.
4. Алиса и Боб сообщают друг другу, какие базисы были использованы. Измерения, в которых базисы не совпали, удаляются. Оставшиеся измерения образуют 20-битный код шифрования. В случае, если по итогам отбраковки совпавших битов не хватило для кода, проводятся дополнительные измерения.

Кодировка 4-х буквенного слова

1. Зашифруйте послание Алисы (4 буквы), используя ключ, полученный ранее. (Полный список кодировок для букв английского алфавита см. в “**Примечании**”)

2. Передайте зашифрованное сообщение Бобу. Передача информации должна быть выполнена в одном базисе, Алиса посылает биты информации в соответствие с: 0 это 0° , 1 это 90° . Если это базис X , то -45° это 1, а $-45^\circ - 0$
3. Расшифруйте полученную Бобом последовательность, используя ключ шифрования.

Введение в установку Евы и обнаружение перехватчика Алисой и Бобом

1. Между Алисой и Бобом установите плату с Евой, и оба блока сенсоров установите в режим **“настройки”**. Для передатчика и приемника Алисы и Евы проверьте выполнение 8 тестов передачи данных, в соответствие с таблицей на рисунке 8, приведенной выше. То же самое сделайте для Евы и Боба. Затем верните сенсоры в режим **“измерений”**.
2. Подготовьте таблицу измерений для Евы, в которой учтен случайный выбор базиса для каждого измерения. Также случайный выбор базисов должны выполнить Алиса и Боб, равно как случайным должен быть выбор битов Алисой. Заранее подготовленная таблица расписанная для всех участников нужна, так как при выполнении работы все находятся в одном месте, рядом с установкой и не могут выполнять измерения и выставлять базисы тайно друг от друга.
3. Отправьте первый бит информации от Алисы в соответствие с таблицей. Ева выбирает свой первый базис, также по таблице, записывает бит, и передает Бобу копию того, что было получено. Боб также производит запись, и этот шаблон повторяется для всех 52-х измерений.
4. Алиса и Боб обмениваются использованными базисами. Измерения с не совпавшими базисами удаляются. Оставшаяся последовательность битов проверяется на наличие перехватчика с помощью подсчета процента битов, переданных с ошибкой (см. **“Протокол шифрования в присутствии Евы”**).

Контрольные вопросы

1. В чем заключается метод одноразового ключа?
2. Каковы правила данного метода шифрования?
3. Чем однобазисная система отличается от двух базисной?
4. Для чего в установке используется полуволновая пластинка?
5. Как производится выполнение протокола шифрования?
6. Как можно обнаружить перехватчика сообщения (Еву)?
7. Как выбираются Алисой базис и бит при создании ключа шифрования?
8. Каковы правила бинарного сложения?

Приложение

Таблица 2: Бинарное представление букв английского алфавита

A	0	0	0	0	0
B	0	0	0	0	1
C	0	0	0	1	0
D	0	0	0	1	1
E	0	0	1	0	0
F	0	0	1	0	1
G	0	0	1	1	0
H	0	0	1	1	1
I	0	1	0	0	0
J	0	1	0	0	1
K	0	1	0	1	0
L	0	1	0	1	1
M	0	1	1	0	0
N	0	1	1	0	1
O	0	1	1	1	0
P	0	1	1	1	1
Q	1	0	0	0	0
R	1	0	0	0	1
S	1	0	0	1	0
T	1	0	0	1	1
U	1	0	1	0	0
V	1	0	1	0	1
W	1	0	1	1	0
X	1	0	1	1	1
Y	1	1	0	0	0
Z	1	1	0	0	1

Правила бинарного сложения

$$0 + 0 = 0$$

$$1 + 0 = 1$$

$$0 + 1 = 1$$

$$1 + 1 = 0$$