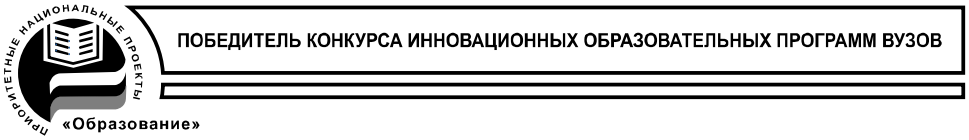
МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНОЕ АГЕНТСТВО ПО ОБРАЗОВАНИЮ

САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ, МЕХАНИКИ И ОПТИКИ



Ю.Т.Мазуренко, С.А.Чивилихин, А.И.Трифанов, В.В.Орлов, В.И.Егоров

КВАНТОВАЯ ИНФОРМАТИКА
ЛАБОРАТОРНЫЙ ПРАКТИКУМ

Санкт-Петербург

2009

Мазуренко Ю.Т., Чивилихин С.А., Трифанов А.И., Орлов В.В., Егоров В.И. КВАНТОВАЯ ИНФОРМАТИКА. ЛАБОРАТОРНЫЙ ПРАКТИКУМ. Учебное пособие, – СПб: СПбГУИТМО, 2009. – 58с.

В пособии представлены методические материалы к экспериментальному практикуму по дисциплине «Квантовая информатика». Даны описания лабораторных работ с кратким изложением теоретического материала, необходимого для подготовки к лабораторным работам.

Учебное пособие предназначено для студентов СПбГУ ИТМО специальностей NN 2006006802, 010500. Рекомендовано к печати Ученым Советом факультета фотоники и оптоинформатики, протокол N5 от 18 февраля 2009 г

В 2007 году СПбГУ ИТМО стал победителем конкурса инновационных образовательных программ вузов России на 2007–2008 годы. Реализация инновационной образовательной программы «Инновационная система подготовки специалистов нового поколения в области информационных и оптических технологий» позволит выйти на качественно новый уровень подготовки выпускников и удовлетворить возрастающий спрос на специалистов в информационной, оптической и других высокотехнологичных отраслях экономики.

Содержание

Предисловие

Пособие содержит описание виртуальных и реальных лабораторных работ, посвященных различным аспектам квантовой информатики. Начиная с элементарных квантовых логических алгоритмов и квантовых схем, пособие знакомит студентов со все более сложными и практически важными вопросами. Алгоритм Гровера быстрого поиска в базах данных и реализация квантового оптического вентиля CNOT требуют для своего понимания углубленных знаний в области квантовой механики и квантовой теории информации. Две заключительные работы пособия позволяют студентам познакомиться с практической реализацией принципов квантовой криптографии. Эти работы проводятся на квантово-криптографической учебно-исследовательской установке на основе несимметричного волоконно-оптического интерферометра Майкельсона.

Лабораторная работа №1

Элементарные квантовые алгоритмы

Цель работы: Изучение основных однокубитовых квантовых логических алгоритмов.

***Объект исследования*:** Виртуальная лабораторная работа.

Задачи, решаемые в работе:

1. Изучение работы квантовых логических алгоритмов X, Z и H.
2. Прогнозирование результатов виртуального эксперимента и сравнение результатов теоретических и экспериментальных расчетов.
3. Распознавание неизвестного однокубитового квантового логического алгоритма.

СВЕДЕНИЯ ИЗ ТЕОРИИ

Логический элемент NOT.

Обозначим квантовый логический элемент NOT через X. Определим сначала действие этого оператора на базисные вектора. Потребуем, чтобы он переводил $|0\rangle$ в $|1\rangle$, а $|1\rangle$ в $|0\rangle$:

$$X|0\rangle = |1\rangle,$$

$$X|1\rangle = |0\rangle.$$

Тем самым квантовый оператор NOT становится естественным обобщением классического оператора NOT. Используя линейность оператора X, определим действие оператора на произвольный кубит:

$$X|\psi\rangle = X\left(\alpha|0\rangle + \beta|1\rangle\right) = \alpha X|0\rangle + \beta X|1\rangle.$$

Окончательно

$$X|\psi\rangle = \alpha|1\rangle + \beta|0\rangle = \beta|0\rangle + \alpha|1\rangle.$$

Таким образом, оператор X меняет местами коэффициенты при базисных векторах $|0\rangle$ и $|1\rangle$.

Матричные элементы X_{mn} оператора X:

$$\mathrm{X}_{00} = 0, \quad \mathrm{X}_{10} = 1,$$

$$X_{01} = 1, \quad X_{11} = 0.$$

Запишем матрицу X оператора X_{mn}:

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

Подействуем этой матрицей на вектор входного кубита. Тогда получаем вектор выходного кубита в виде

$$\begin{pmatrix} \tilde{\alpha} \\ \tilde{\beta} \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} \alpha \\ \beta \end{pmatrix} = \begin{pmatrix} \beta \\ \alpha \end{pmatrix}.$$

Полученная матрица X является унитарной. В самом деле

$$X^{+}X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}^{+} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = I.$$

Действие оператора X на кубит

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$$

для вещественных α и β легко интерпретировать геометрически. В вещественном случае используем тригонометрическое представление

$$\alpha = \cos\varphi, \quad \beta = \sin\varphi, \quad \tilde{\alpha} = \cos\tilde{\varphi}, \quad \tilde{\beta} = \sin\tilde{\varphi}.$$

Тогда,

$$\tilde{\varphi} = \frac{\pi}{2} - \varphi.$$

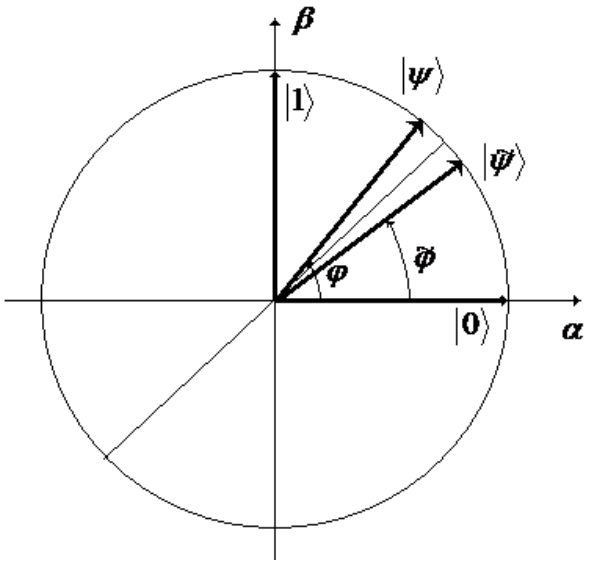


Рис.1.Геометрическое изображение преобразования NOT для случая вещественных коэффициентов α и β.

Таким образом, оператор X поворачивает единичный вектор, изображающий кубит на единичной окружности, отражая его от биссектрисы первого и третьего координатных углов – см. рис.1.

Логический элемент Z.

Определим сначала действие оператора **Z** на базисные вектора. Потребуем, чтобы он не изменял $|0\rangle$, а $|1\rangle$ переводил в $-|1\rangle$:

$$Z|0\rangle = |0\rangle,$$

$$Z|1\rangle = -|1\rangle.$$

Используя линейность оператора Z, определим действие оператора на произвольный кубит:

$$Z|\psi\rangle = Z\left(\alpha|0\rangle + \beta|1\rangle\right) = \alpha Z|0\rangle + \beta Z|1\rangle.$$

Тогда,

$$Z|\psi\rangle = \alpha|0\rangle - \beta|1\rangle.$$

Таким образом, оператор Z не изменяет коэффициент при базисном векторе $|0\rangle$ и меняет знак коэффициента при базисном векторе $|1\rangle$. Матричные элементы Z_{mn} оператора Z:

$$\mathrm{Z}_{00} = 1, \quad \mathrm{Z}_{10} = 0,$$

$$\mathrm{Z}_{01} = 0, \quad \mathrm{Z}_{11} = -1.$$

Запишем матрицу Z оператора Z_{mn}:

$$\mathrm{Z} = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

Подействуем этой матрицей на вектор входного кубита. Тогда получаем вектор выходного кубита в виде

$$\begin{pmatrix} \tilde{\alpha} \\ \tilde{\beta} \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \begin{pmatrix} \alpha \\ \beta \end{pmatrix} = \begin{pmatrix} \alpha \\ -\beta \end{pmatrix}.$$

Полученная матрица Z является унитарной. В самом деле

$$\mathrm{Z}^{+}\mathrm{Z} = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}^{+} \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \mathrm{I}.$$

Действие оператора Z на кубит

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$$

для вещественных α и β легко интерпретировать геометрически. В вещественном случае используем тригонометрическое представление

$$\alpha = \cos\varphi, \quad \beta = \sin\varphi, \ \ \tilde{\alpha} = \cos\tilde{\varphi}, \quad \tilde{\beta} = \sin\tilde{\varphi}.$$

В самом деле,

$$\tilde{\varphi} = -\varphi.$$

Таким образом, оператор Z поворачивает единичный вектор, изображающий кубит на единичной окружности, отражая его от оси абсцисс – см. рис.2.

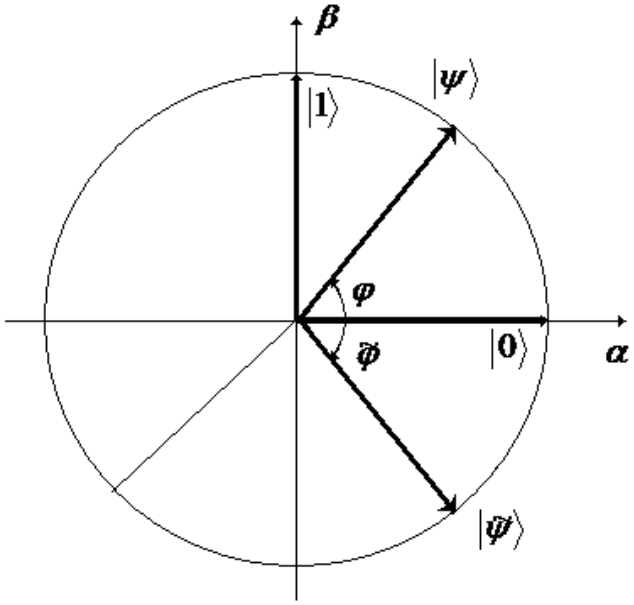


Рис.2.Геометрическое изображение преобразования Z для случая вещественных коэффициентов α и β.

Логический элемент Адамара H.

Элемент Адамара задается матрицей

$$\mathrm{H} = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}.$$

Подействуем этой матрицей на вектор входного кубита. Тогда получаем вектор выходного кубита в виде

$$\begin{pmatrix} \tilde{\alpha} \\ \tilde{\beta} \end{pmatrix} = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}\begin{pmatrix} \alpha \\ \beta \end{pmatrix} = \frac{1}{\sqrt{2}}\begin{pmatrix} \alpha+\beta \\ \alpha-\beta \end{pmatrix}.$$

Соответствующий оператор H действует на кубит по правилу

$$H|\psi\rangle = \frac{\alpha+\beta}{\sqrt{2}}|0\rangle + \frac{\alpha-\beta}{\sqrt{2}}|1\rangle .$$

Матрица H является унитарной. В самом деле

$$\mathrm{H}^{+}\mathrm{H} = \frac{1}{2}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix}^{+}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix} = \frac{1}{2}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix} = \frac{1}{2}\begin{pmatrix}2 & 0\\ 0 & 2\end{pmatrix} = \mathrm{I}.$$

Из унитарности матрицы оператора вытекает унитарность самого оператора.

ПОРЯДОК ВЫПОЛНЕНИЯ РАБОТЫ

1. Студент подает кубит на вход известного логического элемента и получает выходной кубит. Результаты работы схемы сравниваются со свойствами алгоритма, известными из теории.
2. Используя матричное представление элемента, студент прогнозирует результаты виртуального эксперимента и сравнивает результаты теоретических и экспериментальных расчетов.
3. Студент распознает неизвестный однокубитовый квантовый логический элемент X, Z или H см. рис.3.

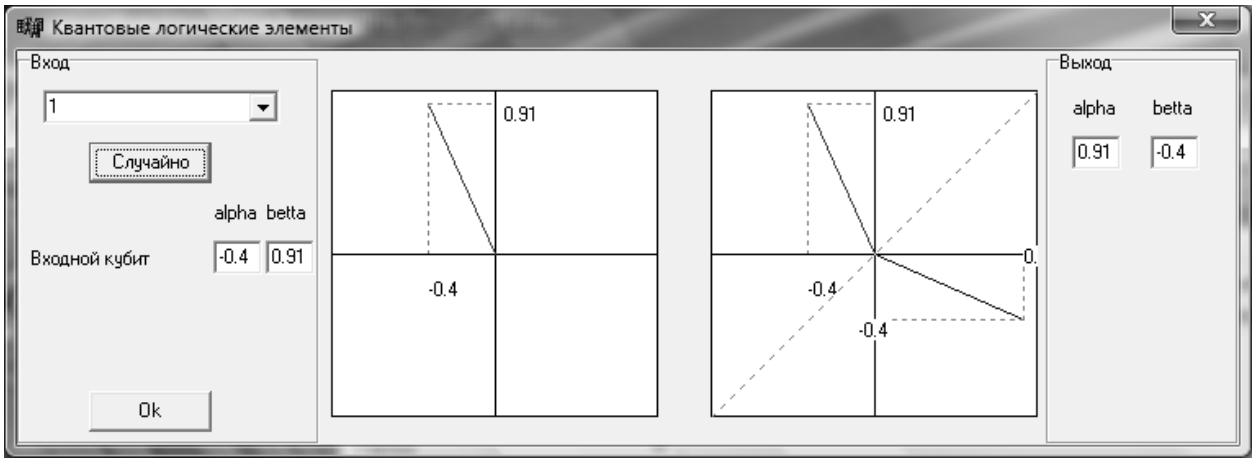


Рис.3. Исследование неизвестного квантового элемента

ЛИТЕРАТУРА

1. Нильсен М., Чанг И. Квантовые вычисления и квантовая информация. М.: Мир. 2006 г. - 824 с.
2.Попов И.Ю. Квантовый компьютер и квантовые алгоритмы. – СПб: СПбГУ ИТМО, 2007г. - 88 с.

Лабораторная работа №2

Однокубитовые квантовые схемы

Цель работы: Изучение простейших однокубитовых квантовых логических схем.

***Объект исследования*:** Виртуальная лабораторная работа.

Задачи, решаемые в работе:
1. Изучение работы квантовых логических схем, составленных из элементов алгоритмов X, Z и H.
2. Прогнозирование результатов виртуального эксперимента и сравнение результатов теоретических и экспериментальных расчетов.

СВЕДЕНИЯ ИЗ ТЕОРИИ

Рассмотрим два последовательно включенных однокубитовых квантовых логических элемента. На вход первого элемента поступает кубит, описываемый волновым вектором $|\psi\rangle$. Действие первого элемента на кубит описывается оператором U_1. Результатом действия оператора U_1 на вектор $|\psi\rangle$ является волновой вектор $|\psi_1\rangle$ - см. рис.1.

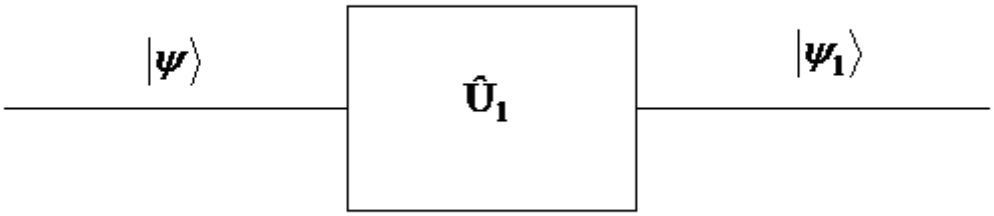


Рис.1. Действие квантового логического элемента U_1.

Рассмотрим теперь второй однокубитовый квантовый логический элемент U_2. На его вход поступает волновой вектор $|\psi_1\rangle$ - результат действия логического элемента U_1. На выходе логического элемента U_2 появляется волновой вектор $|\psi_2\rangle$ - см. рис.2.

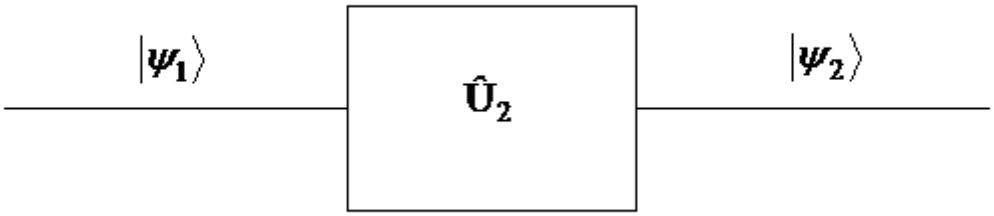


Рис.2. Действие квантового логического элемента U_2.

Последовательное действие операторов U_1 и U_2 представляется квантовой схемой, изображенной на рис.3.

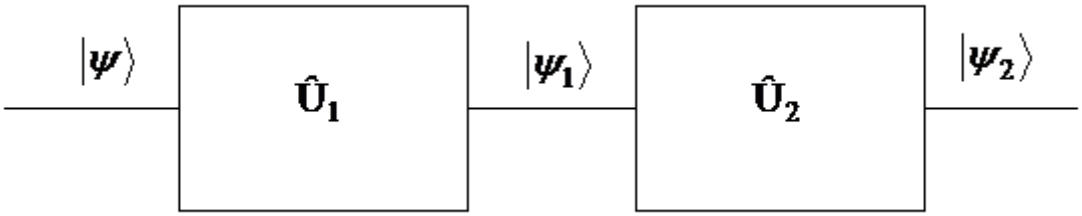


Рис.3. Последовательное действие квантового логического элемента U_1 и квантового логического элемента U_2.

Таким образом, преобразование начального вектора $|\psi\rangle$ в конечный вектор $|\psi_2\rangle$ за счет последовательного действия операторов U_1 и U_2 можно записать следующим образом

$$|\psi_2\rangle = U_2|\psi_1\rangle = U_2U_1|\psi\rangle.$$

В матричном представлении, квантовая схема, изображенная на рис.6 описывается матрицей U равной произведению матриц U_1 и U_2:

$$\mathrm{U} = \mathrm{U}_2\mathrm{U}_1.$$

Произведение унитарных матриц унитарно. Поэтому результат последовательного действия двух унитарных преобразований является унитарным преобразованием.

Описанный алгоритм конструирования однокубитовых квантовых логических схем обобщается на общий случай последовательно действия

n логических элементов. На рис.4 изображена цепочка из n последовательно включенных логических элементов $U_1,\dots U_n$.

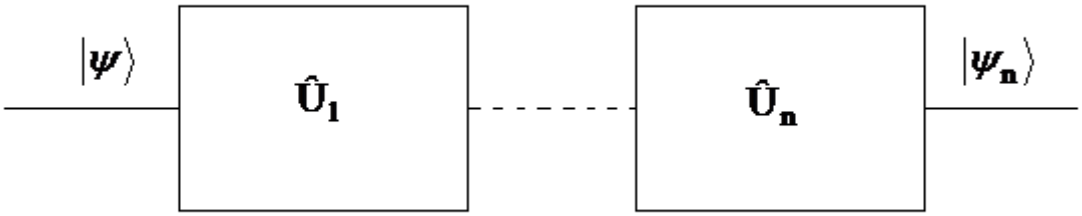


Рис.4. Последовательное действие квантовых логических элементов $U_1,\dots U_n$.

На вход цепочки поступает волновой вектор $|\psi\rangle$, на выходе появляется волновой вектор $|\psi_n\rangle$. Преобразование начального вектора $|\psi\rangle$ в конечный вектор $|\psi_n\rangle$ за счет последовательного действия операторов $U_1,\dots U_n$ можно записать следующим образом

$$|\psi_n\rangle = U_n|\psi_{n-1}\rangle = \dots = U_n U_{n-1}\dots U_1|\psi\rangle.$$

В матричном представлении, квантовая схема, изображенная на рис.7 описывается матрицей U равной произведению матриц $U_n U_{n-1}\dots U_1$:

$$\mathrm{U} = \mathrm{U_n U_{n-1}}\dots \mathrm{U_1}.$$

Произведение унитарных матриц унитарно. Поэтому результат последовательного действия n унитарных преобразований является унитарным преобразованием.

Однокубитовые квантовые схемы, построенные из одинаковых элементов.

Рассмотрим простейший случай последовательного действия одинаковых вещественных симметричных квантовых элементов. Матрицы, описывающие такие элементы, симметричны и имеют вещественные коэффициенты. Примером таких элементов являются логические элементы NOT (X), Z и элемент Адамара H.

$$\mathrm{X} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

$$\mathrm{Z} = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}.$$

Как и любые матрицы, описывающие квантовые логические элементы, предлагаемые матрицы унитарны, т.е.

$$U^{+}U = I.$$

Вещественные симметричные матрицы обладают дополнительным свойством

$$U^{+} = U.$$

Отсюда

$$UU = I.$$

Таким образом, последовательное действие двух одинаковых вещественных симметричных квантовых элементов эквивалентно единичному оператору. Следовательно, последовательное действие четного числа вещественных симметричных квантовых элементов, также эквивалентно единичному оператору:

$$\underbrace{U \quad U \quad \ldots \quad U}_{2n} = I.$$

Последовательное действие нечетного числа вещественных симметричных квантовых элементов U, эквивалентно одному элементу U:

$$\underbrace{U \quad U \quad \ldots \quad U}_{2n+1} = U.$$

ПОРЯДОК ВЫПОЛНЕНИЯ РАБОТЫ

Студент выбирает несколько квантовых элементов, подает на вход цепочки элементов кубит, получает выходной кубит и, используя матричное представление схемы, сравнивает результаты теоретических расчетов с полученными экспериментальными данными – см. рис.5.

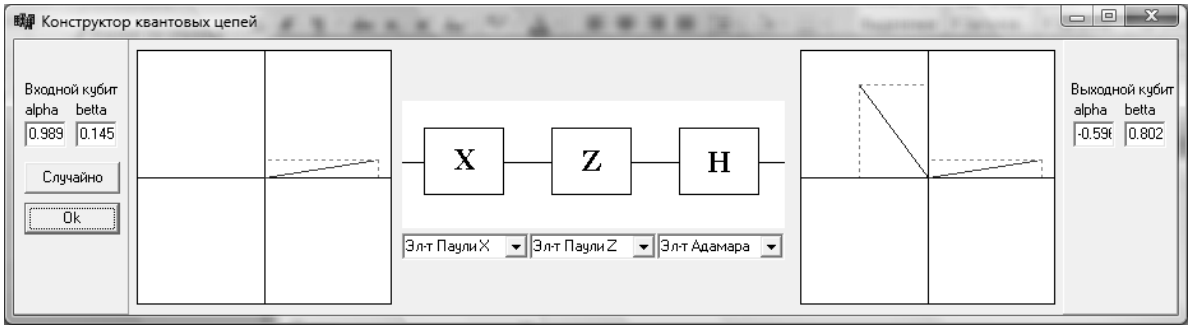


Рис.5. Исследование цепочки однокубитовых элементов

ЛИТЕРАТУРА

1. Нильсен М., Чанг И. Квантовые вычисления и квантовая информация. М.: Мир. 2006 г. - 824 с.
2.Попов И.Ю. Квантовый компьютер и квантовые алгоритмы. – СПб: СПбГУ ИТМО, 2007г. - 88 с.

Лабораторная работа №3

Двухкубитовые квантовые схемы

Цель работы: Изучение простейших двухкубитовых квантовых логических схем.

***Объект исследования*:** Виртуальная лабораторная работа.

Задачи, решаемые в работе:
1. Изучение работы квантовых логических схем, составленных из элементов алгоритмов CNOT, X, Z и H.
2. Прогнозирование результатов виртуального эксперимента и сравнение результатов теоретических и экспериментальных расчетов.

СВЕДЕНИЯ ИЗ ТЕОРИИ

Рассмотрим квантовую систему, состоящую из двух кубитов:

$$|\psi_1\rangle = \alpha_1|0_1\rangle + \beta_1|1_1\rangle,$$
$$|\psi_2\rangle = \alpha_2|0_2\rangle + \beta_2|1_2\rangle,$$

где $|0\rangle_1, |1\rangle_1, |0\rangle_2, |1\rangle_2$ - базисные состояния первого и второго кубита соответственно, α_1, β_1, α_2, β_2 - комплексные числа.

Отметим, что кубиты $|\psi_1\rangle$ и $|\psi_2\rangle$ (а также и соответствующие базисные вектора $|0\rangle_1, |1\rangle_1, |0\rangle_2, |1\rangle_2$) относятся к разным векторным пространствам – назовем их H_1 и H_2:

$$|\psi_1\rangle \in \mathrm{H}_1, \quad |\psi_2\rangle \in \mathrm{H}_2.$$

Построим векторное пространство, элементами которого являются пары векторов, первый из которых принадлежит пространству H_1, а второй – пространству H_2. Такое пространство называется тензорным произведением пространств H_1 и H_2. Оно обозначается $\mathrm{H}_1 \otimes \mathrm{H}_2$. Элементы его обозначим $|\psi\rangle = |\psi_1\rangle \otimes |\psi_2\rangle$. Базисные вектора этого пространства представляют собой тензорные произведения базисных векторов из пространств H_1 и H_2:

$$|00\rangle = |0_1\rangle \otimes |0_2\rangle, \quad |01\rangle = |0_1\rangle \otimes |1_2\rangle,$$

$$|10\rangle = |1_1\rangle \otimes |0_2\rangle,\ |11\rangle = |1_1\rangle \otimes |1_2\rangle.$$

Операторы, определенные в H_1 и H_2, действуют в тензорном произведении пространств $H_1 \otimes H_2$ покомпонентно:

$$(U_1 \otimes U_2)(|\psi_1\rangle \otimes |\psi_2\rangle) = (U_1|\psi_1\rangle) \otimes (U_2|\psi_2\rangle).$$

В базисах пространств H_1 и H_2, вектора $|\psi_1\rangle$ и $|\psi_2\rangle$ представляются в виде столбцов

$$|\psi_1\rangle = \begin{pmatrix} \alpha_1 \\ \beta_1 \end{pmatrix},\ |\psi_2\rangle = \begin{pmatrix} \alpha_2 \\ \beta_2 \end{pmatrix},$$

а операторы $U^{(1)}$ и $U^{(2)}$, действующие в пространствах H_1 и H_2 соответственно – в виде матриц

$$U^{(1)} = \begin{pmatrix} U_{00}^{(1)} & U_{01}^{(1)} \\ U_{10}^{(1)} & U_{11}^{(1)} \end{pmatrix},$$

$$U^{(2)} = \begin{pmatrix} U_{00}^{(2)} & U_{01}^{(2)} \\ U_{10}^{(2)} & U_{11}^{(2)} \end{pmatrix}.$$

Для того, чтобы представить волновые векторы и оператора тензорного произведения пространств $H_1 \otimes H_2$, введем понятие тензорного (Кронекерова) произведения матриц.

Пусть A – матрица $m \times n$, B – матрица $r \times s$. Произведение Кронекера матриц A и B определяется как матрица $(m \cdot r) \times (n \cdot s)$

$$A \otimes B = \begin{pmatrix} A_{11}B & A_{12}B & \ldots & A_{1n}B \\ A_{21}B & A_{22}B & \ldots & A_{2n}B \\ \ldots & \ldots & \ldots & \ldots \\ A_{m1}B & A_{m1}B & \ldots & A_{mn}B \end{pmatrix}.$$

Представим базисные вектора пространств H_1 и H_2 в виде

$$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix},\ |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}.$$

$$|00\rangle = |0_1\rangle \otimes |0_2\rangle = \begin{pmatrix} 1 \cdot \begin{pmatrix} 1 \\ 0 \end{pmatrix} \\ 0 \cdot \begin{pmatrix} 1 \\ 0 \end{pmatrix} \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix},$$

$$|01\rangle = |0_1\rangle \otimes |1_2\rangle = \begin{pmatrix} 1\cdot\begin{pmatrix}0\\1\end{pmatrix} \\ 0\cdot\begin{pmatrix}0\\1\end{pmatrix} \end{pmatrix} = \begin{pmatrix}0\\1\\0\\0\end{pmatrix},$$

$$|10\rangle = |1_1\rangle \otimes |0_2\rangle = \begin{pmatrix} 0\cdot\begin{pmatrix}1\\0\end{pmatrix} \\ 1\cdot\begin{pmatrix}1\\0\end{pmatrix} \end{pmatrix} = \begin{pmatrix}0\\0\\1\\0\end{pmatrix},$$

$$|11\rangle = |1_1\rangle \otimes |1_2\rangle = \begin{pmatrix} 0\cdot\begin{pmatrix}0\\1\end{pmatrix} \\ 1\cdot\begin{pmatrix}0\\1\end{pmatrix} \end{pmatrix} = \begin{pmatrix}0\\0\\0\\1\end{pmatrix}.$$

Запишем теперь двухкубитовое состояние $|\psi\rangle = |\psi_1\rangle \otimes |\psi_2\rangle$

$$|\psi\rangle = \begin{pmatrix}\alpha_1\\\beta_1\end{pmatrix} \otimes \begin{pmatrix}\alpha_2\\\beta_2\end{pmatrix} = \begin{pmatrix} \alpha_1\begin{pmatrix}\alpha_2\\\beta_2\end{pmatrix} \\ \beta_1\begin{pmatrix}\alpha_2\\\beta_2\end{pmatrix} \end{pmatrix} = \begin{pmatrix}\alpha_1\alpha_2\\\alpha_1\beta_2\\\beta_1\alpha_2\\\beta_1\beta_2\end{pmatrix}.$$

Наконец, тензорное (Кронекерово) произведение матричных представлений операторов $U^{(1)}$ и $U^{(2)}$ имеет вид

$$\mathrm{U} = \mathrm{U}^{(1)} \otimes \mathrm{U}^{(2)} = \begin{pmatrix} \mathrm{U}_{00}^{(1)}\begin{pmatrix}\mathrm{U}_{00}^{(2)} & \mathrm{U}_{01}^{(2)}\\ \mathrm{U}_{10}^{(2)} & \mathrm{U}_{11}^{(2)}\end{pmatrix} & \mathrm{U}_{01}^{(1)}\begin{pmatrix}\mathrm{U}_{00}^{(2)} & \mathrm{U}_{01}^{(2)}\\ \mathrm{U}_{10}^{(2)} & \mathrm{U}_{11}^{(2)}\end{pmatrix} \\ \mathrm{U}_{10}^{(1)}\begin{pmatrix}\mathrm{U}_{00}^{(2)} & \mathrm{U}_{01}^{(2)}\\ \mathrm{U}_{10}^{(2)} & \mathrm{U}_{11}^{(2)}\end{pmatrix} & \mathrm{U}_{11}^{(1)}\begin{pmatrix}\mathrm{U}_{00}^{(2)} & \mathrm{U}_{01}^{(2)}\\ \mathrm{U}_{10}^{(2)} & \mathrm{U}_{11}^{(2)}\end{pmatrix} \end{pmatrix},$$

или

$$\mathrm{U} = \mathrm{U}^{(1)} \otimes \mathrm{U}^{(2)} = \begin{pmatrix} \mathrm{U}_{00}^{(1)}\mathrm{U}_{00}^{(2)} & \mathrm{U}_{00}^{(1)}\mathrm{U}_{01}^{(2)} & \mathrm{U}_{01}^{(1)}\mathrm{U}_{00}^{(2)} & \mathrm{U}_{01}^{(1)}\mathrm{U}_{01}^{(2)} \\ \mathrm{U}_{00}^{(1)}\mathrm{U}_{10}^{(2)} & \mathrm{U}_{00}^{(1)}\mathrm{U}_{11}^{(2)} & \mathrm{U}_{01}^{(1)}\mathrm{U}_{10}^{(2)} & \mathrm{U}_{01}^{(1)}\mathrm{U}_{11}^{(2)} \\ \mathrm{U}_{10}^{(1)}\mathrm{U}_{00}^{(2)} & \mathrm{U}_{10}^{(1)}\mathrm{U}_{01}^{(2)} & \mathrm{U}_{11}^{(1)}\mathrm{U}_{00}^{(2)} & \mathrm{U}_{11}^{(1)}\mathrm{U}_{01}^{(2)} \\ \mathrm{U}_{10}^{(1)}\mathrm{U}_{10}^{(2)} & \mathrm{U}_{10}^{(1)}\mathrm{U}_{11}^{(2)} & \mathrm{U}_{11}^{(1)}\mathrm{U}_{10}^{(2)} & \mathrm{U}_{11}^{(1)}\mathrm{U}_{11}^{(2)} \end{pmatrix}.$$

ПОРЯДОК ВЫПОЛНЕНИЯ РАБОТЫ

Студент собирает квантовую схему используя квантовые логические элементы CNOT, X, H и Z, подает на вход цепочки элементов двухкубитовое состояние кубит, получает выходное двухкубитовое состоянииe и, используя матричное представление схемы, сравнивает результаты теоретических расчетов с полученными экспериментальными данными – см. рис.1.

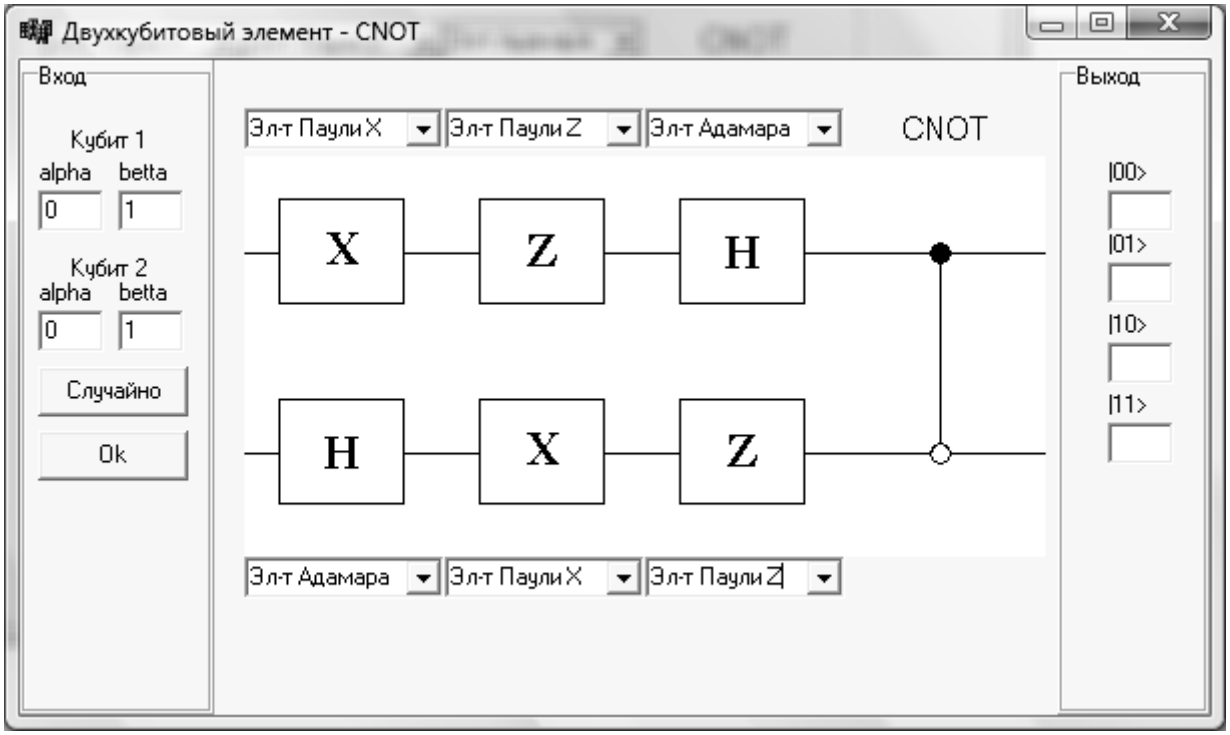


Рис.1. Исследование двухкубитовой квантовой схемы

ЛИТЕРАТУРА

1. Нильсен М., Чанг И. Квантовые вычисления и квантовая информация. М.: Мир. 2006 г. - 824 с.
2.Попов И.Ю. Квантовый компьютер и квантовые алгоритмы. – СПб: СПбГУ ИТМО, 2007г. - 88 с.

Лабораторная работа №4

Квантовый алгоритм Гровера

Цель работы: Изучение принципов работы алгоритма Гровера.

***Объект исследования*:** Виртуальная лабораторная работа.

Задачи, решаемые в работе:
1. Изучение работы квантовой логической схемы, реализующей алгоритм Гровера.
2. Выбор свободных параметров алгоритма для получения требуемых результатов работы схемы.

СВЕДЕНИЯ ИЗ ТЕОРИИ

Задача состоит в следующем. Имеется база данных, в которой один элемент отмечен. Надо его найти во всем наборе. Классический алгоритм фактически сводится к перебору. Это требует в среднем $n/2$ операций. Квантовый компьютер позволяет сделать это быстрее (Grover, 1996). Сформулируем задачу точнее. У нас есть $n = 2^m$ элементов, пронумерованных числами в двоичной системе. Следовательно, есть набор m-значных двоичных чисел s_i. Что нам делать, если мы хотим выбрать некоторый элемент s_v, выделяемый условием $C(s_v) = 1,\ C(s_i) = 0$ при $i \neq v$? Считаем, что проверка условия выполняется за одну операцию без классических измерений.

Алгоритм Гровера состоит из следующих шагов:

(1) На нулевое состояние действуем оператором Уолша-Адамара:

$$\mathsf{W}|0,0,...,0\rangle = \frac{1}{\sqrt{n}}\sum_{i=0}^{n-1}|i\rangle;$$

(2) Этот пункт будет циклически повторяться определенное количество раз

(a) Контролируемое изменение фазы с контролем в виде C (нашего условия). В результате все состояния, кроме s_v, останутся без изменений, а у s_v фаза изменится на π, то есть поменяется знак;

(b) Применим к полученному состоянию «оператор диффузии» (инверсии относительно среднего) $\hat{D} = -\hat{I} + 2\hat{P}$, где $P_{ij} = n^{-1}$;

(3) Измерение.

Проследим за этой процедурой шаг за шагом на конкретном примере с $n = 8$.

Выберем для примера некоторую конкретную матрицу проверки условия:

$$C = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & -1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}.$$

Оператор $\hat{P}$ имеет матрицу

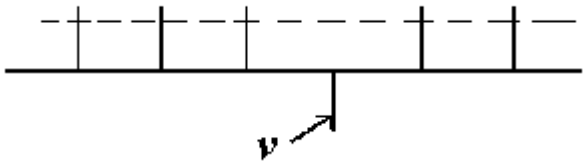
$$P = \frac{1}{8}\begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{pmatrix}.$$

Заметим, что оператор $\hat{P}$ самосопряжён (матрица симметрична и вещественна) и $\hat{P}^2 = 8^{-2} \cdot 8^2 P = P$. Следовательно, $\hat{P}$ - ортогональный проектор.

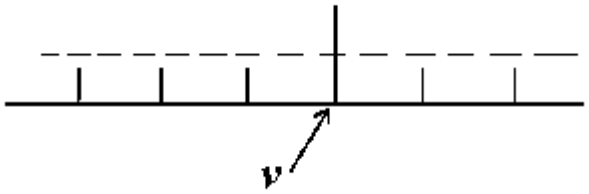
Рассмотрим оператор диффузии, а именно, $\hat{D}^2 = \left(-\hat{I} + 2\hat{P}\right)\left(-\hat{I} + 2\hat{P}\right) = 4\hat{P} - 2\hat{P} - 2\hat{P} + \hat{I} = \hat{I}$. Учитывая, что $\hat{D}$ самосопряжён, получаем, что $\hat{D}$ - унитарный оператор. Это означает, что данный оператор, вообще говоря, может быть реализован.

Пусть есть некоторое состояние $|z\rangle = \sum_{|x\rangle} \alpha_x |x\rangle$. Оператор $\hat{P}$ превратит его в вектор с компонентами, равными среднему значению $A = \frac{1}{n}\sum_{|x\rangle} \alpha_x$. Что же тогда делает оператор $\hat{D}$? $\hat{D} = -\hat{I} + 2\hat{P} = \hat{P} + \left(\hat{P} - \hat{I}\right)$. Так как $\hat{P}|z\rangle$ - вектор, состоящий из средних значений, то $\hat{D}$ есть инверсия относительно среднего.

После первого изменения фазы и перед применением инверсии относительно среднего имеем (среднее значение обозначено пунктирной линией):



После применения оператора диффузии $\hat{D}$ (операции инверсии), столбцы, смотрящие вверх, будут ниже среднего уровня ровно настолько, насколько были выше до этого:



Если попробуем провести измерения, то нужное нам значение v получим с наибольшей вероятностью, но вероятность остальных значений всё ещё велика. Чтобы «нарастить» вероятность v, надо произвести операции изменения фазы ещё несколько раз.

Рассмотрим плоскость, порождённую двумя векторами, один из которых – начальный вектор, у которого все координаты равны, а другой – элемент базиса, соответствующий ответу (у него одна координата равна 1, а все остальные – 0). Заметим, что эти два вектора не ортогональны, угол между ними равен $\pi/2 - \theta/2$, где $\theta > 0$ задано формулой $\sin(\theta/2) = n^{-1/2}$. Операция изменения фазы является ортогональным отражением относительно прямой, проходящей через начальный вектор с равными координатами. Композиция двух ортогональных отражений есть поворот. Для вычисления угла поворота применим эти две операции к вектору ответа $|z\rangle$. После первой операции получим $-|z\rangle$, после второй $-|z\rangle - 2n^{-1/2}|y\rangle$, где $|y\rangle$ обозначает начальный вектор. Косинус угла между этими двумя векторами равен их скалярному произведению, то есть

$\cos\theta = 1 - 2n^{-1}$. Искомый угол равен θ. Отсюда имеем, что достаточно около $\pi/2\theta - 1/2$ шагов (здесь надо помнить, что начальный угол равен $\pi/2 - \theta/2$), чтобы угол стал равен $\pi/2$ с ошибкой не больше $\theta/2$. Точнее, следует округлить указанное число шагов до ближайшего целого. Теперь при измерении вероятность получить правильный ответ равна квадрату модуля скалярного произведения соответствующих векторов. В силу монотонности, максимальная вероятность ошибки достигается при угле $\theta/2$ и составляет $1 - \cos^2(\theta/2) = \sin^2(\theta/2) = 1/n$. Итак, в любом случае, вероятность получения неправильного ответа не превосходит $1/n$, притом эта оценка точна.

Заметим, что если провести большее число операций, то вероятность правильного ответа сначала будет уменьшаться, потом увеличиваться и далее таким же образом колебаться. Это означает, что в алгоритме надо правильно выбрать момент остановки.

Алгоритм Гровера даёт выигрыш в числе операций при больших значениях *n*, ибо он требует $O\left(\sqrt{n}\right)$ шагов, в то время, как классический алгоритм требует $O(n)$. Правда есть и проблемы. В квантовом алгоритме всегда есть ненулевая вероятность получить неверный результат. Впрочем, его легко проверить и, если требуется, запустить алгоритм ещё раз.

ПОРЯДОК ВЫПОЛНЕНИЯ РАБОТЫ

В приложенном файле QGA.cmd смоделирован квантовый алгоритм Гровера. Задачу можно описать следующим образом: имеется база данных, состоящая из тридцати двух элементов (которые кодируются пятью кубитами), один из которых помечен. Вашей задачей является определить номер помеченного элемента. В вашем распоряжении имеется возможность указать сколько раз необходимо применить операторы контролируемой фазы и диффузии (второй шаг алгоритма Гровера), а также увидеть теоретические результаты измерений (распределение амплитуд вероятностей по элементам) и результаты того, что может получиться на практике (гистограмма результатов измерений ансамбля одинаковых состояний базы). Число кубитов системы (размер базы) менять не рекомендуется – при большем числе элементов (а число их растет как 2^n) наглядность схемы сильно ухудшится. В подразделе **“Algorithm realization”** описываются основные операторы, используемые в программе.

Меняя число итераций второго шага алгоритма, изучите, как меняется распределение амплитуд вероятностей получить в результате

поиска тот или иной элемент базы данных (в нашем случае чисел). Также определите количество повторений, при котором один из элементов базы появиться с вероятностью большей 95%. Как зависит это число от количества элементов в базе? Убедитесь, что при дальнейшем увеличении числа итераций эта амплитуда вероятности начнет уменьшаться.

На гистограмме (рис.2) приводится результат 16-ти одинаковых измерений состояния базы. Высота столбика показывает, сколько раз в результате данного числа измерений получили заданное число. Это реальная ситуация того, что может получиться в эксперименте, когда теория предсказывает распределение, приведенное на рисунке 1. Меняя количество измерений, посмотрите, как гистограмма результатов будет приближаться к теоретическому распределению.

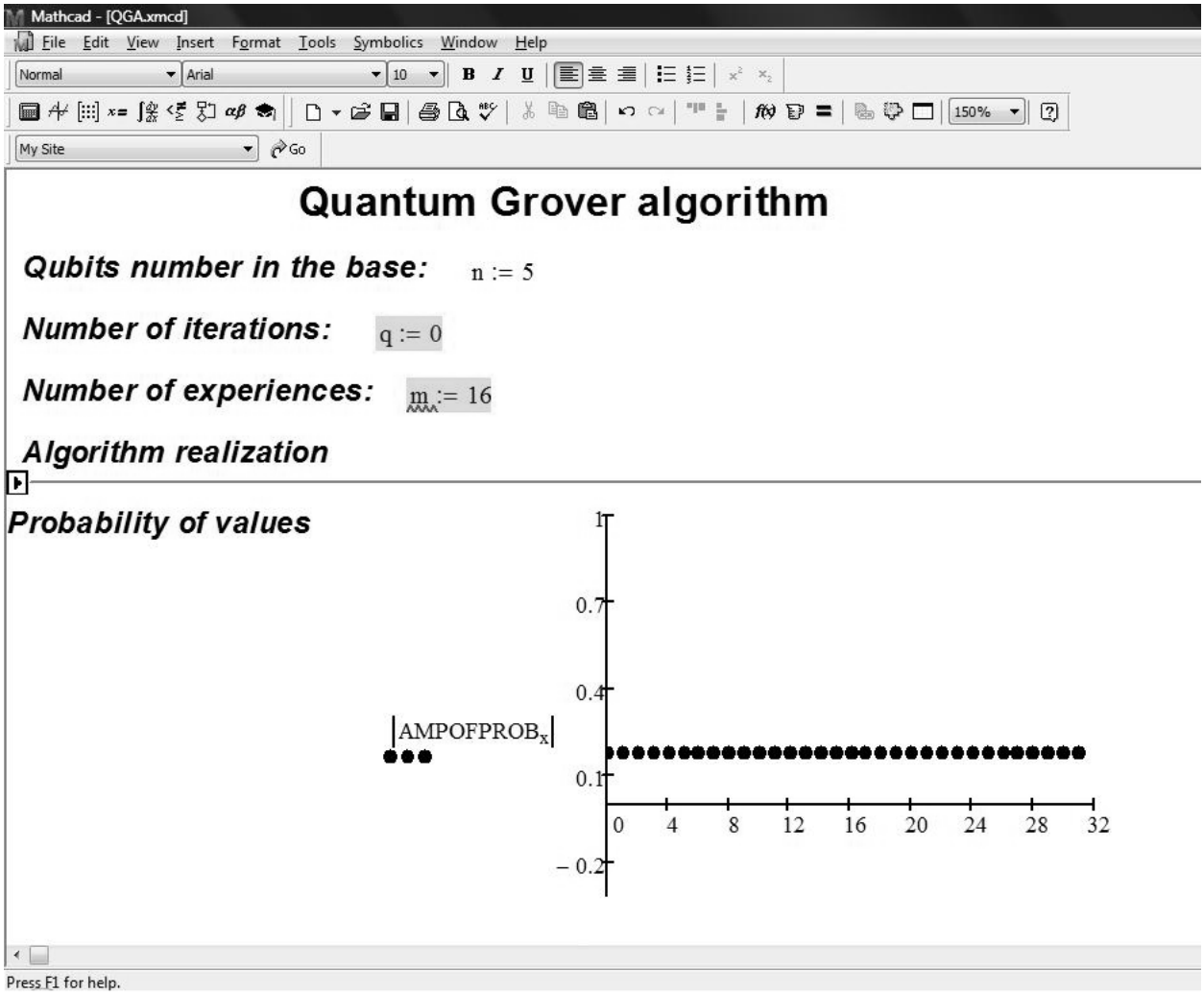


Рис.1. Реализация алгоритма Гровера: распределение амплитуд вероятностей для элементов в базе в начальном состоянии.

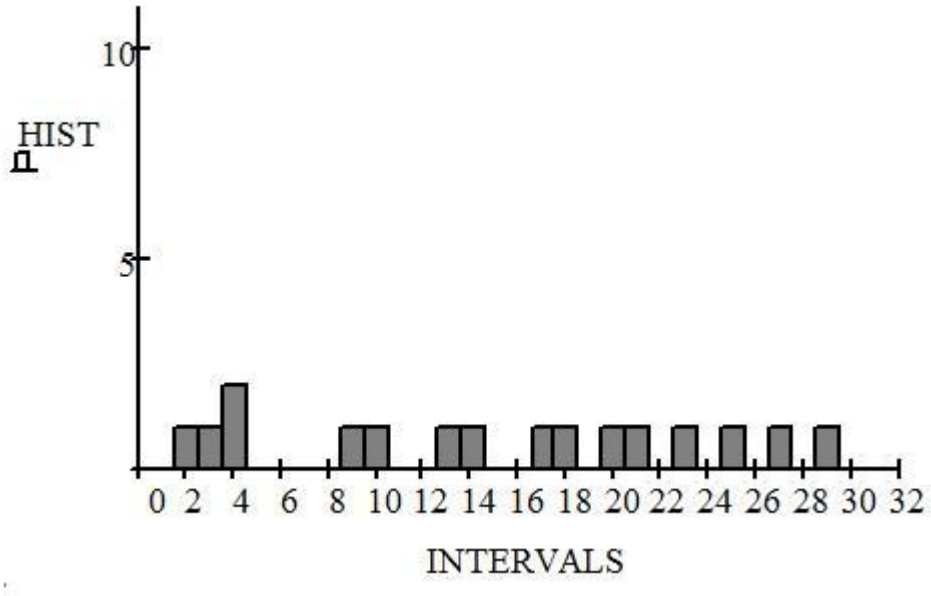


Рис.2. Гистограмма результатов эксперимента

ЛИТЕРАТУРА

1. Попов И.Ю., «Квантовый компьютер и квантовые алгоритмы», / Учебное пособие. СПб:СПбГУ ИТМО, 2007, 88 с.
2. Валиев К.А, Кокин А.А. Квантовые компьютеры: надежды и реальность -Ижевск: РХД, -2001, 352 с.

Лабораторная работа №5

Реализация квантового оптического вентиля CNOT

Цель работы: Изучение принципов работы М-схемы, реализующей квантовый оптический вентиль CNOT.

***Объект исследования*:** Виртуальная лабораторная работа.

Задачи, решаемые в работе:
1. Изучение работы М-схемы, реализующей квантовый оптический вентиль CNOT.
2. Выбор свободных параметров для получения требуемых результатов работы схемы.

СВЕДЕНИЯ ИЗ ТЕОРИИ

В данной работе изучается одна из возможных реализаций логического вентиля CNOT (контролируемое НЕ) на основе эффектов квантовой оптики. Матрица оператора этого преобразования имеет следующий вид:

$$CNOT = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}. \qquad (1)$$

Сложность реализации такого устройства заключается в том, что требуется отслеживание результатов взаимодействия квантовых физических величин, которыми кодируются кубиты, что является весьма нетривиальной задачей. Однако и роль этого вентиля в квантовых вычислениях очень велика.

Прежде всего, необходимо определиться, какая физическая величина интерпретируется как состояние кубита. В нашем случае речь пойдет об однофотонном пакете с круговой поляризацией. Для того чтобы воздействовать на это состояние можно реализовать схему, которая позволяет менять фазу круговой поляризации одного из однофотонных пакетов под действием другого. Мы используем оператор контролируемого сдвига фазы (Controlled Phase Shift - CPS) на π для решения этой задачи:

$$CPS = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix}. \qquad (2)$$

Связь его с CNOT преобразованием, можно записать так:

$$CNOT = I \otimes H \cdot CPS \cdot I \otimes H \qquad (3)$$

где $H = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$ - оператор Адамара; $I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ - единичная матрица.

Реализовать однокубитовый оператор Адамара, как правило, не составляет труда, и задача, таким образом, сводится к реализации оператора контролируемого сдвига фазы. В данной работе мы построим полуклассическую модель данного оператора. Это значит, что мы учтем квантовую природу вещества, а однофотонные поляризованные волновые пакеты заменим слабыми классическими электромагнитными полями с круговой поляризацией. Контролируемым будет суммарный фазовый сдвиг круговой поляризации электромагнитных полей.

Необходимо отметить, что обеспечение контролируемого взаимодействия между двумя полями является нетривиальной задачей, для решения которой необходимы среды с особыми оптическими свойствами. В нашей работе роль такой среды будет играть ячейка с парами металла, в которой сильное взаимодействие между полями реализуется за счет эффекта Керра[1].

Теперь настало время приступить к описанию оптической системы. Пусть у нас имеется ячейка с парами некоторого щелочноземельного элемента (например ^{87}Rb), которую мы поместим в сильное магнитное поле. Затем из системы атомных уровней выберем подсистему, состоящую из пяти зеемановских[2] подуровней. Подействуем на данные атомные переходы резонансными поляризованными по кругу модами излучения на частотах $\omega_1, \omega_2, \omega_3, \omega_4$. Обозначим $e_j^+,\ e_j^-,\ j = 1,2,3,4$ - векторы циркулярных (соответственно правых и левых) поляризаций мод излучения. Будем считать, что резонансный переход $|1\rangle \to |2\rangle$ разрешен для поля с вектором поляризации e_1^+, переход $|2\rangle \to |3\rangle$ разрешен для поля с

[1] Эффект Керра (квадратичный электрооптический эффект) - изменение значения коэффициентов преломления оптических материалов пропорционально второй степени напряженности приложенного электрического поля.

[2] Уровни Зеемана (т.н. тонкая структура) возникают при расщеплении основных энергетических уровней атома в сильном магнитном поле (поле снимает вырождение по магнитному квантовому числу).

вектором поляризации e_2^-, переход $|3\rangle \to |4\rangle$ разрешен для поля с вектором поляризации e_3^-, переход $|4\rangle \to |5\rangle$ разрешен для поля с вектором поляризации e_4^+. Получившаяся таким образом оптическая схема носит название М-схемы (по графическому сходству см. Рис. 1).

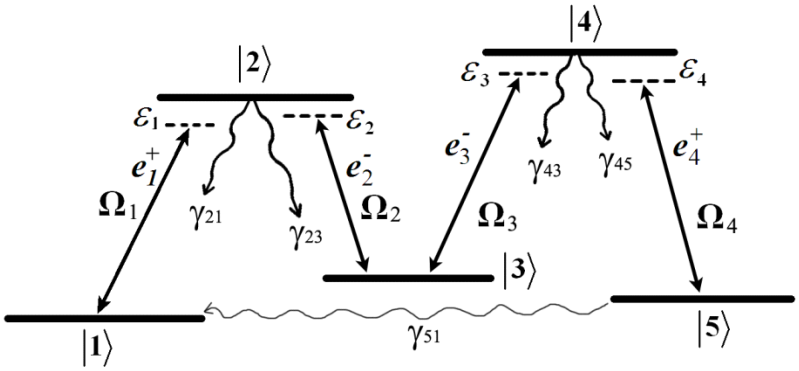


Рис.1. Атомно–полевая М-схема

На рис. 1 символами $\Omega_{i,i+1}, i = 1..4$ обозначены частоты Раби соответствующих переходов:

$$\Omega_{i,i+1} = \frac{\left(\vec{F}_{i,i+1}\vec{d}_{i,i+1}\right)}{2} \qquad (4)$$

где $\vec{d}_{i,j}$- вектор дипольного момента, $\vec{F}_{i,j}$ - напряженность поля на переходе $|i\rangle \to |j\rangle$. Далее $\varepsilon_i, i = 1\ldots4$ - однофотонные отстройки частот электромагнитных полей от частот переходов между атомными уровнями, $\gamma_{21}, \gamma_{23}, \gamma_{43}, \gamma_{45}, \gamma_{51}$ - скорости спонтанного распада верхних уровней. Считается, что вначале электронами заселен только уровень $|1\rangle$.

Для лучшего понимания динамки системы рассмотрим следующие две ситуации:

a) пусть поле частоты ω_1 имеет поляризацию ε_1^- а ω_4 - поляризацию ε_4^- (комбинация $(\varepsilon_1^-;\varepsilon_4^-)$). При такой комбинации поляризаций нелинейный набег фазы поляризации для этих полей наблюдаться не будет. Правила отбора в нашей схеме не разрешают резонансный переход электрона с уровня $|1\rangle$ на уровень $|2\rangle$. Поле ω_1 пройдет через вещество, не взаимодействуя с ним (то есть не будет возбуждать электроны до уровня $|2\rangle$), а значит, и остальные поля со средой взаимодействовать не будут. Суммарный нелинейный набег фазы в этом случае будет равен нулю.

b) пусть теперь поле ω_1 имеет поляризацию ε_1^+ а ω_4 - поляризацию ε_4^+(комбинация $(\varepsilon_1^+;\varepsilon_4^+)$). В этом случае электрон в результате

резонансного взаимодействия может перейти с уровня $|1\rangle$ на уровень $|2\rangle$. Сильное поле частоты ω_2 выравнивает вероятности нахождения электрона на уровнях $|2\rangle$ и $|3\rangle$, так же как и ω_3 уровней $|3\rangle$ и $|4\rangle$. Находясь на уровне $|4\rangle$ электрон может заставить поле ω_4 взаимодействовать с переходом $|4\rangle \to |5\rangle$. Таким образом, все поля, включенные в данную оптическую схему взаимодействуют с соответствующими переходами и потенциально возможен нелинейный набег фазы поляризации.

Остальные два случая ($(\varepsilon_1^-;\varepsilon_4^+)$ и $(\varepsilon_1^+;\varepsilon_4^-)$) рассматриваются подобным же образом. Используя эти результаты, мы можем записать оператор CPS с использованием нелинейных набегов фаз поляризации следующим образом:

$$CPS = \begin{pmatrix} \exp(-i\varphi_{00}) & 0 & 0 & 0 \\ 0 & \exp(-i\varphi_{01}) & 0 & 0 \\ 0 & 0 & \exp(-i\varphi_{10}) & 0 \\ 0 & 0 & 0 & \exp(-i\varphi_{11}) \end{pmatrix} \qquad (5)$$

где, φ_{00} и φ_{01} - суммарные нелинейные набеги фазы поляризации полей ω_1 и ω_4 когда резонансное взаимодействие со средой отсутствует (комбинации поляризации полей $(\varepsilon_1^-,\varepsilon_4^-)$ и $(\varepsilon_1^-,\varepsilon_4^+)$ соответственно), φ_{10} - суммарный нелинейный набег фазы поляризации тех же полей когда резонансное взаимодействие имеет место только для поля ω_1 (комбинация поляризаций $(\varepsilon_1^+,\varepsilon_4^-)$). Наконец, φ_{11} - суммарный нелинейный набег фазы поляризации когда резонансное взаимодействие имеет место для обоих полей (комбинация поляризаций $(\varepsilon_1^+,\varepsilon_4^+)$).

Если сравнить (2) и (5), то получается условие, необходимое для того чтобы при помощи М – схемы реализовать CPS - преобразование, а именно: суммарный набег фазы φ_{11} должен отличаться от набегов фаз φ_{00}, φ_{01} и φ_{10} как можно сильнее (в идеале на π). Подобрав, таким образом, параметры М - схемы (однофотонные отстройки), можно получить единицы на первых трех диагональных элементах и -1 на четвертом.

Теперь определимся с интерпретацией кубитов в нашей схеме. Пусть состояние поляризации ε_1^+ электромагнитного поля ω_1 кодирует первый кубит в состоянии «1», а ε_1^- - в состоянии «0». Точно также пусть состояние поляризации ε_4^+ электромагнитного поля ω_4 кодирует второй кубит в состоянии «1», а ε_4^- - в состоянии «0».

В табл. 1 приведены суммарные набеги фаз для возможных комбинаций поляризации однофотонных пакетов (идеальный случай). Левая позиция в паре чисел соответствует состоянию поля ω_1 с частотой ω_1, правая - ω_4. Во втором и третьем столбцах плюс соответствует наличию резонансного перехода между уровнями, минус – его отсутствию.

	$1 \to 2$	$4 \to 5$	Суммарный набег
$\|00\rangle$	-	-	0
$\|01\rangle$	-	-	0
$\|10\rangle$	+	-	0
$\|11\rangle$	+	+	π

Табл. 1. Наличие переходов между уровнями и суммарный нелинейный набег фазы поляризации в зависимости от поляризации входных пучков.

ПОРЯДОК ВЫПОЛНЕНИЯ РАБОТЫ

В приложенном файле CNOT.mcd смоделирована оптическая схема, на основе которой можно реализовать оптический логический элемент CNOT. В работе предлагается, меняя параметры этой системы добиться того, чтобы она осуществляла эту логическую операцию. В вашем распоряжении имеются однофотонные отстройки и частоты Раби, которые можно изменять (в файле они подсвечены зеленым цветом).

Значения однофотонных отстроек Вам потребуется изменять для того, чтобы получить нелинейные набеги фаз как показано в таблице 1. Для того, чтобы смоделировать ситуацию, когда одно из полей не находится в резонансном взаимодействии с соответствующим ему переходом, необходимо установить частоту Раби этого поля равной нулю. Другие значения частот Раби (кроме нуля и того, что приведено на рисунке) мы использовать не рекомендуем, так как для настройки схемы вполне достаточно однофотонных отстроек. Значения остальных параметров схемы, таких как фазовые сбои на переходах и ширины полос спонтанного распада, менять крайне не рекомендуется в связи с тем, что для их настройки требуется глубокий анализ всей схемы, что выходит за рамки данной работы.

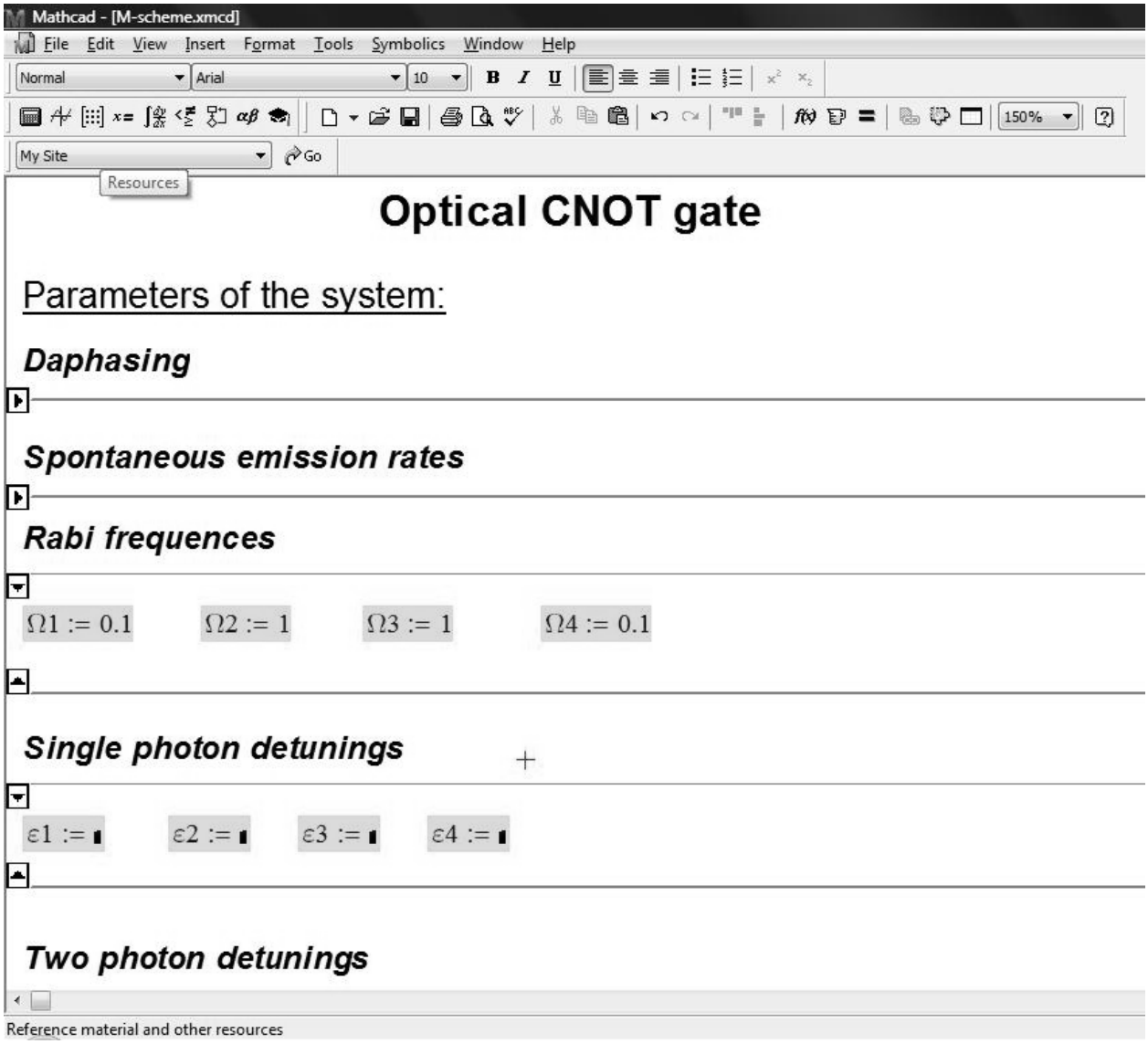


Рис.2. Фрагмент файла с программой; значения параметров в выделенных областях можно изменять

После того, как Вы установили пробные значения однофотонных отстроек, обратите внимание на оператор Гамильтона системы, который записан в резонансном приближении (объекты, за которыми необходимо наблюдать в работе отмечены светло-желтым цветом). На диагонали этого оператора стоят многофотонные отстройки, значения которых вычисляются по формулам, приведенном в подразделе **“Two photon detunings”**.

Далее следуют несколько подразделов, которые касаются программной реализации, изучение которых выводит за рамки данной работы. Следующим объектом, достойным внимания, служит матрица плотности атомной системы. Диагональ этой матрицы представляет собой вероятности найти электрон на данных атомных уровнях (номер строки или столбца равен номеру атомного уровня).

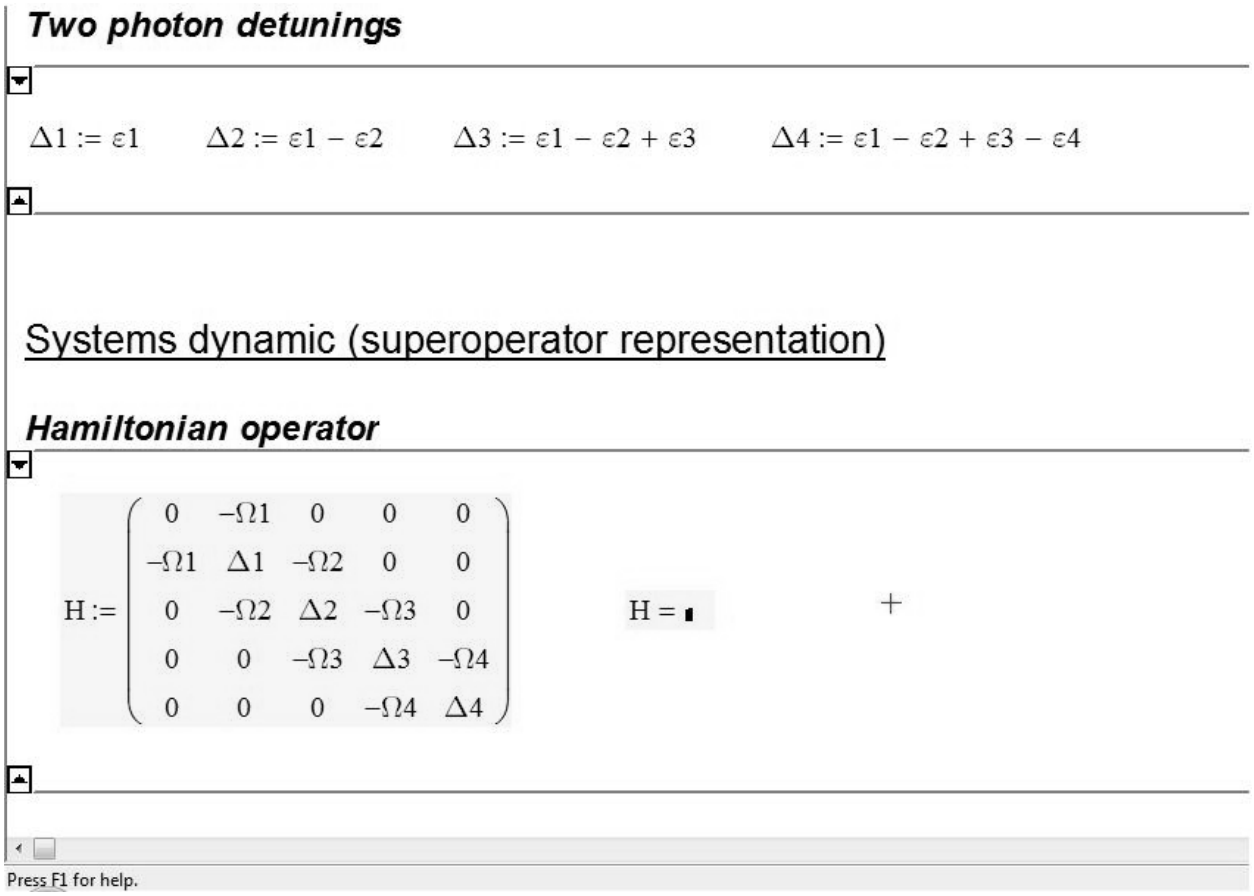


Рис.3. Оператор Гамильтона атомно-полевой системы; на диагонали находятся многофотонные отстройки, частоты Раби находятся на пересечении строки и столбца, номера которых совпадают с номерами атомных уровней на переходах, между которыми включено соответствующее поле

Недиагональные элементы матрицы представляют собой величины, пропорциональные электромагнитной восприимчивости, индуцированной на соответствующем переходе (переход между уровнями с номерами равными номерам строки и столбца). Коэффициент пропорциональности выбран равным единице. Особый интерес, как нетрудно догадаться, здесь представляют элементы DM_{21} и DM_{45}, так как равны (при выбранном коэффициенте пропорциональности) восприимчивостям на переходах, где нас интересует нелинейный фазовый набег поляризации поля. В файле приведена только вещественная часть элементов матрицы плотности, которая отвечает за дисперсию, тогда как мнимая часть отвечает за поглощение на данном переходе (см. закон Бугера).

На следующем этапе предлагается вычислить суммарный нелинейный набег фазы круговой поляризации полей ω_1 и ω_4 (нумерация строк и столбцов в MathCad начинается с нуля). Формула для его вычисления и получившееся значение (выраженное в радианах) приведены в следующем подразделе.

Nonlinear phase shifts

Electromagnetic susceptibilities and corresponding conditional phase shifts

$\chi 12 := DM_{1,0}$ $\qquad$ $\chi 45 := DM_{3,4}$

$\phi 12 := 6\cdot\pi\cdot Re\left(\sqrt{1 + 4\cdot\pi\cdot\chi 12} - 1\right)$ $\qquad$ $\phi 45 := 6\cdot\pi\cdot Re\left(\sqrt{1 + 4\cdot\pi\cdot\chi 45} - 1\right)$

$\phi 12 = \blacksquare\cdot rad$ $\qquad$ $\phi 45 = \blacksquare\cdot rad$

$CPS := \phi 12 + \phi 45$ $\qquad$ $CPS = \blacksquare\cdot rad$

Рис.4. Расчет суммарного нелинейного набега фазы

В последней части работы предлагается сравнить работу реализованного устройства с теорией. Для этого необходимо составить оператор преобразования, которое выполняет система при данном наборе введенных Вами параметров. Он называется “yCPS ” (кратко your CPS) – Ваш оператор контролируемого набега фазы. Форма этого оператора взята из теоретической части (выражение (5)). Для его составления необходимо знать компоненты вектора “SCPS” (Summary CPS), которые представляют собой суммарные нелинейные набеги фаз круговой поляризации полей ω_1 и ω_4 для четырех различных комбинаций. Так первая компонента отвечает нелинейному набегу фаз, когда отсутствует резонансное взаимодействие этих полей с соответствующими переходами (устанавливаем соответствующие частоты Раби в ноль). Вторая компонента – результат резонансного взаимодействия поля ω_4 со «своим» переходом, когда у поля ω_1 такое взаимодействие отсутствует. Третья компонента – результат обратной ситуации. Четвертая – когда резонансное взаимодействие имеет место для обоих электромагнитных полей.

Далее следует наглядное сравнение операторов CPS и yCPS – идеальный и реальный случай. Также сравниваются операторы CNOT и yCNOT, которые получаются из CPS и yCPS соответственно преобразованием, приведенным в теоретической части (выражение (3)). Значение Posibility возвращает вероятность того, что при выбранных Вами параметрах устройство сработает как CNOT.

Checking Results

Input summary conditional phase shifts into the vector

$$SCPS = (\phi 00 \quad \phi 01 \quad \phi 10 \quad \phi 11)$$

$$SCPS := \pi(\blacksquare \quad \blacksquare \quad \blacksquare \quad \blacksquare)^T$$

$$yCPS := \begin{pmatrix} \exp(-i \cdot SCPS_0) & 0 & 0 & 0 \\ 0 & \exp(-i \cdot SCPS_1) & 0 & 0 \\ 0 & 0 & \exp(-i \cdot SCPS_2) & 0 \\ 0 & 0 & 0 & \exp(-i \cdot SCPS_3) \end{pmatrix}$$

Рис.5. Построение “Вашего” оператора CPS.

При выбранных значениях однофотонных отстроек изучить вид оператора Гамильтона системы и матрицы плотности. Вычислить суммарные нелинейные набеги фаз для четырех возможных комбинаций круговых поляризаций электромагнитных полей ω_1 и ω_4 и составить вектор SCPS как описано выше. Сравнить получившиеся операторы yCPS и yCNOT с операторами, получающимися из теории. Вычислить вероятность корректного срабатывания Вашего устройства. Подбором параметров добиться того, чтобы эта вероятность была не ниже 90%.

Theory

$$CPS := \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix}$$

$$CNOT := TP(I, Hmr)\ CPS \cdot TP(I, Hmr)$$

$$CNOT = \blacksquare$$

$$ket := \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix}$$

Your result

$$yCPS = \blacksquare$$

$$yCNOT := TP(I, Hmr)\ yCPS \cdot TP(I, Hmr)$$

$$yCNOT = \blacksquare$$

$$Cket := yCNOT \cdot ket$$

$$Posibility := Cket_3 \cdot \overline{Cket_3}$$

$$Posibility = \blacksquare$$

Рис.6. Сравнение результата (справа) с теорией (слева).

ЛИТЕРАТУРА

1. Попов И.Ю., «Квантовый компьютер и квантовые алгоритмы», / Учебное пособие. СПб:СПбГУ ИТМО, 2007, 88 с.
2. Валиев К.А, Кокин А.А. Квантовые компьютеры: надежды и реальность -Ижевск: РХД, -2001, -С 352.
3. Ottaviani C., Vitali D, Artoni M., Cataliotti F., Tombesi P., // Phys. Rev. Lett., -2003, -V. **90**, -P. 197902.
4. Скалли М.О., Зубайри М.С., Квантовая оптика, М. Физматлит., -2003, -512с.

Лабораторная работа №6

Генерация секретного ключа с помощью квантово-криптографической учебно-исследовательской установки на основе несимметричного волоконно-оптического интерферометра Майкельсона

Цель работы: Изучение основ квантовой криптографии.

***Объект исследования*:** Plug&Play система квантовой криптографии, работающая по протоколу B92 с использованием фазы излучения.

Задачи, решаемые в работе:

1. Генерация и рассылка секретного ключа.
2. Кодирование секретным ключом сообщения и передача сообщении легитимному пользователю.
3. Декодирование сообщения.

СВЕДЕНИЯ ИЗ ТЕОРИИ

Основными проблемами классической криптографии являются аутентификация и распределение ключа. Первая проблема связана с распознаванием легитимных пользователей друг другом. Вторая проблема призвана обеспечить наличие у сторон идентичного секретного ключа, который в дальнейшем используется для кодирования и декодирования информации.

Безусловно-секретным ключом (по Шеннону) является такой ключ, который представляет собой набор случайных (двоичных) символов, длина которого не меньше длины передаваемого сообщения и который используется лишь один раз. Однако снабжать каждое сообщение новым секретным ключом представляется трудоемкой и дорогостоящей задачей. На сегодняшний день известны способы частичного решения проблемы распределения ключа. Некоторые из них связаны с так называемыми двухключевыми или асимметричными протоколами. Они принадлежат к классу вычислительно стойких, т.е. когда раскрытие ключа становится экономически невыгодным или когда вычисление требует больше времени, чем время «ценности» сообщения. Примером асимметричных способов шифрования служит метод, предложенный в 1976 году У. Диффи и М. Хеллманом. Другим решением проблемы распределения ключа является использование квантовых носителей информации –

квантовая криптография. На основе квантовых состояний в принципе, можно генерировать безусловно секретные ключи и легко их менять. Однако заметим, что квантовое распределение ключа не решает проблему аутентификации.

Принцип генерации и квантовой рассылки секретного ключа

Квантовая криптография является, по всей видимости, единственной ветвью науки о квантовой информации и квантовой связи, реализованной на приборном уровне. Безусловная секретность ключа, распределенного между легитимными пользователями при помощи квантовых систем, определяется теоремой о запрете клонирования неизвестного квантового состояния. В известных на сегодняшний день квантовых криптографических системах используется кодирование информации в неортогональных состояниях двухуровневых систем, или кубитах, наиболее известными из которых являются протокол на двух (B92) и на четырех состояниях (BB84). Вместе с тем в литературе рассматривается множество других способов реализации секретных сообщений на основе квантовых состояний, например, протокол на перепутанных состояниях. Однако на практике секретность квантового распределения ключа (КРК) ограничена рядом факторов. Это ошибки и потери, возникающие в канале связи при передаче, отличие подготовленных состояний от идеальных, погрешности системы измерения (например, вызванные темновыми отсчетами фотодетекторов) и т.д. Именно перечисленные ошибки в основном ограничивают длину канала связи, в пределах которой гарантирована секретность квантового распределения ключа.

И так, квантовая рассылка ключа происходит между отправителем, называемым Алисой (Alice), и получателем, называемым Бобом (Bob). Последовательность битов передается по квантовому каналу. Алиса кодирует отправляемые данные, задавая определенный квантовые состояния, Боб регистрирует эти состояния. Идея КРК состоит в том, что если какая либо третья сторона внедрится в канал передачи и перехватит часть из последовательности фотонов, то при их измерении она неизбежно изменит с вероятностью 50% передаваемые квантовые состояния. Отправитель и получатель смогут легко отследить эти изменения и прекратить передачу секретного ключа.

Общий порядок действий при пересылке секретного ключа можно описать пятью этапами:

1. Алиса генерирует случайную последовательность битов. Боб генерирует свою последовательность битов не зависимо от Алисы.
2. Алиса сообщает фотонам необходимое квантовое состояние в соответствии с генерируемой случайной последовательностью и

выбранным протоколом. Боб измеряет текущие квантовые состояния фотонов, изменяя состояние модулятора (ов) в соответствии с генерируемой им случайной последовательностью и выбранным протоколом (п.1).

3. После окончания передачи последовательности Алиса и Боб обсуждают проведенные измерения по открытому каналу. Алисе необходимо знать последовательность базисов, которые использовал Боб при измерении состояния зарегистрированного фотона (результат измерения Боб не сообщает) или необходимо знать номера битов зарегистрированных фотонов (состояние модулятора Боба не сообщается.)
4. Алиса и Боб сравнивают свои последовательности битов и отбрасывают те случаи, когда их базисы не совпали и (или) когда фотон не был зарегистрирован. Оставшиеся значения бит и составляют «сырой» ключ. Ключ называется «сырым», поскольку он содержит ошибки. Под ошибками понимается не совпадение ключей Алисы и Боба. Алиса и Боб определяют число ошибок при передаче ключа, путём раскрытия небольшой части сырого ключа. Если число ошибок выше некоторого критического значения, то это свидетельствует о присутствии злоумышленника, обычно называемого Евой (Eve), и ключ аннулируется.
5. Алиса и Боб проводят коррекцию полученного ключа.

ЭКСПЕРИМЕНТАЛЬНАЯ УСТАНОВКА

В данной лабораторной работе генерация кода осуществляется по протоколу B92, а информационную нагрузку несет **фазовое** состояние частицы. При этом используются базис: фазовые сдвиги вносимые модулятором **0** и $\boldsymbol{\pi}$ для логических значений **0** и **1** соответственно. Для кодировки информации в данном случае используется несимметричный интерферометр Майкельсона. Это так называемая «самонастраивающаяся» (англ. Plug&Play) установка, которая несколько сложнее базовой модели на двух интерферометрах Маха-Цендера, но она обладает несколькими важными преимуществами.

а) интерферирующие импульсы проходят один и тот же путь по линиям связи, что позволяет избежать влияния флуктуаций параметров, вызванных внешними условиями и несовершенством используемого оптического волокна.

б) использование фазовой модуляции избавляет от необходимости постоянного контроля поляризации.

в) применение Фарадеевских зеркал вместо обычных позволяет избавиться от негативного влияния эффектов двулучепреломления в волокне.

г) отсутствует необходимость точной оптической подстройки интерферометров Алисы и Боба. Они могут просто подключиться к существующей оптической линии связи на одномодовом волокне. Необходимо только подстроить время задержки для включения счётчика фотонов.

Рассмотрим ключевые моменты работы этой системы. (рис.1)

Лазерный импульс (λ=1310 nm, τ=5nsec), излучаемый со стороны Боба, пройдя волоконный светоделитель (1) делится в отношении 50/50 светоделителем (2). Один из световых импульсов попадает сразу на линию связи и именуется как **Fast**. Другой пучок сначала проходит через линию задержки (задерживающее волокно) и фазовый модулятор, затем отражается от Фарадеевского зеркала и проходит обратный путь к светоделителю. Попадает на второе Фарадеевское зеркало ,отражается и только после этого выходит на линию связи. Этот луч именуется как **Slow**. Разделенные по времени импульсы Fast и Slow, двигаются к Алисе: 90% света через светоделитель Алисы (30) уходит на фотодиод Алисы. Более мощный импульс Fast используется для синхронизации срабатывания модулятора Алисы, а оставшиеся 10% проходят через ослабитель (аттенюатор) и фазовый модулятор Алисы, затем отражаются от Фарадеевского зеркала и двигаются обратно к Бобу.

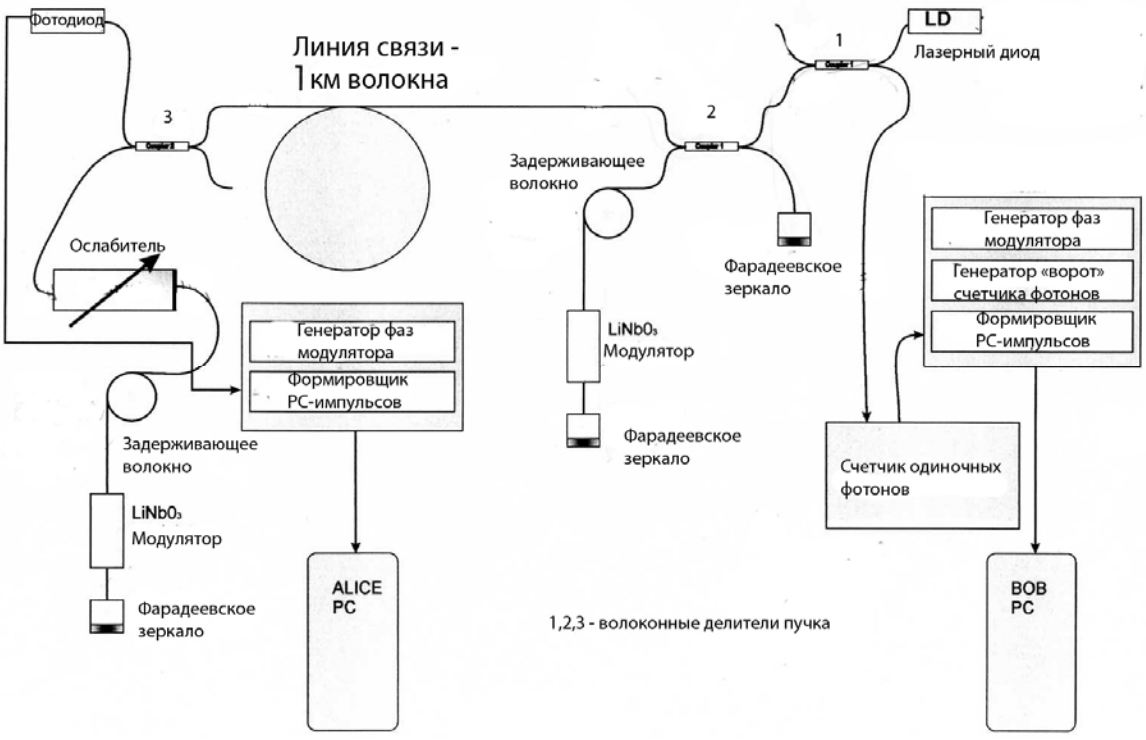


Рис.1. Схема Plug-and-play системы квантовой криптографии

Прибывшие к Бобу импульсы проходят через делитель 2 с зеркалами Фарадея в обратном порядке и попадают на светоделитель 1. После этого делителя образуются четыре импульса **FastFast, FastSlow, SlowFast и SlowSlow**, два из которых **FastSlow** и **SlowFast** интерферируют. Необходимо отметить, что фазовый модулятор Боба активен только для импульса Fast, уже вернувшегося со стороны Алисы. Разница фаз импульсов **FastSlow и SlowFast** может быть равной **0** или **π**, что, соответствует конструктивной или деструктивной интерференции на входе счётчика фотонов на стороне Боба. Результат интерференции измеряется счетчиком единичных фотонов. Для правильной работы счётчика фотонов необходим точный выбор времени задержки открывания счетчика фотонов. Счётчик должен открываться только на время, в течении которого ожидается приход интерферирующих импульсов. Время открытия счётчика (10nsec, так называемые "ворота") выбрано немного больше длительности импульса (5nsec). Время задержки "ворот" можно менять в двоичном коде с помощью восьми переключателей, расположенных на передней панели блока Боба. Справа расположены младшие разряды, слева старшие. **Время задержки можно менять только с разрешения преподавателя**. Процесс передачи информации можно описать следующим образом:

1. Алиса случайным образом выбирает фазовый сдвиг, но только для импульса **Slow**. Для **Fast** ее фазовый модулятор не активен. В итоге она модулирует импульсы **SlowFast** и **SlowSlow**.
2. Боб случайным образом и независимо от Алисы выбирает фазовый сдвиг только для импульсов, возвращающихся от Алисы. В итоге он модулирует импульсы **FastSlow** и **SlowSlow**.
3. Боб включает счётчик фотонов на короткий промежуток времени (10nsec), в течении которого ожидается приход интерферирующих импульсов **FastSlow и SlowFast**
4. Боб по открытому каналу сообщает Алисе последовательность, полученную от счетчика фотонов. В этой последовательности каждому такту задающего генератора присваивается **0** если Боб не принял фотон и **1** в случае принятия фотона. Для каждого такта задающего генератора, для которого был получен отсчёт счётчика фотонов, Боб и Алиса формируют "сырой" ключ по правилу: если модулятор абонента стоял в положении **0**, то биту ключа присваивается логическая единица. Для положения модулятора **π**, присваивается **1**.

Следует учесть, что из-за низкой квантовой эффективности детектирования единичных фотонов (порядка 10%) и малой средней

оптической мощности (меньше одного фотона на импульс в интерферирующих импульсах) средний процент зарегистрированных фотонов в единицу времени значительно меньше числа передаваемых импульсов за тот же промежуток времени. Это приводит к тому, что длина сырого ключа оказывается значительно меньше длины передаваемой последовательности импульсов в течении сеанса связи, но это не даёт ошибки в сыром ключе. Ошибки сырого ключа возникают из-за несовершенства оптической схемы (видность интерференции не равна 100%), темновых отсчетов и деятельности потенциального злоумышленника. В данной работе основной вклад в ошибку дают темновые отсчёты. Это приводит к тому, что криптографические сырые ключи Боба и Алисы будут в некоторой степени различаться. Ошибка порядка 1,5% считается допустимой.

ПОРЯДОК ВЫПОЛНЕНИЯ РАБОТЫ

Включить блоки Алисы и Боба черным тумблером на задней панели каждого устройства. Пока не запущены программы Алисы и Боба на соответствующих компьютерах, блоки Алисы и Боба работают в автоколебательном режиме. С блока Боба передаётся непрерывная последовательность оптических импульсов. Модулятор Боба может работать в трёх режимах – всегда фаза **0** для **FastSlow**, случайная фаза для **FastSlow** и всегда фаза **π** для **FastSlow**. Выбор режима осуществляется трёх позиционным тумблером, расположенным внизу справа на передней панели блока Боба. Переключение производится в горизонтальном направлении. Правое положение – **фаза 0**, среднее положение – **фаза случайная**, левое положение – **фаза π** . Блок Алисы в автоматическом режиме постоянно принимает световые импульсы и модулятор Алисы работает в режиме случайной модуляции. Счетчик фотонов включается при длительном нажатии (около 5 секунд) красной кнопки на передней панели устройства. При этом на дисплее счетчика высветится численное значение частоты отсчётов принимаемого сигнала в герцах. После нажатия на кнопку «отсчеты» на дисплее отобразится текущая температура активного элемента счетчика (лавинного фотодиода), для корректной работы устройства это значение не должно превышать -56°. Повторное нажатие приводит к переключению на показания отсчётов принимаемого сигнала. Время выхода на рабочую температуру лавинного фотодиода составляет около 10 минут.

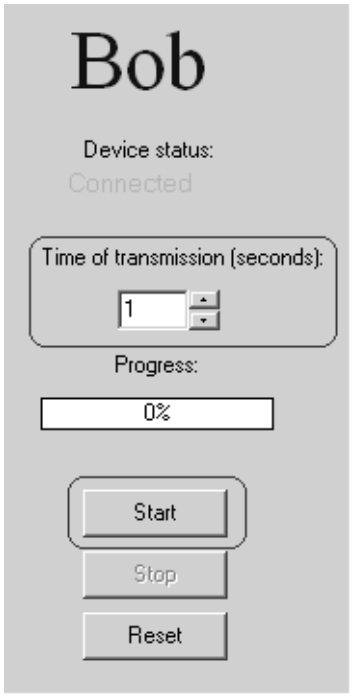
1. Вначале включается только блок Боба. Режим модулятора – **фаза π**. В этом случае модулятор Алисы **не работает,** импульсы **Fast** и **Slow** не модулируются Алисой и будет наблюдаться только **деструктивная**

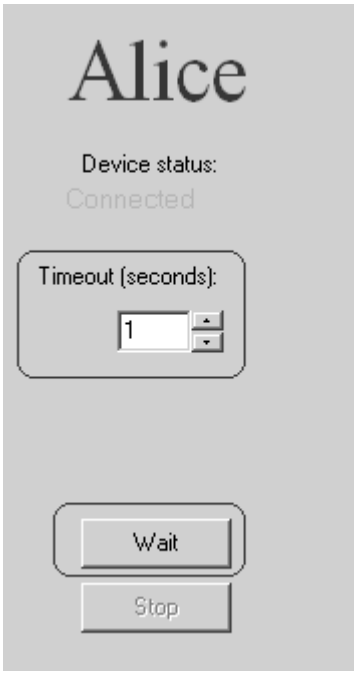
интерференция. Если **время задержки включения счётчика фотонов выбрано правильно**, то счётчик фотонов будет регистрировать только темновые отсчёты. При этом частота отсчётов должна находиться в диапазоне 40 – 120 Гц. При других значениях частоты отсчётов есть возможность установить обратное напряжение на фотодиоде в ручном режиме. При переключении режима модулятора на **фаза 0**, счётчик принимает только конструктивную интерференцию. При этом частота отсчётов должна быть порядка несколько тысяч. При переключении режима модулятора на **фаза случайная**, счётчик принимает и конструктивную и деструктивную интерференцию. При этом частота отсчётов должна быть приблизительно раза в два меньше, чем в предыдущем случае.

Если счетчик дает другие показания, то необходимо подстроить **время задержки включения счётчика фотонов** в диапазоне 1-2 младших разрядов. **Только под руководством преподавателя.**

Затем устанавливаем режим модулятора Боба в среднее положение - **фаза случайная.**

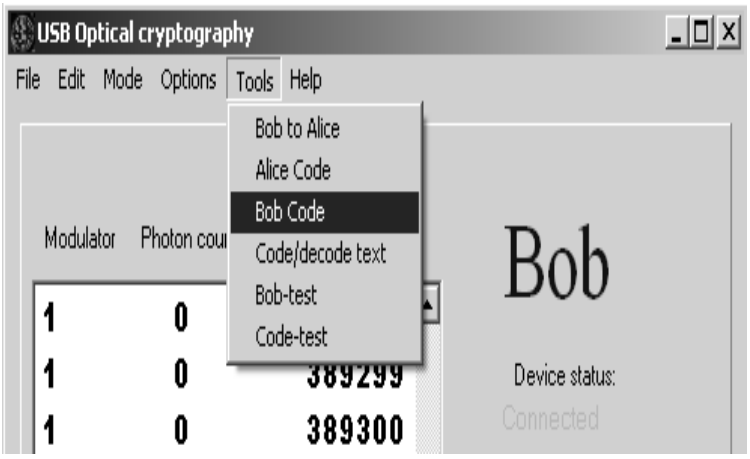
2. Включается блок Алисы. При этом будет иметь место как деструктивная, так и конструктивная интерференция (с вероятностью примерно 50% для каждой) не зависимо от режима модулятора Боба. Это можно проверить переключая режимы модулятора Боба и следя за отсчётами счётчика фотонов.
3. С рабочего стола компьютера Боба запускаем программу Боба, а с компьютера Алисы- соответствующую программу Алисы. В появившемся окне программы Боба выбираем продолжительность сеанса генерации ключа (длительность передачи лазерных импульсов), (Time of transmission), обычно это 5 – 10 секунд. Продолжительность генерации ключа определяет длину ключа. В аналогичном окне Алисы выбираем время ожидания после окончания сеанса передачи, после которого Алиса заканчивает сеанс связи (Timeout). 1 секунда – достаточное время.
4. **Сначала** на стороне Алисы нажимаем кнопку **«wait»**, **затем** на стороне Боба – кнопку **«start»**.

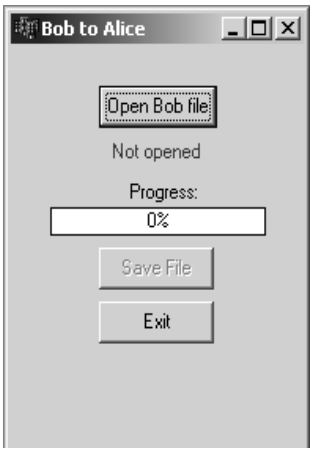




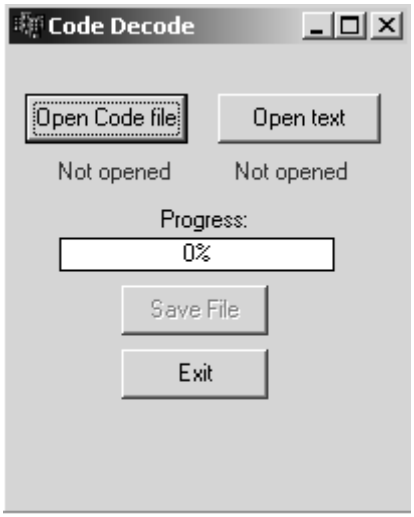
Итак, по прошествии времени сеанса мы получили последовательность состояний на модуляторе Боба (столбец Modulator), показания отсчётов счетчика (столбец Photon counter), а также столбец с порядковым номером каждого отсчета. У Алисы своя пронумерованная последовательность. У Алисы отсутствует столбец Photon counter. Из этих данных формируются файлы Bob.txt и Alice.txt соответственно, состоящие из соответствующих столбцов.

5. **Сформируем сырой ключ Боба**. В верхнем меню Боба выбираем вкладку Tools и нажимаем на «Bob code». Затем в появившемся окне нажимаем на кнопку «Open Bob file», выбираем файл Bob.txt и завершаем операцию кнопкой «Save Code» (имя нового файла «Bob_Code.txt») и кнопками «Save» и «Exit». На этом этапе отсеиваются все значения состояния модулятора, для которых значение счетчика оказалось нулевым. Оставшаяся последовательность состояний модулятора и формирует сырой ключ Боба.





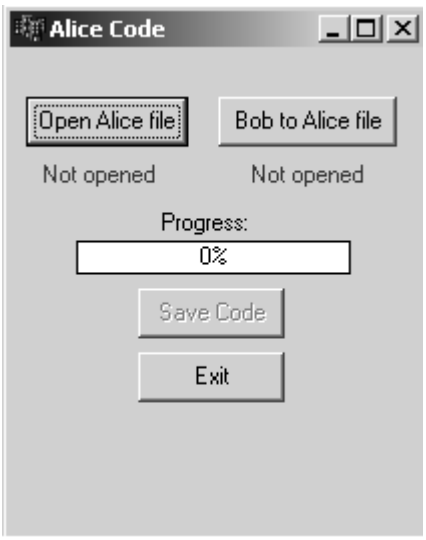
6. **Сформируем файл отсчётов счётчика фотонов**, который будет передаваться по открытому каналу Алисе. Выполняем следующую операцию: Tools→Bob to Alice. В Появившемся окне нажимаем на кнопку «Open Bob file» и также выбираем файл Bob.txt. Заканчиваем операцию: «Save File» (имя нового файла Bob_to_Alice.txt) и «Exit». На этом этапе мы подготовили необходимые данные для Алисы, а именно показания счетчика фотонов и порядковые номера отсчетов.
7. **Закодируем текстовый файл** полученным сырым ключом. Операция: Tools→Code/decode text. В появившемся окне нажимаем на кнопку «Open Code file», выбираем Bob_Code.txt. Далее – кнопка «Open text», выбираем любой текстовый файл с расширением .txt (содержание текста не имеет значения, но его длина не должна превышать размер секретного ключа). Новый файл сохраняем под именем Coded_text.txt и завершаем начатую операцию кнопками «Save File» и «Exit». На этом этапе мы закодировали текст секретным ключом, находящимся у Боба.

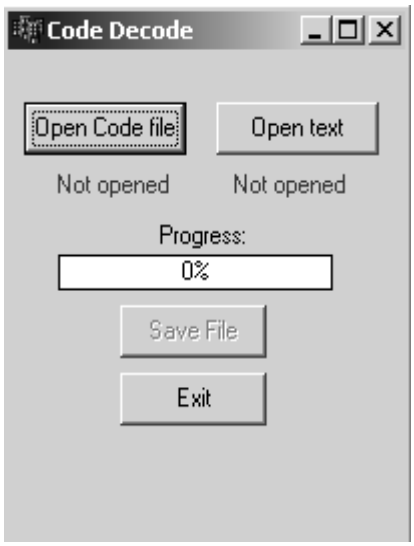


8. С помощью флэшкарты **переносим с компьютера Боба на компьютер Алисы** два файла: Bob_to_Alice.txt и Coded_text.txt, находящиеся в папке «Bob folder» на рабочем столе. (копируем их в папку «Alice folder», ярлык на рабочем столе). Первый необходим для формирования ключа Алисы, а второй содержит в себе закодированный текст, который Алиса должна декодировать. Оба файла не являются секретными и могут передаваться по открытому каналу, например по Интернету. В нашем случае используется флэшкарта.
9. **Сформируем сырой ключ Алисы.** На компьютере Алисы: Tools→Alice_Code. В появившемся окне: кнопка «Open Alice file» - выбираем Alice.txt, кнопка «Bob to Alice file» - выбираем скопированный на флэшкарту Bob_to_Alice.txt файл. Сохраняем этот файл под именем Alice_Code.txt. Завершаем операцию нажатием кнопок «Save code» и «Exit». Таким образом, у Алисы есть последовательность состояний собственного модулятора и показания

счетчика фотонов, которые прислал Боб. Имея эти данные Алиса формирует свой секретный ключ.

10. С помощью **секретного ключа Алиса декодирует** полученное сообщение от Боба (Coded_text.txt). Выполняется операция: Tools→Code/decode text. В появившемся окне нажимаем кнопку «Open Code file» и выбираем Alice_Code.txt. Следующая кнопка «Open text» и выбираем Coded_text.txt. Сохраняем новый файл как Decoded_text.txt и завершаем операцию. Далее можно проверить декодированный текст, в котором из-за несовершенства оборудования (конкретные причины описаны в общих положениях) будут содержаться ошибки. Статистика ошибок изучается в другой лабораторной работе.





ОБРАБОТКА ЭКСПЕРИМЕНТАЛЬНЫХ ДАННЫХ

1. Представить значение частоты темновых отсчётов счетчика фотонов при выключенном блоке Алисы (деструктивная интерференция).
2. Представить значение частоты отсчётов счетчика фотонов при конструктивной интерференции при выключенном блоке Алисы.
3. Представить значение частоты отсчётов счетчика фотонов при работе случайной фазовой модуляции у Боба при выключенном блоке Алисы.
4. Располагая текстом Боба и текстом декодированным Алисой определить процент ошибок в декодированном тексте.

Контрольные вопросы

1. Что изучает квантовая криптография?
2. Какие свойства квантовых объектов используются в квантовой криптографии?

3. Почему используемая в работе установка называется «Plug&Play»? В чём состоят основные её преимущества?
4. Поясните, используя схему лабораторной установки, каким образом выполняется генерация битов АСК.

ЛИТЕРАТУРА

1. В. Желтиков, Криптография от папируса до компьютера, ABF, Москва, 1997.
2. Физика квантовой информации, сб. статей, под редакцией Боумейстера и др., Постмаркет, Москва, 2002.

Лабораторная работа №7

Анализ шумов квантово – криптографической учебно-исследовательской установки на основе несимметричного волоконно-оптического интерферометра Майкельсона

Цель работы: Исследование шумов квантово-криптографической установки**.**

***Объект исследования*:** Plug&Play система квантовой криптографии, работающая по протоколу B92 с использованием фазы излучения.

Задачи, решаемые в работе:

1. Определение процента ошибок в сыром криптографическом ключе.
2. Анализ ошибок, обусловленных темновыми отсчётами счётчика фотонов.

СВЕДЕНИЯ ИЗ ТЕОРИИ

Принцип генерации и квантовой рассылки секретного ключа

Основными проблемами классической криптографии являются аутентификация и распределение ключа. Первая проблема связана с распознаванием легитимных пользователей друг другом. Вторая проблема призвана обеспечить наличие у сторон идентичного секретного ключа, который в дальнейшем используется для кодирования и декодирования информации.

Безусловно-секретным ключом (по Шеннону) является такой ключ, который представляет собой набор случайных (двоичных) символов, длина которого не меньше длины передаваемого сообщения и который используется лишь один раз. Однако снабжать каждое сообщение новым секретным ключом представляется трудоемкой и дорогостоящей задачей. На сегодняшний день известны способы частичного решения проблемы распределения ключа. Некоторые из них связаны с так называемыми двухключевыми или асимметричными протоколами. Они принадлежат к классу вычислительно стойких, т.е. когда раскрытие ключа становится экономически невыгодным или когда вычисление требует больше времени, чем время «ценности» сообщения. Примером асимметричных способов шифрования служит метод, предложенный в 1976 году У.

Диффи и М. Хеллманом. Другим решением проблемы распределения ключа является использование квантовых носителей информации – квантовая криптография. На основе квантовых состояний в принципе, можно генерировать безусловно секретные ключи и легко их менять. Однако заметим, что квантовое распределение ключа не решает проблему аутентификации.

Квантовая криптография является, по всей видимости, единственной ветвью науки о квантовой информации и квантовой связи, реализованной на приборном уровне. Безусловная секретность ключа, распределенного между легитимными пользователями при помощи квантовых систем, определяется теоремой о запрете клонирования неизвестного квантового состояния. В известных на сегодняшний день квантовых криптографических системах используется кодирование информации в неортогональных состояниях двухуровневых систем, или кубитах, наиболее известными из которых являются протокол на двух (B92) и на четырех состояниях (BB84). Вместе с тем в литературе рассматривается множество других способов реализации секретных сообщений на основе квантовых состояний, например, протокол на перепутанных состояниях. Однако на практике секретность квантового распределения ключа (КРК) ограничена рядом факторов. Это ошибки и потери, возникающие в канале связи при передаче, отличие подготовленных состояний от идеальных, погрешности системы измерения (например, вызванные темновыми отсчетами фотодетекторов) и т.д. Именно перечисленные ошибки в основном ограничивают длину канала связи, в пределах которой гарантирована секретность квантового распределения ключа.

И так, квантовая рассылка ключа происходит между отправителем, называемым Алисой (Alice), и получателем, называемым Бобом (Bob). Последовательность битов передается по квантовому каналу. Алиса кодирует отправляемые данные, задавая определенный квантовые состояния, Боб регистрирует эти состояния. Идея КРК состоит в том, что если какая либо третья сторона внедрится в канал передачи и перехватит часть из последовательности фотонов, то при их измерении она неизбежно изменит с вероятностью 50% передаваемые квантовые состояния. Отправитель и получатель смогут легко отследить эти изменения и прекратить передачу секретного ключа.

Общий порядок действий при пересылке секретного ключа можно описать пятью этапами:

1. Алиса генерирует случайную последовательность битов. Боб генерирует свою последовательность битов не зависимо от Алисы.
2. Алиса сообщает фотонам необходимое квантовое состояние в соответствии с генерируемой случайной последовательностью и

выбранным протоколом. Боб измеряет текущие квантовые состояния фотонов, изменяя состояние модулятора (ов) в соответствии с генерируемой им случайной последовательностью и выбранным протоколом (п.1).

3. После окончания передачи последовательности Алиса и Боб обсуждают проведенные измерения по открытому каналу. Алисе необходимо знать последовательность базисов, которые использовал Боб при измерении состояния зарегистрированного фотона (результат измерения Боб не сообщает) или необходимо знать номера битов зарегистрированных фотонов (состояние модулятора Боба не сообщается.)
4. Алиса и Боб сравнивают свои последовательности битов и отбрасывают те случаи, когда их базисы не совпали и (или) когда фотон не был зарегистрирован. Оставшиеся значения бит и составляют «сырой» ключ. «Сырым» называется ключ, содержащий ошибки. Под ошибками понимается не совпадение ключей Алисы и Боба. Существуют методы исправления таких ошибок. Определяется уровень ошибок при передаче ключа, раскрытием небольшой части сырого ключа. Если он выше некоторого критического значения, то это свидетельствует о присутствии злоумышленника, обычно называемого Евой (Eve) и ключ аннулируется.
5. Алиса и Боб проводят коррекцию ошибок полученного ключа.

Квантово-криптографическая установка

В данной лабораторной работе генерация кода осуществляется по протоколу B92, а информационную нагрузку несет **фазовое** состояние частицы. При этом используются базис: фазовые сдвиги вносимые модулятором **0** и $\boldsymbol{\pi}$ для логических значений **0** и **1** соответственно. Для кодировки информации в данном случае используется несимметричный интерферометр Майкельсона. Это так называемая «самонастраивающаяся» (англ. Plug&Play) установка, которая несколько сложнее базовой модели на двух интерферометрах Маха-Цендера, но она обладает несколькими важными преимуществами.

а) интерферирующие импульсы проходят один и тот же путь по линиям связи, что позволяет избежать влияния флуктуаций параметров, вызванных внешними условиями и несовершенством используемого оптического волокна.

б) использование фазовой модуляции избавляет от необходимости постоянного контроля поляризации.

в) применение Фарадеевских зеркал вместо обычных позволяет избавиться от негативного влияния эффектов двулучепреломления в волокне.

г) отсутствует необходимость точной оптической подстройки интерферометров Алисы и Боба. Они могут просто подключиться к существующей оптической линии связи на одномодовом волокне. Необходимо только подстроить время задержки для включения счётчика фотонов.

Рассмотрим ключевые моменты работы этой системы. (Рис.1)

Лазерный импульс (λ=1310 nm, τ=5nsec), излучаемый со стороны Боба, пройдя волоконный светоделитель (1) делится в отношении 50/50 светоделителем (2). Один из световых импульсов попадает сразу на линию связи и именуется как **Fast**. Другой пучок сначала проходит через линию задержки (задерживающее волокно) и фазовый модулятор, затем отражается от Фарадеевского зеркала и проходит обратный путь к светоделителю. Попадает на второе Фарадеевское зеркало ,отражается и только после этого выходит на линию связи. Этот луч именуется как **Slow**. Разделенные по времени импульсы Fast и Slow, двигаются к Алисе: 90% света через светоделитель Алисы (30) уходит на фотодиод Алисы. Более мощный импульс Fast используется для синхронизации срабатывания модулятора Алисы, а оставшиеся 10% проходят через ослабитель (аттенюатор) и фазовый модулятор Алисы, затем отражаются от Фарадеевского зеркала и двигаются обратно к Бобу.

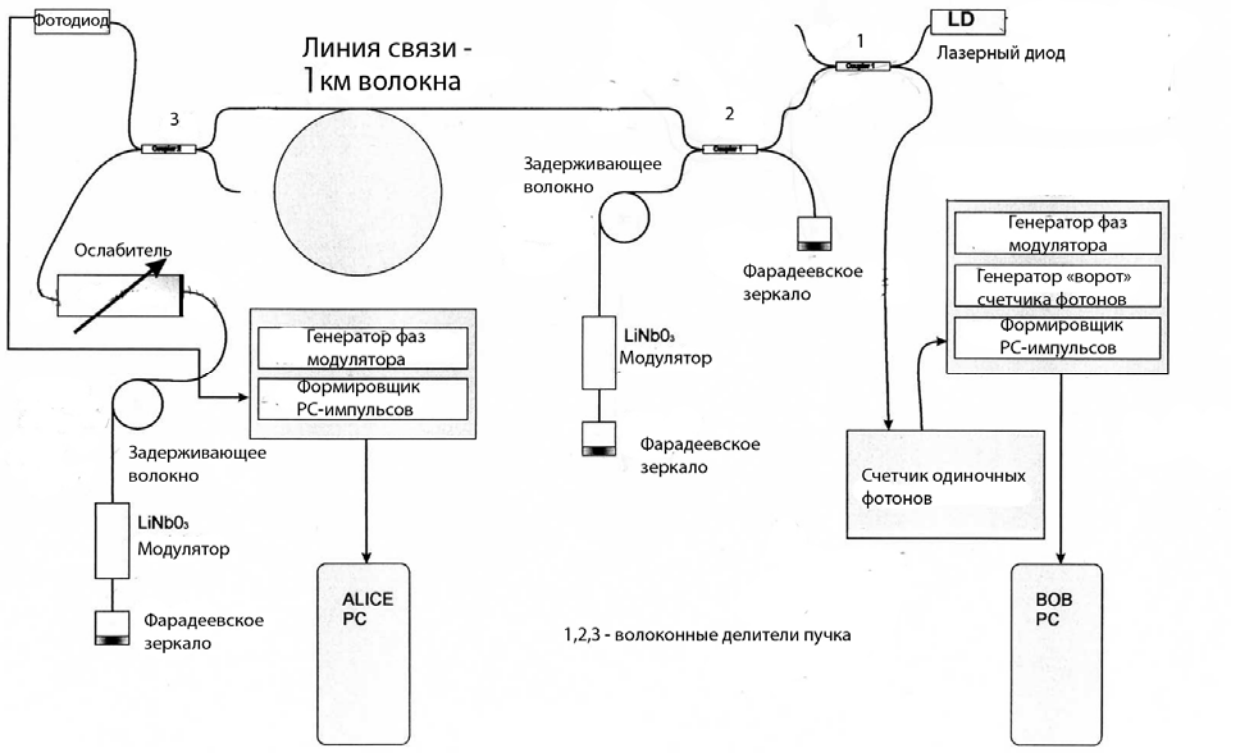


Рис.1. Схема Plug-and-play системы квантовой криптографии

Прибывшие к Бобу импульсы проходят через делитель 2 с зеркалами Фарадея в обратном порядке и попадают на светоделитель 1. После этого делителя образуются четыре импульса **FastFast, FastSlow, SlowFast и SlowSlow**, два из которых **FastSlow** и **SlowFast** интерферируют. Необходимо отметить, что фазовый модулятор Боба активен только для импульса Fast, уже вернувшегося со стороны Алисы. Разница фаз импульсов **FastSlow и SlowFast** может быть равной **0** или $\boldsymbol{\pi}$, что, соответствует конструктивной или деструктивной интерференции на входе счётчика фотонов на стороне Боба. Результат интерференции измеряется счетчиком единичных фотонов. Для правильной работы счётчика фотонов необходим точный выбор времени задержки открывания счетчика фотонов. Счётчик должен открываться только на время, в течении которого ожидается приход интерферирующих импульсов. Время открытия счётчика (10nsec, так называемые "ворота") выбрано немного больше длительности импульса (5nsec). Время задержки "ворот" можно менять в двоичном коде с помощью восьми переключателей, расположенных на передней панели блока Боба. Справа расположены младшие разряды, слева старшие. **Время задержки можно менять только с разрешения преподавателя**. Процесс передачи информации можно описать следующим образом:

1. Алиса случайным образом выбирает фазовый сдвиг, но только для импульса **Slow**. Для **Fast** ее фазовый модулятор не активен. В итоге она модулирует импульсы **SlowFast** и **SlowSlow**.
2. Боб случайным образом и независимо от Алисы выбирает фазовый сдвиг только для импульсов, возвращающихся от Алисы. В итоге он модулирует импульсы **FastSlow** и **SlowSlow**.
3. Боб включает счётчик фотонов на короткий промежуток времени (10nsec), в течении которого ожидается приход интерферирующих импульсов **FastSlow и SlowFast**
4. Боб по открытому каналу сообщает Алисе последовательность, полученную от счетчика фотонов. В этой последовательности каждому такту задающего генератора присваивается **0** если Боб не принял фотон и **1** в случае принятия фотона. Для каждого такта задающего генератора, для которого был получен отсчёт счётчика фотонов, Боб и Алиса формируют "сырой" ключ по правилу: если модулятор абонента стоял в положении **0**, то биту ключа присваивается логическая единица. Для положения модулятора $\boldsymbol{\pi}$, присваивается **1**.

Следует учесть, что из-за низкой квантовой эффективности детектирования единичных фотонов (порядка 10%) и малой средней

оптической мощности (меньше одного фотона на импульс в интерферирующих импульсах) средний процент зарегистрированных фотонов в единицу времени значительно меньше числа передаваемых импульсов за тот же промежуток времени. Это приводит к тому, что длина сырого ключа оказывается значительно меньше длины передаваемой последовательности импульсов в течении сеанса связи, но это не даёт ошибки в сыром ключе. Ошибки сырого ключа возникают из-за несовершенства оптической схемы (видность интерференции не равна 100%), темновых отсчетов и деятельности потенциального злоумышленника. В данной работе основной вклад в ошибку дают темновые отсчёты. Это приводит к тому, что криптографические сырые ключи Боба и Алисы будут в некоторой степени различаться. Ошибка порядка 1,5% считается допустимой.

ПОРЯДОК ВЫПОЛНЕНИЯ РАБОТЫ

Формирование сырого криптографического ключа.

Включить блоки Алисы и Боба черным тумблером на задней панели каждого устройства. Пока не запущены программы Алисы и Боба на соответствующих компьютерах, блоки Алисы и Боба работают в автоколебательном режиме. С блока Боба передаётся непрерывная последовательность оптических импульсов. Модулятор Боба может работать в трёх режимах – всегда фаза **0** для **FastSlow**, случайная фаза для **FastSlow** и всегда фаза **π** для **FastSlow**. Выбор режима осуществляется трёх позиционным тумблером, расположенным внизу справа на передней панели блока Боба. Переключение производится в горизонтальном направлении. Левое положение – **фаза 0**, среднее положение – **фаза случайная**, правое положение – **фаза π** . Блок Алисы в автоматическом режиме постоянно принимает световые импульсы и модулятор Алисы работает в режиме случайной модуляции. Счетчик фотонов включается при длительном нажатии (около 5 секунд) красной кнопки на передней панели устройства. При этом на дисплее счетчика высветится численное значение частоты отсчётов принимаемого сигнала в герцах. После нажатия на кнопку «отсчеты» на дисплее отобразится текущая температура активного элемента счетчика (лавинного фотодиода), для корректной работы устройства это значение не должно превышать -56°. Повторное нажатие приводит к переключению на показания отсчётов принимаемого сигнала. Время выхода на рабочую температуру лавинного фотодиода составляет около 10 минут.

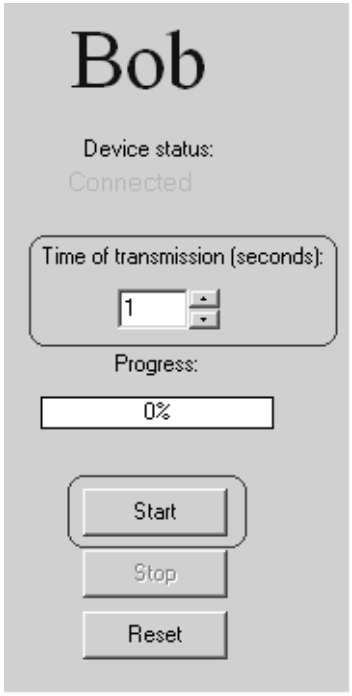
1. Вначале включается только блок Боба. Режим модулятора – **фаза π**. В этом случае модулятор Алисы **не работает,** импульсы **Fast** и **Slow** не

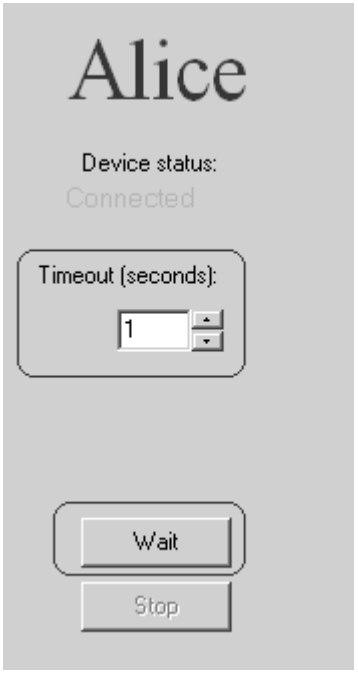
модулируются Алисой и будет наблюдаться только **деструктивная** интерференция. Если **время задержки включения счётчика фотонов выбрано правильно**, то счётчик фотонов будет регистрировать только темновые отсчёты. При этом частота отсчётов должна находиться в диапазоне 40 – 120 Гц. При других значениях частоты отсчётов есть возможность установить обратное напряжение на фотодиоде в ручном режиме. При переключении режима модулятора на **фаза 0**, счётчик принимает только конструктивную интерференцию. При этом частота отсчётов должна быть порядка несколько тысяч. При переключении режима модулятора на **фаза случайная**, счётчик принимает и конструктивную и деструктивную интерференцию. При этом частота отсчётов должна быть приблизительно раза в два меньше, чем в предыдущем случае.

Если счетчик дает другие показания, то необходимо подстроить **время задержки включения счётчика фотонов** в диапазоне 1-2 младших разрядов. **Только под руководством преподавателя.**

Затем устанавливаем режим модулятора Боба в среднее положение - **фаза случайная.**

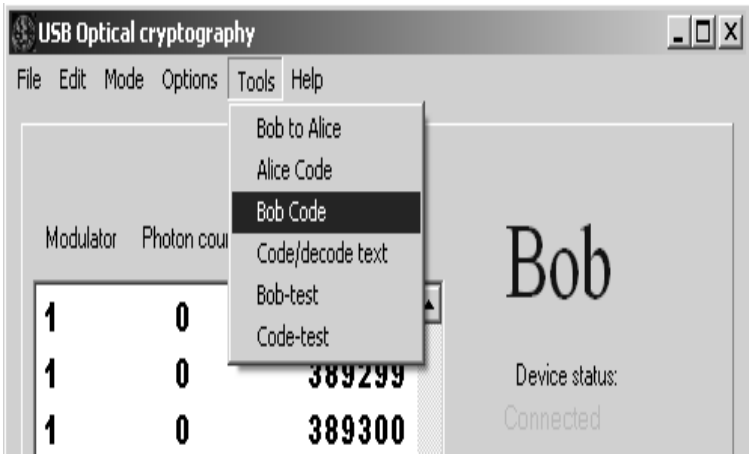
2. Включается блок Алисы. При этом будет иметь место как деструктивная, так и конструктивная интерференция (с вероятностью примерно 50% для каждой) не зависимо от режима модулятора Боба. Это можно проверить переключая режимы модулятора Боба и следя за отсчётами счётчика фотонов.
3. С рабочего стола компьютера Боба запускаем программу Боба, а с компьютера Алисы - соответствующую программу Алисы. В появившемся окне программы Боба выбираем продолжительность сеанса генерации ключа (длительность передачи лазерных импульсов), (Time of transmission), обычно это 5 – 10 секунд. В аналогичном окне Алисы выбираем время ожидания после окончания сеанса передачи, после которого Алиса заканчивает сеанс связи (Timeout). 1 секунда – достаточное время.
4. **Сначала** на стороне Алисы нажимаем кнопку **«wait»**, **затем** на стороне Боба – кнопку **«start»**.

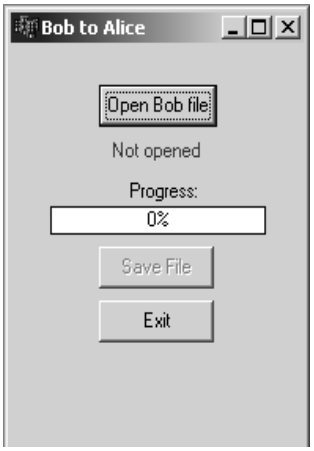




Итак, по прошествии времени сеанса мы получили последовательность состояний на модуляторе Боба (столбец Modulator), показания отсчётов счетчика (столбец Photon counter), а также порядковый номер каждого отсчета. У Алисы своя пронумерованная последовательность. У Алисы отсутствует столбец Photon counter. Из этих данных формируются файлы Bob.txt и Alice.txt соответственно, состоящие из соответствующих столбцов.

5. **Сформируем сырой ключ Боба**. В верхнем меню Боба выбираем вкладку Tools и нажимаем на «Bob code». Затем в появившемся окне нажимаем на кнопку «Open Bob file», выбираем файл Bob.txt и завершаем операцию кнопкой «Save Code» (имя нового файла «Bob_Code.txt») и «Exit». На этом этапе отсеиваются все значения состояния модулятора, для которых значение счетчика оказалось нулевым. Оставшаяся последовательность состояний модулятора и формирует сырой ключ Боба.





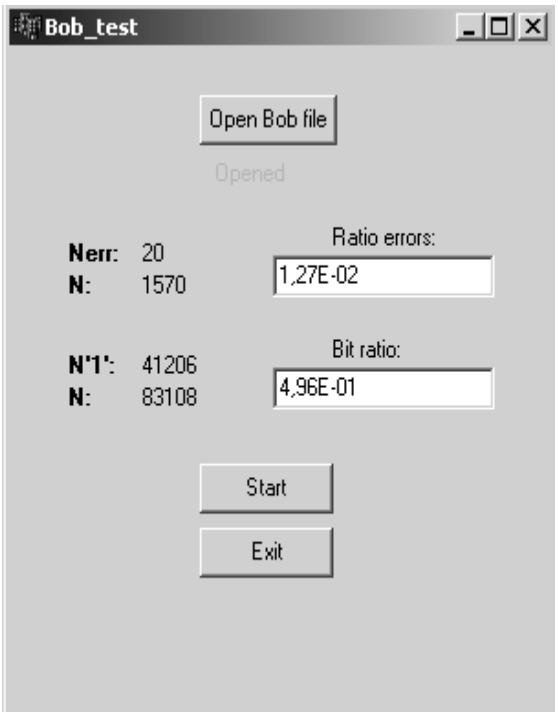
6. **Сформируем файл отсчётов счётчика фотонов**, который будет передаваться по открытому каналу Алисе. Выполняем следующую операцию: Tools→Bob to Alice. В Появившемся окне нажимаем на кнопку «Open Bob file» и также выбираем файл Bob.txt. Заканчиваем операцию: «Save File» (имя нового файла Bob_to_Alice.txt) и «Exit». На этом этапе мы подготовили необходимые данные для Алисы, а именно показания счетчика фотонов и порядковые номера отсчетов.
7. С помощью флэшкарты **переносим с компьютера Боба на компьютер Алисы** файл: Bob_to_Alice.txt (копируем в папку «Alice folder», ярлык на рабочем столе). Файл необходим для формирования ключа Алисы, он не являются секретными и могут передаваться по открытому каналу, например по Интернету. В нашем случае используется флэшкарта.
8. **Сформируем сырой ключ Алисы.** На компьютере Алисы: Tools→Alice_Code. В появившемся окне: кнопка «Open Alice file» - выбираем Alice.txt, кнопка «Bob to Alice file» - выбираем скопированный Bob_to_Alice.txt файл. Сохраняем под именем Alice_Code.txt. Завершаем операцию. Таким образом, у Алисы есть последовательность состояний собственного модулятора и показания счетчика фотонов, которые прислал Боб. Имея эти данные Алиса формирует свой секретный ключ.
9. Определить процент ошибок в сыром криптографическом ключе. Для этого переносим с компьютера Алисы на компьютер Боба файл Alice.txt. В этом файле содержится информация о состояниях модулятора Алисы во время сеанса связи. Этот файл является секретным и используется только для упрощения контроля ошибок в лабораторной работе. В реальной системе Алиса пересылает Бобу только небольшую часть сгенерированного ключа, которая после проверки на ошибки далее не используется. На компьютере Боба выполняем следующее: Tools→Code test. В появившемся окне нажимаем на кнопку «Open Alice file» и выбираем файл Alice.txt (который можно перенести на флэшкарте с компьютера Алисы на компьютер Боба). После нажатия кнопки «Open Bob file» выбираем Bob.txt, жмем «Start». В графе «Error ratio» получим процент ошибок в ключе Боба относительно Ключа Алисы.

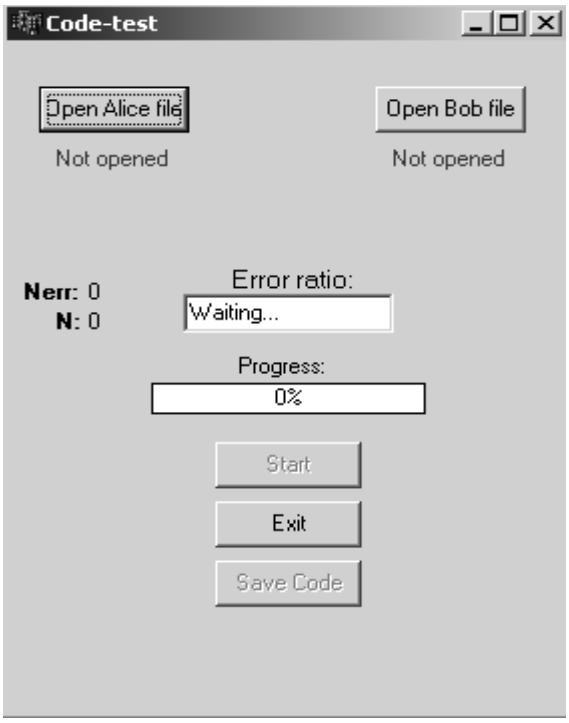
Анализ ошибок, обусловленных темновыми отсчётами счётчика фотонов.

1. Выключаем блок Алисы (черный тумблер на задней панели устройства). Нажимаем кнопку «start» в программе Боба. Модулятор

Боба установлен в режим **фаза случайная.** Отчёт счётчика, полученный при фазе модулятора Боба **π** является ошибкой.

2. Проверяем коэффициент ошибок. Для этого выполняем: Tools→Bob test. В появившемся окне нажимаем на кнопку «Open Bob file» и выбираем Bob.txt, нажимаем «Start». В графе «Ratio errors» получаем проценты темновых отсчетов. В графе «Bit ratio» - процент единичных состояний на модуляторе Боба, что характеризует качество случайной последовательности, подаваемой на модулятор Боба.





ОБРАБОТКА ЭКСПЕРИМЕНТАЛЬНЫХ ДАННЫХ

1. Представить процент ошибок в сыром криптографическом ключе.
2. Представить процент темновых отсчётов счётчика фотонов.
3. Представить процент единичных состояний модулятора Боба.

Контрольные вопросы

1. Что такое Абсолютно Стойкий Ключ? Каковы его свойства и условия применения?
2. В чем состоит алгоритм генерации АСК по протоколу B92?

ЛИТЕРАТУРА

1. В. Желтиков, Криптография от папируса до компьютера, ABF, Москва, 1997.
2. Физика квантовой информации, сб. статей, под редакцией Боумейстера и др., Постмаркет, Москва, 2002.

СПбГУ ИТМО стал победителем конкурса инновационных образовательных программ вузов России на 2007–2008 годы и успешно реализовал инновационную образовательную программу «Инновационная система подготовки специалистов нового поколения в области информационных и оптических технологий», что позволило выйти на качественно новый уровень подготовки выпускников и удовлетворять возрастающий спрос на специалистов в информационной, оптической и других высокотехнологичных отраслях науки. Реализация этой программы создала основу формирования программы дальнейшего развития вуза до 2015 года, включая внедрение современной модели образования.

ИСТОРИЯ КАФЕДРЫ ФОТОНИКИ И ОПТОИНФОРМАТИКИ

Кафедра фотоники и оптоинформатики создана в 2002 году и работает под руководством лауреата премии Ленинского комсомола по науке и технике профессора С.А. Козлова. Одной из важнейших задач кафедры является организация учебного процесса и подготовка специалистов по оптоинформатике – стремительно развивающейся новой области науки и техники, в которой разрабатываются оптические технологии сверхбыстрой передачи, обработки и записи информации, создаются быстродействующие оптические компьютеры и системы искусственного интеллекта. Разработка таких оптических информационно-телекоммуникационных технологий, представляющих собой информационные технологии нового поколения, является приоритетным направлением развития российской науки, техники и технологий.

В рамках образовательного направления 200600 студентам читаются лекционные курсы по оптической физике, теории информации и кодирования, архитектуре вычислительных систем, технологии программирования, цифровым оптическим вычислениям, оптическим технологиям искусственного интеллекта, голографическим системам записи и отображения информации, другим актуальным проблемам оптоинформатики, а также по квантовой информатике. Эти лекционные курсы поддержаны эксклюзивными учебно-исследовательскими экспериментальными практикумами.

Научные подразделения кафедры:

- Проблемная лаборатория волновых процессов, основная задача которой – организация научного руководства студентами и аспирантами молодежной научной ассоциации «Оптика-XXI век», руководитель: д.ф.-м.н., проф.С.А. Козлов.
- Научно-образовательный центр фемтосекундной оптики и фемтотехнологий – руководитель: д.ф.-м.н., проф.В.Г. Беспалов.
- Лаборатория параллельных вычислений, нанофотоники и оптоинформатики – руководитель: д.ф.-м.н., проф.Н.Н. Розанов.
- Лаборатория квантовой информатики – руководитель: к.ф.-м.н., доцент С.А.Чивилихин.
- Лаборатория прикладной голографии – руководитель: к.ф.-м.н., доцент О.В. Андреева

На кафедре сформирована признанная научно-педагогическая школа по фемтосекундной оптике и фемтотехнологиям – руководители: д.ф.-м.н., проф. С.А.Козлов и д.ф.-м.н., проф. В.Г. Беспалов.

Среди студентов и аспирантов кафедры – стипендиаты Президента и Правительства Российской Федерации, победители конкурсов научных работ, проводимых Российской Академией наук, крупнейшими мировыми научными обществами, такими как INTAS (Фонд научно-исследовательских работ Европейского сообщества), SPIE (Международное общество инженеров-оптиков), CRDF (Американский фонд гражданских исследований и развития), OSA (Оптическое общество Америки).

Кафедра фотоники и оптоинформатики постоянно занимает призовые места по итогам конкурсов ведущих научно-педагогических коллективов Университета ИТМО.

Учебное пособие

КВАНТОВАЯ ИНФОРМАТИКА. ЛАБОРАТОРНЫЙ ПРАКТИКУМ

Авторы: Юрий Тарасович Мазуренко
Сергей Анатольевич Чивилихин
Александр Игоревич Трифанов
Вячеслав Васильевич Орлов
Владимир Ильич Егоров

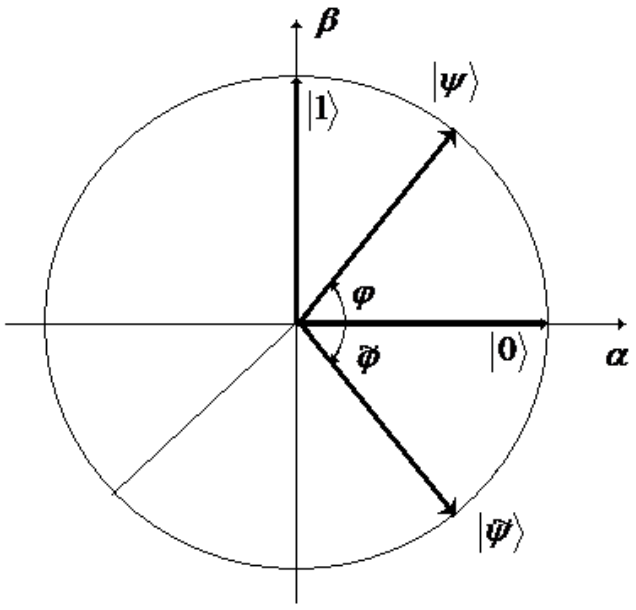
В авторской редакции
Компьютерная верстка В.И.Егоров
Дизайн В.И.Егоров
Зав. РИО Н.Ф.Гусарова

Подписано к печати 00.12.2009
Отпечатано на ризографе Заказ № . Тираж 100

Редакционно-издательский отдел
Санкт-Петербургского государственного
университета информационных
технологий, механики и оптики
197101, Санкт-Петербург, Кронверкский пр., 49

Ю.Т.Мазуренко, С.А.Чивилихин, А.И.Трифанов, В.В.Орлов, В.И.Егоров

КВАНТОВАЯ ИНФОРМАТИКА
ЛАБОРАТОРНЫЙ ПРАКТИКУМ



Санкт-Петербург

2009