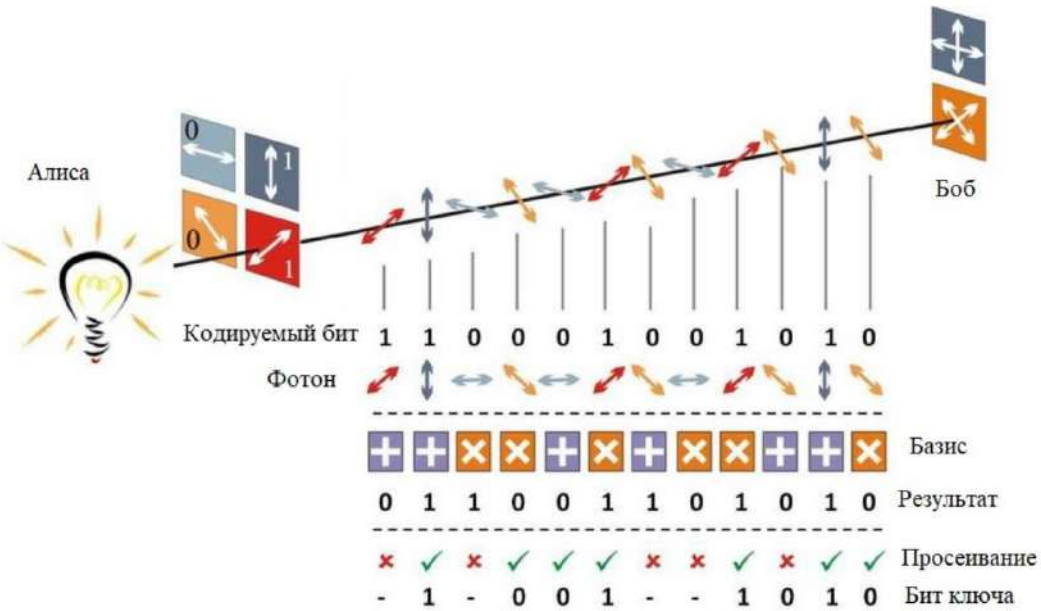
ИТМО

А.А. Гайдаш, В.И. Егоров, А.Е. Иванова, А.В. Козубов, С.М. Кынев, Б.А. Наседкин, Э.О. Самсонов

КВАНТОВЫЕ ТЕХНОЛОГИИ



Санкт-Петербург
2023

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

УНИВЕРСИТЕТ ИТМО

А.А. Гайдаш, В.И. Егоров, А.Е. Иванова, А.В. Козубов, С.М. Кынев, Б.А. Наседкин, Э.О. Самсонов

КВАНТОВЫЕ ТЕХНОЛОГИИ

УЧЕБНО-МЕТОДИЧЕСКОЕ ПОСОБИЕ

РЕКОМЕНДОВАНО К ИСПОЛЬЗОВАНИЮ В УНИВЕРСИТЕТЕ ИТМО по направлениям подготовки 12.03.02 «Оптотехника», 12.03.03. «Фотоника и оптоинформатика», 12.03.04 «Биотехнические системы и технологии», 12.03.05 «Лазерная техника и лазерные технологии», 16.03.01. «Техническая физика» в качестве учебно-методического пособия для реализации основных профессиональных образовательных программ высшего образования бакалавариата.

Санкт-Петербург
2023

Гайдаш А.А., Егоров В.И., Иванова А.Е., Козубов А.В., Кынев С.М., Наседкин Б.А., Самсонов Э.О., Квантовые технологии– СПб: Университет ИТМО, 2023. – 136 с.

Рецензент(ы):
Былина Мария Сергеевна, к.т.н., доцент, зав. кафедрой Фотоники и линии связи, СПбГУТ им. проф. М.А. Бонч-Бруевича;

В пособии приведены основные понятия и принципы квантовых технологий, изложены основы квантовых вычислений, показаны основные принципы и подходы к построению систем квантовой коммуникации и распределенных защищенных сетей на их основе. Приведены принципы формирования, передачи и регистрации квантовых сигналов в волоконно-оптических и атмосферных каналах передачи данных. Рассмотрены базовые протоколы квантовой коммуникации, подходы к обоснованию их стойкости и методы экспериментальной реализации. Рассмотрены различные типы квантовых генераторов случайных чисел.

Содержание

Введение

Представленное пособие охватывает все раздела курса «Квантовые технологии», изучаемые студентами профессиональных образовательных программ высшего образования бакалавариата Университета ИТМО по направлениям подготовки 12.03.02 «Оптотехника», 12.03.03. «Фотоника и оптоинформатика», 12.03.04 «Биотехнические системы и технологии», 12.03.05 «Лазерная техника и лазерные технологии», 16.03.01. «Техническая физика». В соответствии с рабочей программы дисциплины помогает сформировать у студентов следующие компетенции: применять основные законы физики и уравнения квантовой механики для анализа систем квантовых коммуникаций, использовать методы математического моделирования физических явлений, применять численные методы расчета для описания физических явлений и приближенного решения физических задач.

Представленный в пособии теоретический материал будет полезен как молодым преподавателям, так и студентам при подготовке к лекционным и практическим занятиям по курсу «Квантовые технологии».

В данном методическом пособии рассмотрены основные понятия и принципы квантовых технологий. Изложены основы квантовых вычислений, квантовые схемы и алгоритмы.

Подробно рассказывается про виды квантовых технологий и их физическую реализацию: основы квантовых вычислений, квантовые измерения, квантовые коммуникации, квантовая генерация случайных чисел. Даётся представление о текущем состоянии отрасли и векторах её развития.

Показаны основные принципы и подходы к построению систем квантовой коммуникации и распределенных защищенных сетей на их основе. Рассматриваются протоколы квантового распределения ключей, компонентная база квантовой связи. Приведены принципы формирования, передачи и регистрации квантовых сигналов, а также методы и технологии построения квантовых сетей. Детально рассмотрены особенности квантовых коммуникаций в свободном пространстве, а именно квантовая коммуникация по атмосферному каналу связи в условиях прямой видимости, передача запутанных фотонных пар по атмосферному каналу связи на 144 км, квантовая коммуникация между движущимся и наземным объектами, вантовая коммуникация между наземными и низкоорбитальными летательными объектами и др.

Излагаются различные реализации источников одиночных фотонов и детекторов одиночных фотонов, работающих на длинах волн от ультрафиолетового до инфракрасного, а также применение этих технологий

для квантовой связи, области, которая в настоящее время является движущей силой разработки источников и детекторов одиночных фотонов.

Освещается область современной науки такая как квантовая теория информации, основой для которой послужили классическая теория информации и квантовая механика, а также ее математическими основами (матричный и операторный анализ, некоммутативная теория вероятностей и энтропийные (информационные) характеристики квантовых систем). Квантовая теория информации является активно развивающейся областью науки, которая объединяет как квантовые вычисления, так и квантовую коммуникацию.

Рассмотрены различные типы квантовых генераторов случайных чисел. В криптосистемах степень непредсказуемости ключа для шифрования информации во многом зависит от качества генератора случайных чисел, используемого в данной системе. В схемах квантовой криптографии случайным образом могут выбираться базис, а также состояние фотона.

Изучается процесс спонтанного параметрического рассеяния, который на сегодняшний день является неотъемлемой частью квантовой физики и применяется во многих исследованиях, часть из которых будет рассмотрена в данном пособии.

Показаны общие принципы формирования нового способа регистрации изображений, получившего название «фантомные изображения», который основан на пространственных корреляциях двух пучков оптического излучения фантомных изображений, современные его модификации и применения, а также необходимый минимум математического аппарата.

1 Введение в квантовые вычисления

1.1 Понятие кубита

Кубитом называется квантовая система, которая может находиться в двух состояниях $|0\rangle$ и $|1\rangle$ (обозначения Дирака). Примером такой системы может служить фотон с двумя возможными поляризациями или электрон с двумя возможными направлениями спина. В общем случае состояние такой системы задается волновой функцией вида

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle, \tag{1}$$

где α и β – комплексные коэффициенты. При измерении состояния с такой волновой функцией, вероятность обнаружить ее в состоянии $|0\rangle$ равна $|\alpha|^2$, а вероятность обнаружить ее в состоянии $|1\rangle$ равна $|\beta|^2$. Сумма этих вероятностей равна единице.

$$|\alpha|^2 + |\beta|^2 = 1. \tag{2}$$

Волновую функцию $|\psi\rangle$ будем рассматривать как вектор в двумерном линейном пространстве. При этом волновые функции $|0\rangle$ и $|1\rangle$ играют роль базиса этого пространства. Основные состояния будем считать ортонормированными

$$\langle 0 \mid 0\rangle = 1, \quad \langle 1 \mid 1\rangle = 1, \quad \langle 0 \mid 1\rangle = 0. \tag{3}$$

Тогда из условия нормировки волнового вектора кубита $\langle\psi|\psi\rangle = 1$ сразу вытекает требование (2) на коэффициенты α и β.

Кубит допускает геометрическое изображение. В общем случае комплексные коэффициенты могут быть представлены в виде

$$\alpha = \mathrm{e}^{\mathrm{i}\gamma}\cos\frac{\theta}{2}, \quad \beta = \mathrm{e}^{\mathrm{i}\lambda}\sin\frac{\theta}{2}, \tag{4}$$

где i – мнимая единица, γ, λ, θ – действительные числа.
Тогда кубит принимает вид

$$|\psi\rangle = \mathrm{e}^{\mathrm{i}\gamma}\cos\frac{\theta}{2}|0\rangle + \mathrm{e}^{\mathrm{i}\lambda}\sin\frac{\theta}{2}|1\rangle, \tag{5}$$

или

$$|\psi\rangle = \mathrm{e}^{\mathrm{i}\gamma}\left(\cos\frac{\theta}{2}|0\rangle + \mathrm{e}^{\mathrm{i}(\lambda-\gamma)}\sin\frac{\theta}{2}|1\rangle\right) \tag{6}$$

.

Фазовый множитель во многих случаях оказывается несущественным, поскольку он не приводит к наблюдаемым эффектам. Опуская этот множитель и переобозначая $\varphi = \lambda - \gamma$, представим кубит в виде

$$|\psi\rangle = \cos\frac{\theta}{2}|0\rangle + \mathrm{e}^{\mathrm{i}\varphi}\sin\frac{\theta}{2}|1\rangle. \tag{7}$$

Таким образом, полученное представление кубита имеет два параметра - θ и φ. Будем интерпретировать их как углы сферической системы координат. Такое геометрическое изображение кубита называется его представлением на сфере Блоха (рисунок 1).

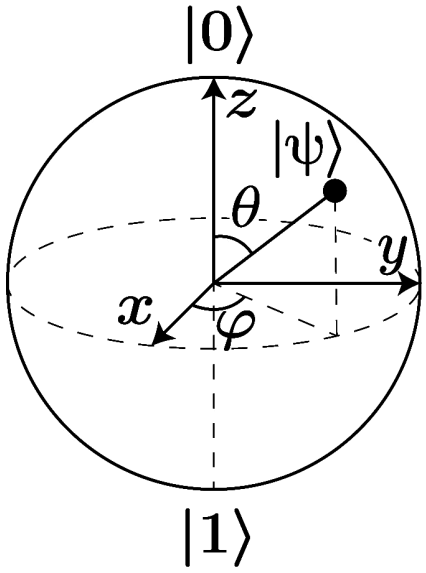


Рис. 1: Изображение кубита на сфере Блоха

В соответствии с выражением 7, при $\theta = 0$ получаем $|0\rangle$, а при $\theta = \pi$, $|\psi\rangle = |1\rangle$ (с точностью до фазового множителя).

На сфере Блоха бесконечно много точек. Соответственно, кубит может находиться в одном из бесконечного множества состояний. Казалось бы, используя один кубит, можно хранить бесконечно много информации. Однако на самом деле это не так. При измерении состояния кубита он может быть найден в одном из двух возможных состояний - $|0\rangle$ или $|1\rangle$.

1.2 Однокубитовые квантовые вентили

В классической теории информации манипуляция над информацией, переводящая её из одного вида в другой, производится с помощью логи-

ческих элементов, иногда называемых гейтами (от англ. gates). В то же время преобразование кубита, заключающееся в переводе его из одного состояние в другое, происходит за счет физического воздействия. В квантовой механике любое воздействие на систему описывается линейным оператором $\hat{\mathrm{U}}$, действующим на состояния системы

$$|\tilde{\psi}\rangle = \hat{\mathrm{U}}|\psi\rangle. \tag{8}$$

Линейность оператора $\hat{\mathrm{U}}$ вытекает из линейности уравнения Шредингера. В самом деле, пусть $|\Psi\rangle$ - зависящий от времени вектор состояния системы. Уравнение Шредингера с гамильтонианом $\hat{\mathrm{H}}$ запишем в виде

$$\mathrm{i}h\frac{\partial|\Psi\rangle}{\partial \mathrm{t}} = \hat{\mathrm{H}}|\Psi\rangle. \tag{9}$$

где t - время, h - постоянная Планка. Пусть, для простоты, гамильтониан системы не зависит от времени. Тогда решение этого уравнения с начальным условием

$$|\Psi\rangle|_{t=0} = |\psi\rangle \tag{10}$$

может быть записано в виде

$$|\tilde{\psi}\rangle = \exp(-\mathrm{i}\hat{\mathrm{H}}t/h)|\psi\rangle. \tag{11}$$

Сравнение уравнений 8 и 11 позволяет связать линейный оператор $\hat{\mathrm{U}}$ с гамильтониантом $\hat{\mathrm{H}}$, описывающим внешнее воздействие на кубит

$$\hat{\mathrm{U}} = \exp(-\mathrm{i}\hat{\mathrm{H}}t/h). \tag{12}$$

Оператор Гамильтона должен быть эрмитовым

$$\hat{\mathrm{H}} = \hat{\mathrm{H}}^{\dagger}, \tag{13}$$

где $\dagger$ – операция эрмитова сопряжения (транспонирование матрицы и поэлементное комплексное сопряжение), для того чтобы его собственные числа – допустимые значения энергии системы – были бы вещественными. Из этого вытекает, что оператор $\hat{\mathrm{U}}$ должен быть унитарным. Унитарность оператора означает, что если исходное состояние системы нормировано, то и состояние, в которое система переходит после взаимодействия, также является номированным.

В дальнейшем мы будем рассматривать воздействие на кубит как процесс вычисления. При этом вектор $|\psi\rangle$ играет роль входного сигнала, а оператор $\hat{\mathrm{U}}$ (квантовый вентиль, квантовый элемент) определяет

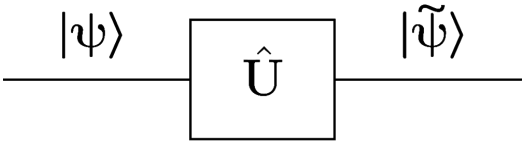


Рис. 2: Квантовый логический элемент $\hat{\mathrm{U}}$ преобразует вектор $|\psi\rangle$ в $|\tilde{\psi}\rangle$

вычислительный процесс. Вектор $|\tilde{\psi}\rangle$ представляет собой результат вычисления (рисунок 2).

Но так как каждый унитарный оператор обратим

$$\hat{\mathrm{U}}^{+}\hat{\mathrm{U}} = \mathrm{I} \Rightarrow \hat{\mathrm{U}}^{+}\hat{\mathrm{U}}\hat{\mathrm{U}}^{-1} = \hat{\mathrm{U}}^{-1} \Rightarrow \hat{\mathrm{U}}^{-1} = \hat{\mathrm{U}}^{+}, \tag{14}$$

то существует такой обратный квантовый вычислительный процесс, описываемый оператором $\hat{\mathrm{U}}^{-1}$, который осуществляет обратное преобразование (рисунок 3).

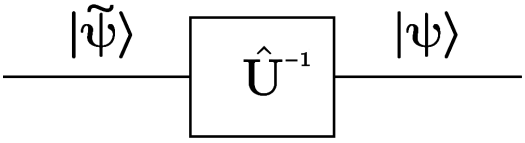


Рис. 3: Квантовый логический элемент $\hat{\mathrm{U}}^{-1}$ осуществляет обратное преобразование вектора $|\tilde{\psi}\rangle$ в $|\psi\rangle$

В дальнейшем мы будем использовать матричное представление операторов $\hat{\mathrm{U}}$. В общем виде однокубитовый квантовый вентиль можно представить как

$$\mathrm{U} = \begin{pmatrix} \mathrm{U}_{00} & \mathrm{U}_{01} \\ \mathrm{U}_{10} & \mathrm{U}_{11} \end{pmatrix}. \tag{15}$$

Матрица U называется матричным представлением оператора $\hat{\mathrm{U}}$.

1.3 Примеры однокубитовых операторов

1.3.1 Оператор $\hat{\mathrm{X}}$

Обозначим квантовый логический элемент NOT через $\hat{\mathrm{X}}$. Определим сначала действие этого оператора на базисные вектора

$$\begin{aligned} \hat{\mathrm{X}}|0\rangle &= |1\rangle, \\ \hat{\mathrm{X}}|1\rangle &= |0\rangle. \end{aligned} \tag{16}$$

Используя линейность оператора $\hat{\mathrm{X}}$, определим действие оператора на произвольный кубит

$$\hat{\mathrm{X}}|\psi\rangle = \hat{\mathrm{X}}(\alpha|0\rangle + \beta|1\rangle) = \alpha\hat{\mathrm{X}}|0\rangle + \beta\hat{\mathrm{X}}|1\rangle, \tag{17}$$

или более наглядно

$$\hat{X}|\psi\rangle = \alpha|1\rangle + \beta|0\rangle = \beta|0\rangle + \alpha|1\rangle. \tag{18}$$

Таким образом оператор $\hat{\mathrm{X}}$ меняет местами коэффициенты при базисных векторах. Матрица такого оператора в вычислительном базисе выглядит как

$$\mathrm{X} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}. \tag{19}$$

Используя тригонометрическое уравнение кубита, легко показать, что оператор $\hat{\mathrm{X}}$ совершает операцию поворота на сфере Блоха. Конкретно, он производит вращение вектора вокруг оси x. Такое преобразование показано на рисунке 4.

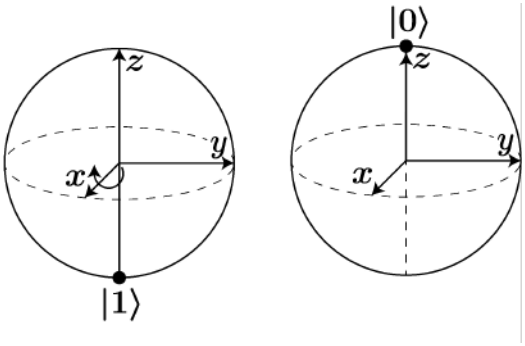


Рис. 4: Оператор $\hat{\mathrm{X}}$ преобразует вектор $|1\rangle$ в вектор $|0\rangle$ путем вращения вокруг оси x

1.3.2 Операторы $\hat{\mathrm{Z}}$ и $\hat{\mathrm{Y}}$

В контексте квантовых вычислений также важными операторами являются $\hat{\mathrm{Z}}$ и $\hat{\mathrm{Y}}$. Действие оператора $\hat{\mathrm{Z}}$ производит отражение от горизонтальной плоскости. Таким образом, его матрица

$$Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \tag{20}$$

а действие, которое он оказывает на базисные вектора, выражается как

$$\begin{array}{l} \hat{Z}|0\rangle = |0\rangle, \\ \hat{Z}|1\rangle = -|1\rangle. \end{array} \tag{21}$$

Логический элемент Y задается матрицей

$$Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}. \tag{22}$$

В отличие от предыдущих рассмотренных нами элементов, элемент Y является комплексным.

1.3.3 Оператор Адамара

Элемент Адамара задается матрицей

$$\mathrm{H} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}. \tag{23}$$

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

$$\begin{pmatrix} \tilde{\alpha} \\ \tilde{\beta} \end{pmatrix} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} \alpha \\ \beta \end{pmatrix} = \frac{1}{\sqrt{2}} \begin{pmatrix} \alpha + \beta \\ \alpha - \beta \end{pmatrix}. \tag{24}$$

Соответственно, элемент Адамара переводит базисные вектора в их суперпозицию.

1.4 Двухкубитовые состояния и операторы

Рассимотрим квантовую систему, состоящую из двух кубитов

$$\begin{array}{l} |\psi_1\rangle = \alpha_1 |0_1\rangle + \beta_1 |1_1\rangle \\ |\psi_2\rangle = \alpha_2 |0_2\rangle + \beta_2 |1_2\rangle \end{array} \tag{25}$$

где $|0_1\rangle, |1_1\rangle, |0_2\rangle, |1_2\rangle$ – базисные состояния первого и второго кубита соответственно, $\alpha_1, \beta_1, \alpha_2, \beta_2$ – комплексные числа. Первый кубит относится к пространству H_1, второй - к пространству H_2. Построим векторное пространство, элементами которого являются пары векторов из двух пространств. Такое пространство называется тензорным произведением пространств H_1 и H_2. Базисные вектора этого пространства представляют собой тензорные произведения базисных векторов из пространств H_1 и H_2

$$|00\rangle = |0_1\rangle \otimes |0_2\rangle\,, |01\rangle = |0_1\rangle \otimes |1_2\rangle\,, \\ |10\rangle = |1_1\rangle \otimes |0_2\rangle\,, |11\rangle = |1_1\rangle \otimes |1_2\rangle\,. \tag{26}$$

Мы будем говорить, что двухкубитовая система находится в состоянии $|00\rangle$, если ее первый кубит находится в состоянии $|0_1\rangle$, а второй кубит – в состоянии $|0_2\rangle$ и т.д.

Операторы, определенные в H_1 и H_2 , действуют в тензорном произведении пространств $\mathrm{H}_1 \otimes \mathrm{H}_2$ покомпонентно

$$\left(\hat{U}_1 \otimes \hat{U}_2\right)(|\psi_1\rangle \otimes |\psi_2\rangle) = \left(\hat{U}_1\,|\psi_1\rangle\right) \otimes \left(\hat{U}_2\,|\psi_2\rangle\right). \tag{27}$$

В то же время двухкубитовый оператор действует на все новое пространство целиком.

Важнейшим двухкубитовым оператором является CNOT, или управляемый NOT. Рассмотрим базис тензорного произведения пространств $\mathrm{H}_1 \otimes \mathrm{H}_2$

$$|00\rangle = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}, \quad |01\rangle = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix}, \quad |10\rangle = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix}, \quad |11\rangle = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix}. \tag{28}$$

В это базисе матрица оператора CNOT имеет вид

$$\mathrm{U_{CN}} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}. \tag{29}$$

Рассмотрим действие этой матрицы на базисные вектора

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}, \quad \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix}, \\ \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix}, \quad \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix}, \tag{30}$$

или

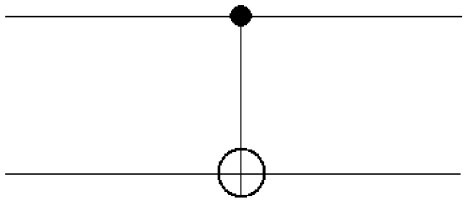


Рис. 5: Условное обозначение, изображающее оператор CNOT

$$\begin{array}{ll} \mathrm{U_{CN}}|00\rangle = |00\rangle, & \mathrm{U_{CN}}|01\rangle = |01\rangle, \\ \mathrm{U_{CN}}|10\rangle = |11\rangle, & \mathrm{U_{CN}}|11\rangle = |10\rangle. \end{array} \tag{31}$$

Таким образом, если первый кубит находится в состоянии $|0\rangle$, а второй кубит находится в одном из базовых состояний $|0\rangle$ или $|1\rangle$, то под действием оператора CNOT (рисунок 5) состояние такой двухбитовой системы не изменяется. Если же первый кубит находится в состоянии $|1\rangle$, а второй – в одном из базовых состояний, то оператор CNOT переводит второй кубит в другое базовое состояние. Состояние же первого кубита не изменяется.

Важным замечанием является то, что любой квантовый алгоритм (речь о которых пойдет дальше) может быть собран из комбинации однокубитных вентилей и двухкубитного вентиля CNOT. В таком случае квантовый комьютер предстает перед нами как цифровое устройство, которое может быть собрано из дискретного набора вентилей.

1.5 Квантовые схемы

Квантовые схемы и алгоритмы собираются из дискретных элементов - квантовых вентилей. Таким образом, если действие первого из них описывается матрицей $\mathrm{U_1}$, а действие второго – матрицей $\mathrm{U_2}$, то результирующее действие двух вентилей будет являться перемножением их матриц

$$\mathrm{U} = \mathrm{U_1}\mathrm{U_2}. \tag{32}$$

Произведение унитарных матриц унитарно. Поэтому последовательное действие двух унитарных преобразований является унитарным преобразованием.

Используя комбинации квантовых вентилей, можно собирать необходимые нам квантовые схемы. Примером может являться схема приготовления состояний Белла, являющихся абсолютно запутанными. Сам

феномен квантовой запутанности будет рассмотрен в главе 4, но на данном этапе формирование состояний Белла является наглядным примером работы квантовых схем. Таких состояний четыре

$$\begin{array}{ll} |\beta_{00}\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle), & |\beta_{01}\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle), \\ |\beta_{10}\rangle = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle), & |\beta_{11}\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle). \end{array} \tag{33}$$

Для получения таких состояний можно использоать схему, представленную на риснуке 6.

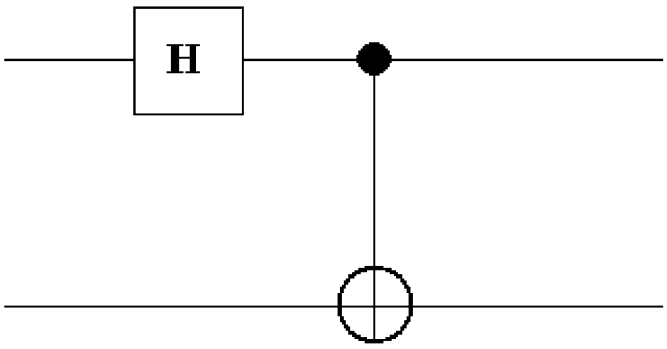


Рис. 6: Квантовая схема, реализующая генерацию состояний Белла

1.6 Квантовые алгоритмы

Для оценки алгоритмов используется теория сложности вычислений. Наиболее часто встречаемой оценкой является асимптотическая оценка алгоритма в худшем случае, то есть верхняя оценка ресурсов. Для обозначения используется большая буква «O» (или же «O большое»). Сложность $O(f(n))$ имеет алгоритм, время работы которого с увеличением размера входных данных n будет возрастать не быстрее, чем некая константа, умноженная на функцию $f(n)$. Для простоты алгоритмы в такой нотации можно разделить на полиномиальные и экспоненциальные. Первые асимптотически ограничены сверху функцией по асимптотике медленнее или соизмеримой с полиномом, такие алгоритмы считаются выполнимыми за «разумное» время. Вторые асимптотически ограничены сверху функцией быстрее полинома (например, показательной или экспоненциальной функцией), такие алгоритмы считаются сложными для вычислений.

Одной из главных особенностей, которая привлекает внимание к квантовым вычислениям, является существование полиномиальных по слож-

ности квантовых алгоритмов. Такие квантовые алгоритмы могут как иметь классические полиномиальные аналоги, так и просто быть асимптотически более быстрыми. Как правило, *квантовое превосходство* достигается для узкого спектра прикладных задач, для вычисления которых на классическом компьютере потребовалось бы на порядки больше временных ресурсов. В современном представлении будущего квантовых вычислений квантовые компьютеры могут быть использованы в дополнение к классическим вычислениям по аналогии с видеокартой, на которой матричные вычисления, необходимые для реализации компьютерной графики, выполняются значительно быстрее, чем на процессоре. Часто встречаемыми являются алгоритмы: Дойча, Дойча-Йожа, квантовое преобразование Фурье, Гровера, Шора.

Если возвращаться к описанию с помощью кубитов и операций над ними, то в общем случае любой квантовый алгоритм представляет собой одну составную матрицу преобразования, на вход которой подается определенное число кубитов. В качестве простейшего квантового алгоритма, который демонстрирует улучшение сложности в нотации О большое, можно рассмотреть алгоритм Дойча. Данный алгоритм не имеет дополнительной практической ценности, кроме как демонстрации снижения сложности вычислений за счёт квантового параллелизма и интерференции.

1.6.1 Алгоритм Дойча

Рассмотрим множество, состоящее из двух базисных векторов $|0\rangle$ и $|1\rangle$, и все возможные функции, отображающие это множество в себя. Таких функций существует четыре. Две функции f_1 и f_2 , называемые постоянными, принимают одно и то же значение при любых значения аргумента

$$\begin{array}{l} \mathrm{f}_1|0\rangle = |0\rangle, \mathrm{f}_1|1\rangle = |0\rangle, \text{ или } \mathrm{f}_1|\mathrm{x}\rangle = |0\rangle, \quad \mathrm{x} = 0, 1, \\ \mathrm{f}_2|0\rangle = |1\rangle, \mathrm{f}_2|1\rangle = |1\rangle, \text{ или } \mathrm{f}_2|\mathrm{x}\rangle = |1\rangle, \quad \mathrm{x} = 0, 1. \end{array} \tag{34}$$

Назовем сбалансированными две другие функции f_3 и f_4, определяемые равенствами

$$\mathrm{f}_3|\mathrm{x}\rangle = |\mathrm{x}\rangle, \mathrm{f}_4|\mathrm{x}\rangle = \mathrm{NOT}|\mathrm{x}\rangle, \mathrm{x} = 0, 1. \tag{35}$$

Легко видеть, что перечисленные функции исчерпывают все возможные отображения $\mathrm{f} : \{|0\rangle, |1\rangle\} \to \{|0\rangle, |1\rangle\}$. Задача формулируется таким образом, что требуется узнать, к какому из двух классов принадлежит неизвестная функция f. Как отмечалось ранее, эта задача не имеет практической значимости и является искусственной с точки зрения формулировки, но позволяет продемонстрировать квантовый параллелизм и

интерференцию. В классическом компьютере для этого требуется две операции - нужно рассчитать $\mathrm{f}|0\rangle$ и $\mathrm{f}|1\rangle$. В квантовом компьютере достаточно одной операции. В случае 2^m значений аргумента классическому компьютеру нужно 2^m операций, квантовому - m операций. Соответствующий квантовый алгоритм называется алгоритмом Дойча.

Для реализации этого алгоритма необходим двухкубитовый унитарный линейный оператор $\mathrm{U_f}$, действующий на базисные элементы $|0\rangle$ и $|1\rangle$ по правилу

$$\mathrm{U_f}(|\mathrm{x}\rangle \otimes |\mathrm{y}\rangle) = |\mathrm{x}\rangle \otimes (|\mathrm{y}\rangle \oplus \mathrm{f}|\mathrm{x}\rangle), \tag{36}$$

где знаком $\oplus$ обозначено сложение по модулю 2. Квантовая схема реализации алгоритма Дойча представлена на риснуке 7.

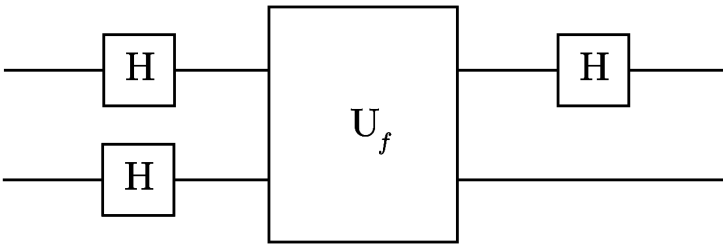


Рис. 7: Квантовая схема, реализущая алгоритм Дойча

Распознование функции f заменяется на распознавание оператора $\mathrm{U_f}$. На вход схемы всегда подается двухкубитовое состояние

$$|0\rangle \otimes |1\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \otimes \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix}. \tag{37}$$

Волновая функция обрабатывается оператором $H \otimes H$, и в результате получается состояние

$$|\chi\rangle = (\mathrm{H} \otimes \mathrm{H})(|0\rangle \otimes |1\rangle) = \frac{1}{2} \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix} \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix} = \frac{1}{2} \begin{pmatrix} 1 \\ -1 \\ 1 \\ -1 \end{pmatrix}, \tag{38}$$

которое и поступает на вход неизвестного логического оператора $\mathrm{U_f}$, а затем на вход оператора $H \otimes H$. Следовательно, сигнал на выходе схе-

мы имеет вид $(H \otimes H \cdot \mathrm{U_f}|\chi\rangle)$. Покажем действие четырех операторов, соответствующих изначальным функциям из уравнений 34 и 35.

Рассмотрим четыре случая

1) $\mathrm{U_1} = \mathrm{I}$

$$|\psi_1\rangle = (\mathrm{H}\otimes\mathrm{H})\cdot|\chi\rangle = \frac{1}{2}\begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix}\cdot\frac{1}{2}\begin{pmatrix} 1 \\ -1 \\ 1 \\ -1 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 1 \end{pmatrix} = |0\rangle\otimes|1\rangle. \tag{39}$$

Этот же результат можно получить проще. Работа схемы в общем виде описывается оператором $\mathrm{L_f} = (\mathrm{H}\otimes\mathrm{H})\cdot\mathrm{U_f}\cdot(\mathrm{H}\otimes\mathrm{H})$, который в данном случае сводится к единичному оператору

$$\mathrm{L_1} = (\mathrm{H}\otimes\mathrm{H})\cdot(\mathrm{I}\otimes\mathrm{I})\cdot(\mathrm{H}\otimes\mathrm{H}) = (\mathrm{H}\cdot\mathrm{H})\otimes(\mathrm{H}\cdot\mathrm{H}) = (\mathrm{I}\otimes\mathrm{I}). \tag{40}$$

Следовательно, $\psi_1 = \mathrm{L_1}|0\rangle\otimes|1\rangle = |0\rangle\otimes|1\rangle$.

2)

$$\mathrm{U_2} = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \tag{41}$$

Тогда

$$\mathrm{U_2}|\chi\rangle = \frac{1}{2}\begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}\begin{pmatrix} 1 \\ -1 \\ 1 \\ -1 \end{pmatrix} = -|\chi\rangle. \tag{42}$$

Используя уравнение 39, получаем

$$|\psi_2\rangle = -(\mathrm{H}\otimes\mathrm{H})\cdot|\chi\rangle = -|0\rangle\otimes|1\rangle \tag{43}$$

3) $\mathrm{U_3} = \mathrm{CNOT}$.

$$|\psi_3\rangle = (\mathrm{H}\otimes\mathrm{H})\cdot\mathrm{CNOT}\cdot(\mathrm{H}\otimes\mathrm{H})|\chi\rangle \tag{44}$$

$$|\psi_3\rangle = \frac{1}{4}\begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix}\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}\begin{pmatrix} 1 \\ -1 \\ 1 \\ -1 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix} = |1\rangle\otimes|1\rangle. \tag{45}$$

4) $\mathrm{U}_4 = \mathrm{CNOT}\cdot(\mathrm{NOT}\otimes\mathrm{NOT})$.

$$|\psi_4\rangle = \frac{1}{4}\begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix}\begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}\begin{pmatrix} 1 \\ -1 \\ 1 \\ -1 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ -1 \end{pmatrix} = -|1\rangle\otimes|1\rangle. \tag{46}$$

Итак, первый канал выходного сигнала для первых двух случаев, т.е. для постоянных функций, содержит $|0\rangle$. Для второй пары случаев (для сбалансированных функций) первый канал выходного сигнала содержит $|1\rangle$. Во втором же канале выходного сигнала во всех четырех случаях находится $|1\rangle$. Таким образом, состояние кубита в первом канале позволяет определить тип используемой функции (сбалансированная или постоянная), что и требовалось при постановке задачи.

1.7 Контрольные вопросы

1. Что такое кубит?
2. Представление кубита на сфере Блоха.
3. Какие состояния может принимать кубит при его измерении?
4. Уравнение Шредингера.
5. Что такое квантовый вентиль?
6. Приведите пример однокубитовых операторов.
7. Что такое квантовое превосходство?
8. Квантовая схема, реализующая алгоритм Дойча.

2 Основы квантовых коммуникаций

2.1 Шифрование данных. Проблема передачи ключа

В современных системах передачи данных информация защищается с помощью шифрования – обратимого преобразования информации в целях сокрытия от неавторизованных лиц, с предоставлением в это же время авторизованным пользователям доступа к ней. Шифрование выполняется с помощью специальной битовой последовательности – ключа, который должен быть известен только авторизованным пользователям. Если все пользователи используют одинаковый ключ для шифрования и дешифрования, такая криптосхема называется симметричной.

Поскольку ключ тоже является данными (представляет собой битовую строку), любая система шифрования на практике сталкивается с рекурсивной проблемой передачи ключа: «Чтобы передать данные, нужно передать ключ, как это сделать?».

На практике существует два метода решения этой проблемы:

- Пересылка ключей доверенными курьерами («ручным» методом»);
- Использование асимметричного шифрования (криптографии с открытым ключом) для шифрования и распределения симметричных ключей.

Первый метод является надёжным, но не технологичным и не подходит для систем с большим количеством пользователей. Второй широко применяется в настоящее время (например, при шифровании паролей в сети Интернет). В нём используется ключ, разделённый на две части: открытую и закрытую. Эти части связаны друг с другом через специальную математическую функцию так, чтобы:

- Закрытый ключ позволял расшифровывать сообщения, зашифрованные открытым ключом;
- Зная только открытый ключ, было практически невозможно вычислить из него закрытый ключ;
- Зная только открытый ключ, было практически невозможно расшифровать сообщения.

Как мы увидим далее, асимметричное шифрование окажется чрезвычайно уязвимым в эпоху квантовых компьютеров. Недостатки существующих методов шифрования:

Криптография с симметричным ключом:

- Необходим защищенный канал для передачи ключа;
- В особо важных случаях (гос. тайна, банковская информация) передача ключа отправителю и получателю осуществляется в ручном режиме на физическом носителе (курьером);
- Для обеспечения высокого уровня безопасности передачи данных необходима частая смена ключа, что влечет проблему его передачи.

Криптография с открытым ключом (асимметричная):

- Безопасность широко используемых методов основана на том, что перехватчик не успеет расшифровать информацию, пока она актуальна;
- Сложность дешифровки сообщений зависит от длины ключа. Увеличение его длины значительно перегружает инфраструктуру и уменьшает скорость обмена сообщениями;
- Подобрать ключ конечной длины технически возможно (RSA длиной 768 бит был успешно «взломан» в 2010 г. даже без квантового компьютера).

2.2 Квантовый компьютер как угроза современной информационной безопасности

В предыдущем разделе упоминалось, что получить закрытую часть асимметричного ключа из открытой «практически невозможно». Что это на самом деле означает?

Когда речь идёт о рисках применения асимметричной криптографии, «практически невозможно» здесь означает «за конечное время на электронном компьютере», то есть с помощью технологии XX века.

Базовый постулат звучит так: расшифровка криптографических ключей длиной от 1024 бит и более на электронном компьютере занимает время, значительно превышающее срок актуальности информации (например, 10 000 лет). Однако из этого напрямую следует, что безопасность зашифрованных с использованием таких ключей систем не является абсолютной и связана напрямую с вычислительными возможностями криптоаналитика. Даже до появления квантового компьютера были предприняты успешные попытки взлома данных, зашифрованных при помощи алгоритма RSA с ключом длиной 768 бит, который считался надёжным.

В качестве примера математической основы асимметричных алгоритмов можно привести пару «умножение простых чисел» (прямая операция) и «разложение большого числа на простые множители» (обратная операция). При этом выполнение обратной операции более затратно по времени и вычислительной мощности. На этом свойстве основан, например, популярный зарубежный алгоритм RSA.

Сегодня известно, что квантовые вычисления могут гораздо (экспоненциально) быстрее и эффективнее решать сложные вычислительные задачи. В 1994 году был представлен квантовый алгоритм быстрой факторизации чисел (алгоритм Шора), пригодный для взлома криптографических систем с открытым ключом со скоростью, близкой к скорости шифрования, что делает такие системы бесполезными. В 2012 году была продемонстрирована его экспериментальная реализация на квантовом компьютере (на примере числа 15). Квантовые алгоритмы могут быть применены и для быстрого решения других задач криптоанализа.

Таким образом, квантовые компьютеры представляют угрозу для применения асимметричного шифрования, лежащего в основе современной инфраструктуры безопасности.

Дополнительным риском является то, что если информацию нельзя взломать прямо сейчас, то ее можно сохранить и расшифровать в будущем — например, с помощью квантовых компьютеров. Известно, что в некоторых странах (в частности, США) существуют гигантские data-центы, хранящие копии зашифрованных данных для последующего криптоанализа.

Эта угроза известна в формулировке «Теоремы Моска», звучащей так: «Если сумма времени, необходимого для переоборудования инфраструктуры безопасности и времени, в течение которого информация должна оставаться зашифрованной, превышает время, оставшееся до создания квантового компьютера, то начинайте беспокоиться!» Принцип работы «Теоремы Моска» представлен на рисунке 8.

Рис. 8: Теорема Моска

Интересно, что криптоалгоритм, устойчивый к любым атакам, в том числе с применением квантовых компьютеров, был придуман задолго до появления даже компьютеров электронных. Речь идёт о методе одноразовых блокнотов (шифре Вернама), для которого было теоретически доказано, что никакие методы его криптоанализа («взлома»), даже квантовые, не дают лучшего результата, чем угадывание ключа прямым перебором всех возможных значений.

Абсолютно стойкий ключ:

- Каждый бит случаен и не связан с остальными;
- Длина ключа равна длине сообщения (побитовое кодирование);
- Применяется только один раз.

Поскольку абсолютно стойкий ключ – симметричный шифр, для него актуальна проблема передачи ключа. Кроме того, необходимость побитового кодирования требует генерации больших объемов ключей, а условие абсолютной случайности ограничивается техническим уровнем генераторов случайных чисел. Эти факторы ограничивали его применение до появления квантовых технологий.

Квантовая рассылка ключей, речь о которой пойдет в следующем разделе, позволяет производить сетевое распределение абсолютно стой-

ких ключей и поэтому рассматривается как один из основных методов защиты информации в эпоху квантовых компьютеров, который придёт на смену асимметричному шифрованию.

2.3 Квантовая рассылка ключей

Как обсуждалось выше, квантовый компьютер представляет серьёзную опасность для современной криптографии. Абсолютно стойкий ключ является решением, но требуются автоматические методы его генерации и распределения в больших объемах.

Квантовая рассылка ключей (КРК, квантовая криптография) позволяет безопасно генерировать и распределять симметричные секретные ключи на основе использования законов квантовой физики. Обнаружение перехвата в канале при этом выполняется за счёт использования одиночных фотонов для кодирования сигналов.

Одиночный фотон:

- Нельзя незаметно измерить (не изменив);
- Нельзя разделить;
- Нельзя скопировать.

В отличие от классических систем передачи данных, в которых возможно незаметное снятие сигнала из канала, в системах КРК нарушитель может получить только несовершенную копию ключа, одновременно «испортив» оригинал (рисунок 9).

Любое подслушивание в квантовом канале сразу обнаруживается, так как вносит в процесс передачи ключей многочисленные легко обнаруживаемые пользователями ошибки. Ошибки при перехвате квантового сигнала неизбежны вследствие фундаментальных свойств квантовых объектов.

В отличие от классических устройств, безопасность систем квантовой рассылки ключей является безусловной, то есть не зависит от времени и вычислительной мощности перехватчика.

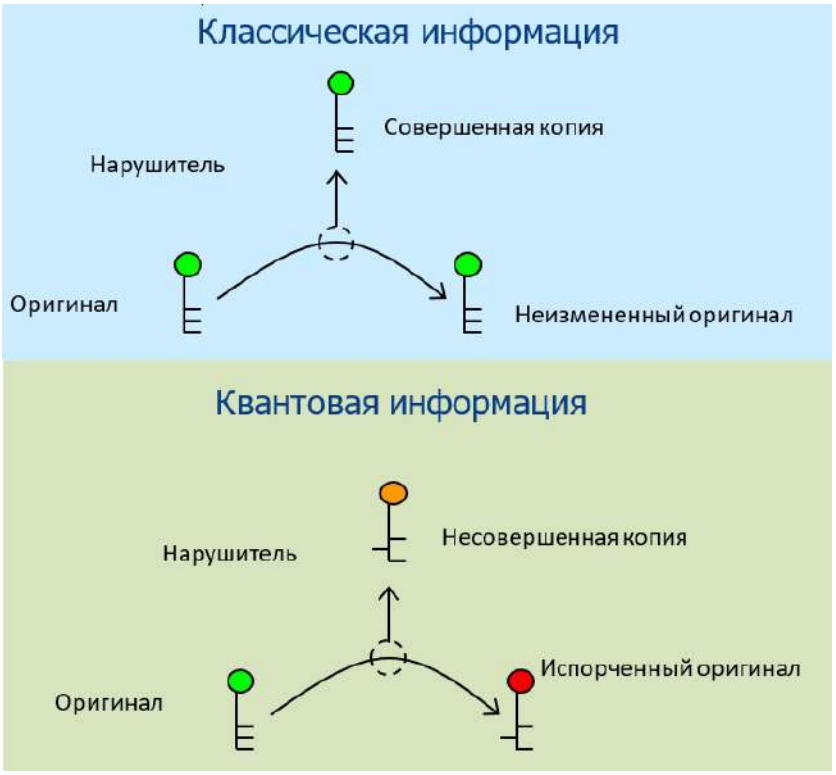


Рис. 9: Передача классической информации и передача квантовой информации

История квантовой криптографии восходит к работе американского учёного С. Визнера «Сопряженное кодирование», где он показал возможность передачи информации с помощью единичных квантов света. Эта работа позднее вдохновила американца Ч. Беннета и канадца Ж. Брассара на создание первого протокола квантовой рассылки ключа, получившего название BB84 по фамилиям авторов и году создания (рисунок 10).

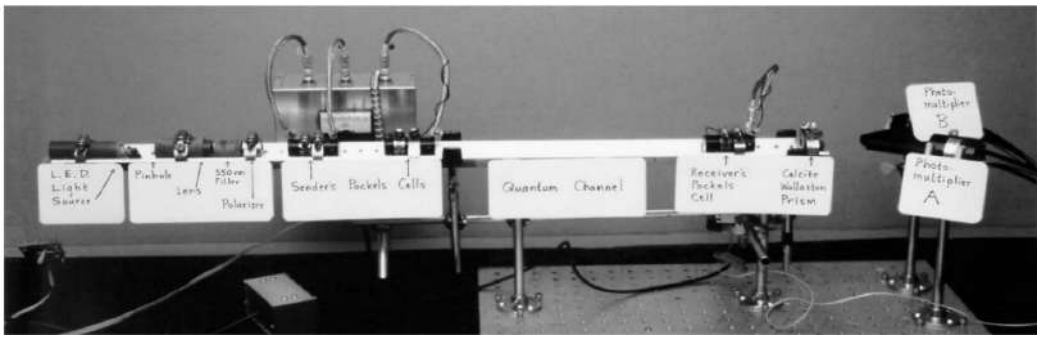


Рис. 10: Фотография первой в мире системы квантовой рассылки ключей (дальность 32,5 см)

2.4 Принципы работы. Протокол BB84.

На рисунке рисунок 11 приведена общая схема системы КРК. Легитимные пользователи (Алиса и Боб) соединены двумя каналами: квантовым (для рассылки ключей с помощью одиночных фотонов) и классическим (для обсуждения результатов). Для работы также необходим канал синхронизации между Алисой и Бобом (на рисунке не показан). Предполагается, что нарушитель (Ева) имеет свободный доступ ко всем трём каналам, но открытый канал должен быть аутентифицированным.

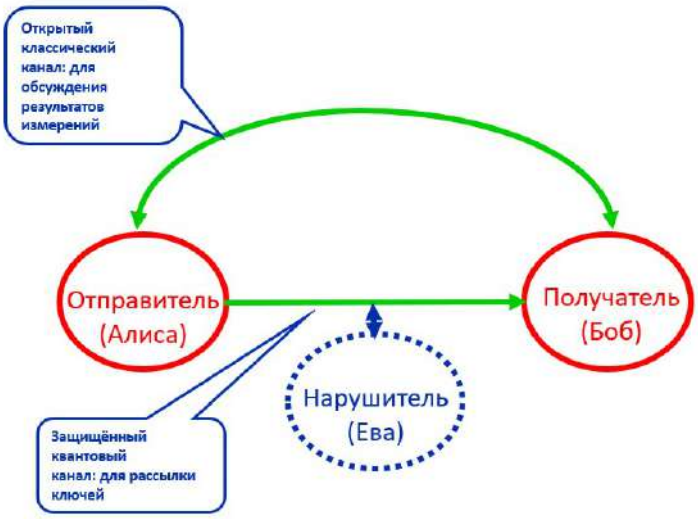


Рис. 11: Общая схема системы КРК

Квантовая рассылка ключей может проводиться по любому оптическому каналу: стандартному оптоволоконному, атмосферному (в пределах прямой видимости) и спутниковому.

Кодирование квантовых сигналов в КРК может выполняться с помощью различных параметров фотона: поляризации, фазы, времени прихода и других.

Протокол BB84 является исторически первым протоколом КРК, но используется по сей день, в том числе и в коммерческих системах. Этот протокол оперирует четырьмя состояниями фотонов (в примере – поляризационными) в двух базисах (в примере – диагональном и вертикально-горизонтальном).

Алгоритм генерации квантовых ключей (рисунок 12):

1. Участники договариваются, как будут интерпретировать каждое из состояний фотонов (например, 0 для вертикальной поляризации, 1 – для горизонтальной в вертикально-горизонтальном базисе, аналогично для диагонального базиса);

2. Отправитель посылает по квантовому каналу одиночные фотоны получателю в случайно выбранном состоянии (выбирает генератор случайных чисел);

3. Получатель измеряет принимаемые фотоны, случайно выбирая базис для измерений. В итоге у получателя будет находиться «сырой» ключ, содержащий около 25% ошибок;

4. Для каждого переданного состояния получатель по открытому каналу сообщает, в каком базисе проводилось измерение, но не сообщает его результаты;

5. Отправитель по открытому каналу сообщает, в каких случаях выбранное ей состояния фотона «подходило» под базис получателя. Если базисы совпали, то бит оставляют, а если нет, то игнорируют его. Так получается «просеянный» ключ;

6. Процесс повторяется, пока пользователи не получат сырой ключ требуемой длины.

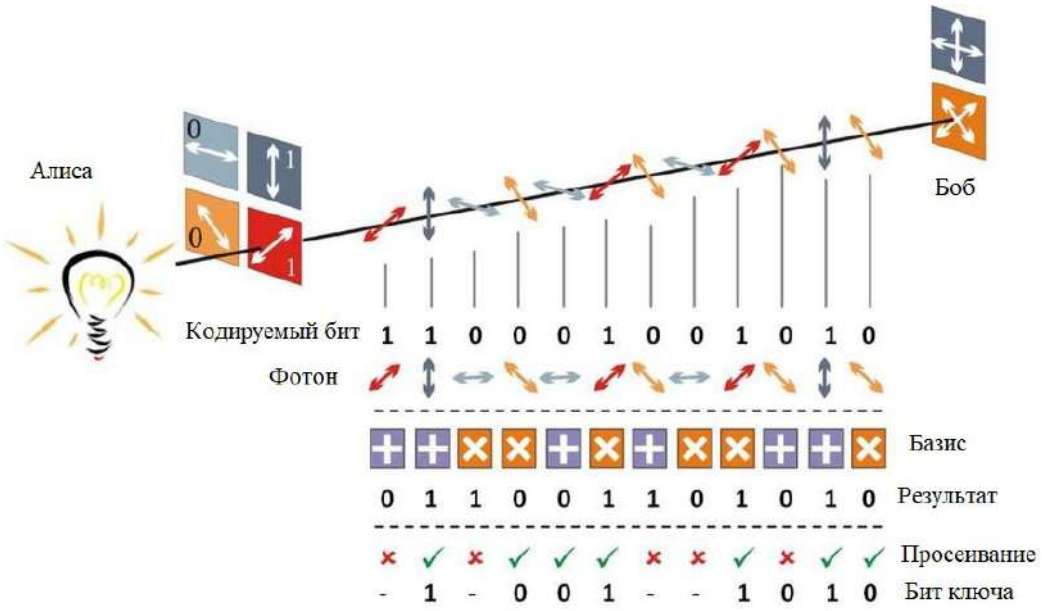


Рис. 12: Алгоритм генерации квантовых ключей

В идеальном случае, при полном отсутствии шумов в системе и подслушивания в канале связи, после просеивания у отправителя и получателя будет находиться коррелированная строка случайных битов. Ошибки, внесённые в просеянный ключ шумами и прослушиванием канала нелегитимным пользователем, могут быть идентифицированы и устранены с помощью специальных математических процедур: исправления ошибок и усиления секретности, если их количество не превышает 11%. В противном случае квантовый канал считается блокированным.

Итоговый ключ, из которого убраны все ошибки и информация, потенциально известная нарушителю, называется «секретным» квантовым ключом. Он удовлетворяет критериям «абсолютно стойкого» ключа.

2.5 Квантовые сети

На основе систем КРК могут быть организованы квантовые сети. Однако при их построении следует учитывать особенности систем квантовой коммуникации, отличающие их от привычной оптической связи:

1. Блоки отправителя и получателя должны быть синхронизированы дополнительным оптическим сигналом

2. Квантовые каналы должны быть полностью оптическими и не допускают промежуточного преобразования сигнала

3. Передача по одному волокну информационного и квантового сигналов на разных длинах волн затруднительна, хотя и принципиально возможна, из-за возникновения “шумовых” фотонов за счёт нелинейных эффектов

4. Предельное расстояние между узлами определяется потерями в канале, так как уровень сигнала на выходе из передатчика не превышает однофотонный, а классическое усиление невозможно

Это объясняет, почему появление первых практических образцов систем квантовой коммуникации в условиях широкого распространения волоконно-оптических линий связи (ВОЛС) не привело к немедленному появлению квантовых сетей.

Сейчас квантовые каналы передают в основном по «тёмным» оптическим волокнам, по которым не идёт передача данных в сети связи.

Поскольку в квантовых сетях невозможно использовать усилители, вместо них применяются доверенные узлы (ретрансляторы КРК), в которых установлены пары устройств КРК (рисунок 13). Внутри доверенного узла происходит расшифровка информации, её шифрование на новом квантовом ключе и передача дальше по сети. Таким же способом можно организовывать резервирование каналов.

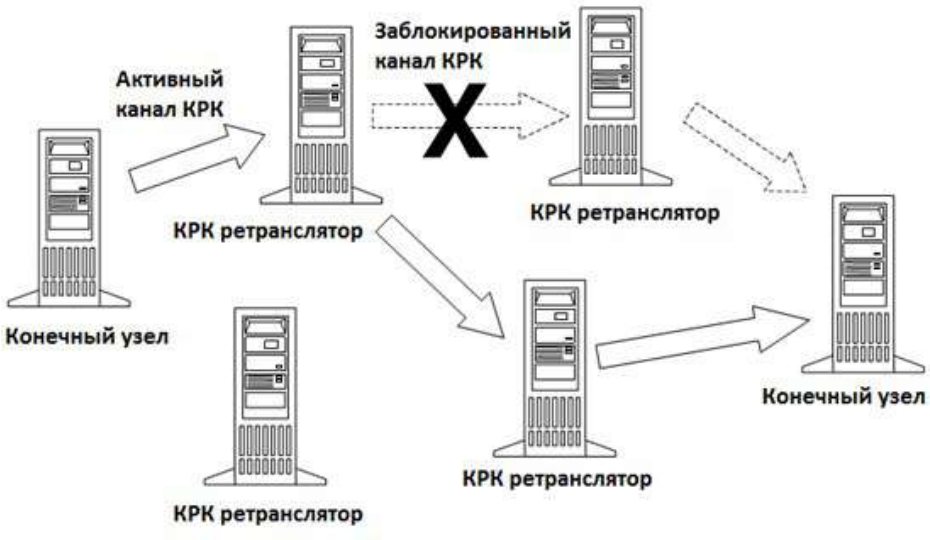


Рис. 13: Передача ключа через доверенные узлы

Путём установки нескольких устройств КРК в доверенных узлах можно строить квантовые сети произвольной топологии (рисунок 14).При этом между каждой парой узлов генерируется свой квантовый ключ. Сетевое распределение ключей (для передачи данных между любой парой пользователей сети) является отдельной задачей, которая должна решаться в системе управления квантовой сетью.

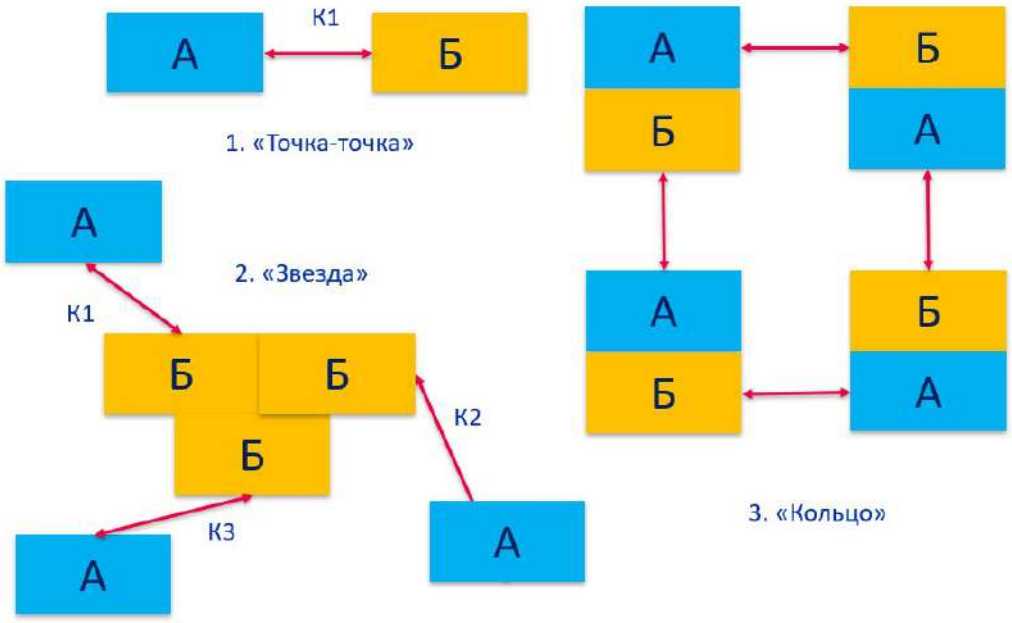


Рис. 14: Виды топологий

Системы КРК позволяют применять частотное и временное мультиплексирование сигналов (рисунок 15). При этом нет ограничений на совместное распространение квантовых сигналов по одному волокну.

Сегодня квантовые сети чаще всего рассматриваются как дополнительный уровень информационной сети: квантовый уровень обеспечивает обновление ключей в крипто маршрутизаторах и остаётся невидимым для конечных пользователей (рисунок 16). Коммутация каналов в квантовой сети может выполняться с помощью оптических переключателей.

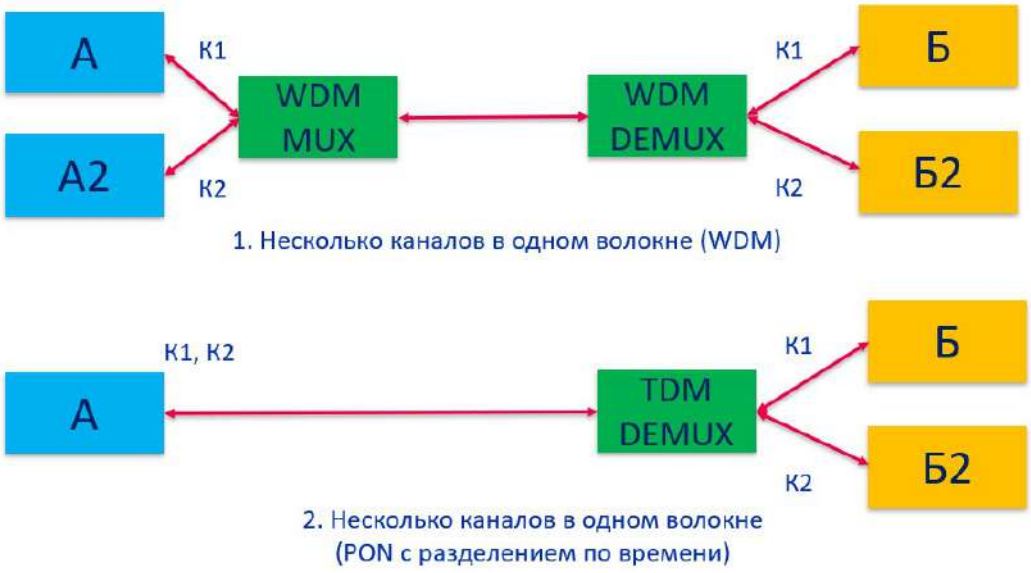


Рис. 15: Мультиплексирование каналов

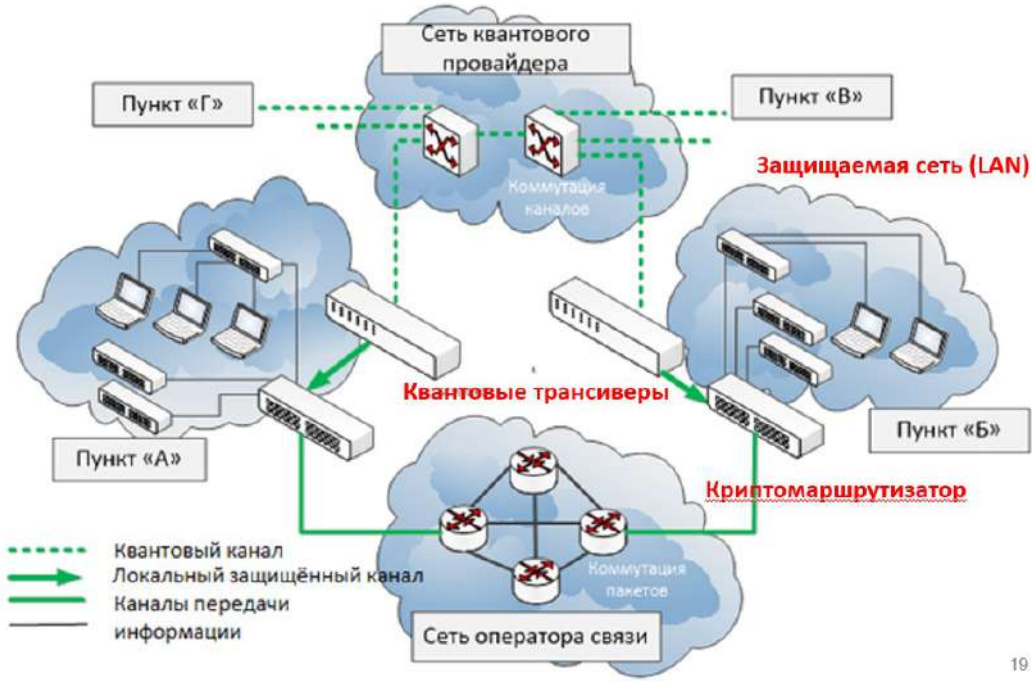


Рис. 16: Квантовая сеть

2.6 Контрольные вопросы

1. Недостатки существующих методов шифрования.
2. Какая криптосхема называется симметричной?
3. Какая криптосхема называется асимметричной?
4. Теорема Моска.
5. Шифр Вернама.
6. Свойства одиночного фотона, используемые в квантовой рассылке ключа.
7. Принцип работы протокола квантовой рассылки ключа BB84.
8. Особенности систем квантовой коммуникации.
9. Топологии квантовых сетей.

3 Источники и детекторы одиночных фотонов

Данный раздел учебного пособия и одноименная лекция составлены на основе обзорной статьи [1]. За подробностями и для более глубоко погружения в тему советуем обратиться к данной статье.

Фотон – элементарное возбуждение одиночной моды квантованного электромагнитного поля. Концепция квантованного электромагнитного поля была предложена Планком в 1900 для объяснения спектра излучения абсолютно черного тела. Эта же концепция была использована Эйнштейном в 1905 году для объяснения фотоэффекта, а также Комптоном в 1923 году для объяснения сдвига длины волны у рассеянных рентгеновских лучей (т.н. комптоновский сдвиг). Термин «фотон» был предложен в 1926 году Льюисом [2], а формальное квантование электромагнитного поля было проведено Дираком в 1927 [3].

Для математического описания одиночного фотона используют оператор рождения. Данный оператор появляется в результате решения уравнения Шредингера для одномерного гармонического осциллятора

$$\Big(-\frac{\hbar^2}{2m}\frac{d^2}{dx^2} + \frac{1}{2}m\omega^2 x^2 \Big)\Psi(x) = E\Psi(x), \tag{47}$$

где $\hbar$ - приведенная постоянная Планка, m - масса частицы, ω - частота колебаний, x - координата, $\Psi(x)$ - волновая функция, связанная с вектором состояния следующим соотношением: $|\Psi\rangle = \int \Psi(x)dx$, E - энергия частицы, а также вводится безразмерные координаты и импульс

$$q = \sqrt{\frac{m\omega}{\hbar}}x, \tag{48}$$

$$p = -i\frac{d}{dq}, \tag{49}$$

соответствующие квадратурам поля. Тогда операторам рождения и уничтожения соответствуют следующие выражения

$$a = \frac{1}{\sqrt{2}}(q + ip), \tag{50}$$

$$a^\dagger = \frac{1}{\sqrt{2}}(q - ip). \tag{51}$$

Данные операторы при действии на произвольное фоковское состояние (т.е. состояние с определенным числом фотонов в моде), соответственно

понижают уровень энергии в данном состоянии или повышают

$$a|n\rangle = \sqrt{n}|n-1\rangle, \tag{52}$$

$$a^\dagger|n\rangle = \sqrt{n+1}|n+1\rangle \tag{53}$$

Таким образом оператор рождения описывает наличие одиночного фотона в моде, действуя на вакуумное состояние

$$a^\dagger|0\rangle = |1\rangle. \tag{54}$$

Также стоит отметить, что операторы рождения и уничтожения не перестановочны, т.е. не коммутируют друг с другом

$$[a, a^\dagger] = aa^\dagger - a^\dagger a = 1. \tag{55}$$

Операторы, коммутирующие на единицу, образуют алгебру Вейля. Алгебраические свойства операторов очень помогают при вычислениях.

Однофотонные состояния света используют в большом числе областей науки и промышленности:

- Квантовая теория информации, включающая квантовую криптографию, квантовую генерацию случайных чисел, симуляцию квантовых процессов и квантовые вычисления и т.д.;
- Медицинские технологии, включая получение изображений различного рода (томографии, рентгеновские снимки и пр.), исследования радиоактивности, микроскопия и т.д.;
- Сенсорика, включая системы наблюдения, улавливание света при низкой освещенности и т.д.;
- Метеорология, включая удаленные климатические измерения, мониторинг окружающей среды, лидары и пр.;
- Физические приложения, включая астрофизику, детектирование ядерных частиц, спектроскопию и пр.;
- Фотоника, включая оптоэлектронику и оптические коммуникации;
- Биотехнологии, включая биолюминесценцию, детектирование одиночных молекул, секвенирование ДНК и т.д.;
- Метрология, включая квантовые стандарты, радиометрические измерения, сверхточные измерения, улучшенные за счет квантовых эффектов и т.п.

3.1 Источники одиночных фотонов

Рассмотрим характеристики идеального источника одиночных фотонов:

- Срабатывание «по запросу» - нажали на кнопку - вылетел фотон, когда нам необходимо;
- 100% эффективность - вылетает фотон всегда, когда мы нажали на кнопку;
- Однофотонность - всегда один фотон, нет многофотонных срабатываний;
- Все фотоны обладают одинаковыми параметрами - длина волны, поляризация, направление;
- Неограниченная (произвольная) скорость генерации;
- Удобство использования - работа при комнатной температуре, малые габариты, устойчивость к воздействиям внешней среды, низкая стоимость и т.д.

Стоит отметить, что идеального источника фотонов не существует. Поэтому всегда стоит хорошо понимать, какие из приведенных выше характеристик наиболее важны в рамках того или иного эксперимента, а какими можно пренебречь.

Для определения однофотонности источника света используют функцию корреляции второго порядка

$$g^{(2)}(\tau) = \frac{\langle a^\dagger(t)a^\dagger(t+\tau)a(t+\tau)a(t)\rangle}{\langle a^\dagger(t)a(t)\rangle^2}. \tag{56}$$

Для истинно однофотонных источников $g^{(2)}(0) = 0$, как показано на рисунке 17. Для когерентного излучения (лазерного) $g^{(2)}(0) = 1$, также для некоторых квантовых состояний света $g^{(2)}(0) > 1$, в таком случае говорят о «слипании» фотонов (bunching).

Функция корреляции второго порядка измеряется на интерферометре Брауна-Твисса, где свет разделяется на два плеча светоделителем, в одном из плечей вводится временная задержка (τ), далее свет регистрируется на детекторах одиночных фотонов в каждом из плечей, а электрические сигналы с них далее идут на коррелятор, который проводит математическую операцию корреляции (аналогично свертке). Впервые такой интерферометр был сооружен для наблюдения за светом звезд.

Существует два основных вида источников одиночных фотонов (за исключением различных экзотических экземпляров):

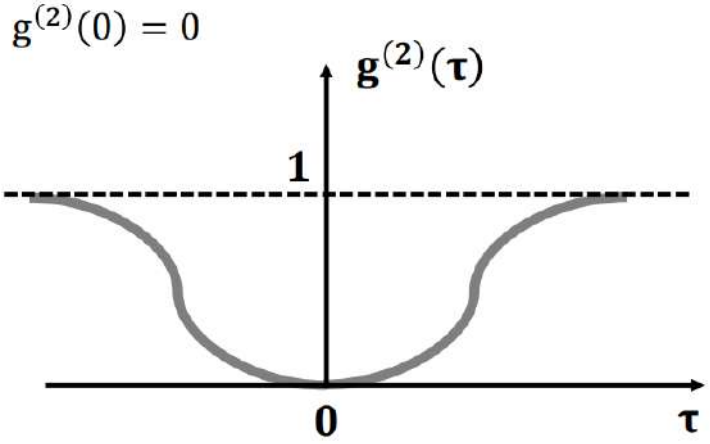


Рис. 17: Типичный вид функции корреляции второго порядка для истинного источника одиночных фотонов

- Атомоподобные источники, включая одиночные атомы, ионы, молекулы, квантовые точки, центры окраски и пр.;
- Параметрические источники, включая основанные на спонтанном параметрическом рассеянии, четырехволновом смешении и т.п.

3.1.1 Атомоподобные источники

Простейшая схема атомоподобного источника представлена на рисунке 18, где за счет сначала перевода атома в возбужденное состояние под действием контрольного излучения, а затем за счет релаксации электрона с возбужденного на основной уровень излучается одиночный фотон. Такая схема имеет ряд недостатков, связанных в основном с тем, что релаксация электрона происходит в случайный момент и параметрами излучения сложно управлять.Поэтому в основном используют схему, показанную на рисунке 19, т.н. Λ-схему, названную из-за расположения энергетических уровней атомоподобной структуры (данная схема упрощена, в действительности схема может содержать промежуточные уровни с переходами без излучения). Данная схема позволяет понять, в какой момент времени система готова к излучению.

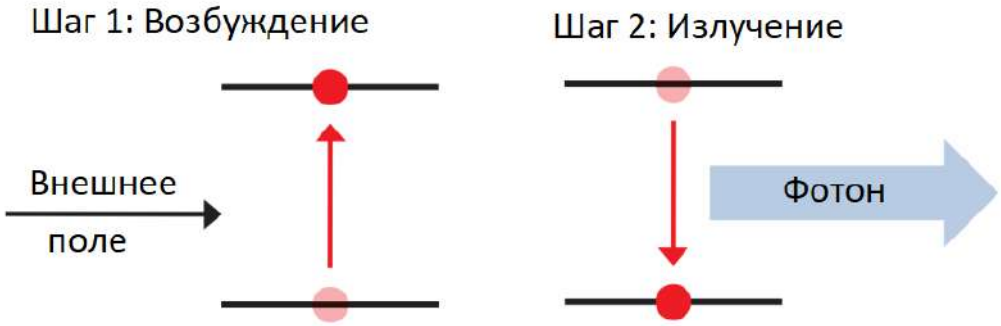


Рис. 18: Схема излучения одиночных фотонов в простейшей атомоподобной структуре. Шаг 1: Возбуждение. Перевод «атома» в возбужденное состояние под действием контрольного излучения. Шаг 2: Излучение. Релаксация электрона с возбужденного на основной уровень с излучением одиночного фотона. [1]

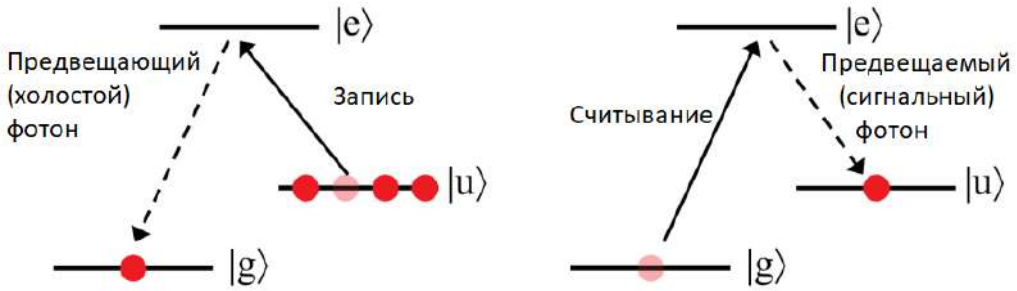


Рис. 19: Схема излучения одиночных фотонов в ансамблевой атомоподобной структуре (Λ-схема). Шаг 1: Запись. Перевод ансамбля из основного состояния $|u\rangle$ в возбужденное состояние $|e\rangle$ под действием контрольного «записывающего» излучения с релаксацией электрона на метастабильный уровень $|g\rangle$. При этом излучается предвещающий (холостой) фотон, детектирование которого говорит нам о том, что ансамбль приготовлен для излучения. Шаг 2: Считывание. Перевод ансамбля из метастабильного состояния $|g\rangle$ в возбужденное состояние $|e\rangle$ под действием контрольного «считывающего» излучения с последующей релаксацией электрона на основного уровень $|u\rangle$. При этом излучается предвещаемый (сигнальный) фотон, направляемый в оптическую схему. [1]

Таким образом, атомоподобные источники одиночных фотонов имеют следующие характеристики:

- Срабатывание «по запросу»;
- Высокая, близкая к 100% эффективность;
- Однофотонность;
- Все фотоны обладают одинаковыми параметрами или близки к этому;
- Скорость генерации невысокая и ограничена временами «чтения» и «записи»;
- Удобства использования практически отсутствуют - работа при криогенных температурах, крупные габариты, высокая стоимость и т.д.

3.1.2 Параметрические источники

Параметрические истоники предсталяют собой специально подготовленный (вырезанный под определенным углом по направлению к оптической оси схемы, т.е. с соблюдением условий фазового синхронизма) нелинейный кристал, в котором под воздействием мощного внешнего лазерного изучения рождаются бифотоны - коррелированные пары фотонов, как проказано на рисунке 20. Один из бифотонов можно регистрировать сразу, в таком случае он будет предвещающим (холостым). Его регистрация будет указывать на то, что в оптической системе находится второй, т.н. сигнальный фотон. Существуют и другие схемы, например схема четырехволнового смешения, где два фотона накачки образуют сигнальные бифотоны с перераспределением энергии фотонов.

Таким образом, источники одиночных фотонов, основанные на параметрических процессах, имеют следующие характеристики:

- Вероятностное срабатывание с предвещением (т.е. регистрация одного события однозначно указывает на другое, в данном случае регистрация холостого фотона однозначно указывает на то, что в системе находится сигнальный фотон);
- Относительно низкая эффективность конверсии фотонов в бифотоны;
- Практически нет многофотонных преобразований;

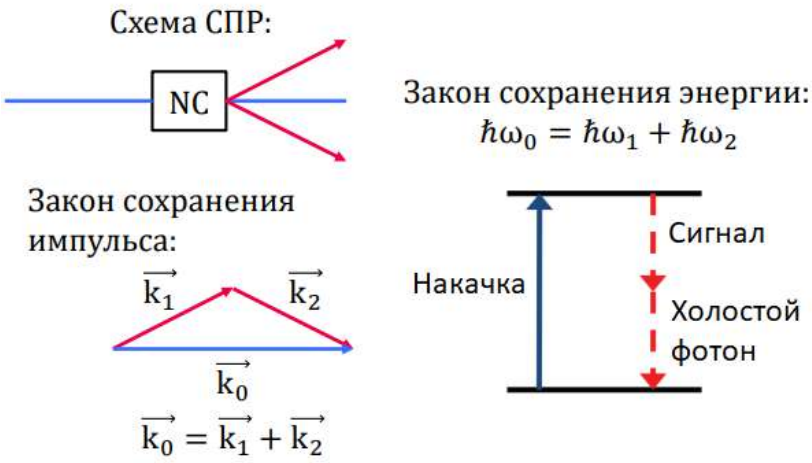


Рис. 20: Принципиальная схема спонтанного параметрического рассеяния, а также демонстрация законов сохранения импульса и энергии (в упрощенном виде)

- Все фотоны обладают одинаковыми параметрами или близки к этому, более того бифотоны могут быть квантово перепутаны между собой;
- Скорость генерации высокая, до десятков-сотни МГц;
- Удобства использования - работа при комнатной температуре, относительно малые габариты (зависит от точности юстировки), относительно невысокая стоимость и т.д.

3.1.3 Ослабленное лазерное излучение

Лазерное илучение может быть описано на квантовом языке следующим образом

$$|\alpha\rangle = e^{-\frac{|\alpha|^2}{2}} \sum_{n=0}^{\infty} \frac{\alpha^n}{\sqrt{n!}} |n\rangle, \tag{57}$$

где α - комплексная (учитывающая фазу) амплитуда, $|\alpha|^2$ - мощность излучения, $|n\rangle$ - фоковское состояние с n фотонов. Данное состояние получается за счет действия оператора смещения на вакуумное состояние

$$D(\alpha)|0\rangle = e^{\alpha a^\dagger - \alpha^* a}|0\rangle = |\alpha\rangle. \tag{58}$$

Как видно, данное состояние описывается взвешенной суперпозицией фоковских состояний, т.е. при измерении мы можем вероятностно обнаружить разное число фотонов. Вероятность определения n фотонов в когерентном состоянии описывается распределением Пуассона

$$P(n) = \frac{(|\alpha|^2)^n}{n!} e^{-|\alpha|^2}, \tag{59}$$

$$\sum_{n=0}^{\infty} P(n) = 1, \tag{60}$$

$$P(n > 1) = 1 - P(0) - P(1). \tag{61}$$

таким образом, при $|\alpha|^2 < 1$ (мощность порядка 13 пВт для длины волны 1550 нм и временного окна порядка 10 нс) вероятность обнаружить большое число фотонов мало, в то время как вероятность обнаружить один фотон, относительно велика. Ослабленное лазерное излучение в некоторых случаях можно с натяжкой (для определенных экспериментов) считать однофотонным, т.е. псевдооднофотонным источником излучения.

Таким образом, квазиоднофотонные источники имеют следующие характеристики:

- Вероятностное срабатывание (за счет высокой $P(0)$);
- Нет предвещения;
- Есть многофотонные преобразования ($P(n > 1)$);
- Все фотоны обладают одинаковыми параметрами или близки к этому;
- Скорость генерации не ограничена;
- Удобства использования максимальные - работа при комнатной температуре, малые габариты, невысокая стоимость и т.д.

3.1.4 Фазомодулированное ослабленное лазерное излучение

Частным случаем ослабленного лазерного излучения является фазомодулированное лазерное излучение (подробнее в методических указаниях к виртуальной лабораторной работе «Квантовое распределение ключа на боковых частотах фазомодулированного излучения»). В данном разделе рассмотрим подробнее процесс фазовой модуляции (в классическом приближении, в квантовом случае процесс фазовой модуляции описан в [4]). Для этого сначала рассмотрим монохроматическое излучение вида

$A(t) = A_0 e^{i\omega t}$, где A_0 – комплексная амплитуда, ω - частота излучения. Процесс модуляции можно представить в виде гармонически изменяющегося показателя преломления в кристалле, дающего соответствующий гармонически меняющийся сдвиг фазы $e^{im\sin(\Omega t+\phi_A)}$, где m – индекс модуляции (пропорционален амплитуде модулирующего сигнала), Ω – частота модулирующего сигнала, ϕ_A – фаза модулирующего сигнала. Применяя разложение Якоби-Ангера, модулированный сигнал принимает следующий вид

$$\begin{aligned} A(t)e^{im\sin(\Omega t+\phi_A)} &= A(t)\sum_{n=-\infty}^{\infty} J_n(m)e^{i(\Omega t+\phi_A)n} \\ &= \sum_{n=-\infty}^{\infty}[A_0 J_n(m)]e^{i(\omega+\Omega n)t+i\phi_A n}, \end{aligned} \tag{62}$$

где $J_n(m)$ – функция Бесселя первого рода n-го порядка. Таким образом, получаем излучение на частотах $\omega + \Omega n$ с амплитудой $A_0 J_n(m)$. Определим частоту ω (при $n = 0$) как центральную, а совокупность частот $\omega + \Omega n$ (при $n \neq 0$) – как боковые.

Мощность излучения может быть найдена в виде модуля квадрата амплитуды $|A_0|^2$. Зная мощность излучения, можно рассчитать среднее число фотонов в посылке (имеется в виду либо импульс, если лазер работает в импульсном режиме, или же просто определенный временной отрезок, если речь о непрерывном излучении) $\mu_0 = |A_0|^2\Delta T/(\hbar\omega)$, где ΔT – временное окно излучения (одной посылки), $\hbar$ – приведенная постоянная Планка. Таким образом, среднее число фотонов на каждой из частот может быть выражено в виде $\mu_0 J_n^2(m)$. В свою очередь, используя тождество $\sum_{n=-\infty}^{\infty} J_n^2(m) = 1$, суммарное среднее число фотонов на всех боковых частотах $\mu = \mu_0(1 - J_0^2(m))$ зависит от начального μ_0 и индекса модуляции m. Таким образом, подбирая индекс модуляции, мы можем обеспечить псевдооднофотонность на боковых частотах. А преимущество фазовой модуляции заключается в том, что при распространении вся фазовая информация записана не во временной, а в частотной области, которая намного более устойчива к воздействиям внешней среды.

Рассмотрим также случай повторной модуляции с фазой модулиру-

ющего сигнала ϕ_B

$$
\begin{aligned}
&A(t)e^{im\sin(\Omega t+\phi_A)}e^{im\sin(\Omega t+\phi_B)} = \\
=&A(t)e^{i2m\cos(\frac{\phi_A-\phi_B}{2})\sin(\Omega t+\frac{\phi_A+\phi_B}{2})} = \\
=&A(t)\sum_{n=-\infty}^{\infty} J_n\left(2m\cos(\frac{\phi_A-\phi_B}{2})\right)e^{i(\Omega t+\frac{\phi_A+\phi_B}{2})n} = \\
=&\sum_{n=-\infty}^{\infty}[A_0 J_n\left(2m\cos(\frac{\phi_A-\phi_B}{2})\right)]e^{i(\omega+\Omega n)t+i\frac{\phi_A+\phi_B}{2}n}. \qquad (63)
\end{aligned}
$$

Таким образом, получаем излучение на боковых частотах $\omega+\Omega n$ с амплитудой $A_0 J_n(\tilde{m})$, где $\tilde{m} = 2m\cos(\frac{\phi_A-\phi_B}{2})$. Значение амплитуды зависит от разности фаз модулирующих сигналов $\phi_A - \phi_B$, происходит аналог интерференции. При разнице фаз $\phi_A - \phi_B = 0$ индекс модуляции увеличивается (с m до $2m$), соответственно, энергия с центральной моды (при $n = 0$) дополнительно перетекает на боковые моды. При разнице фаз $\phi_A - \phi_B = \pi$ индекс модуляции зануляется, приводя к возвращению всей энергии в центральную моду. Среднее число фотонов на боковых и центральной частотах равны $\mu_0(1 - J_0^2(\tilde{m}))$ и $\mu_0 J_0^2(\tilde{m})$ соответственно.

3.2 Детекторы одиночных фотонов

Рассмотрим характеристики идеального детектора одиночных фотонов:

- 100% квантовая эффективность, т.е. всегда получаем сигнал при попадании фотона на чувствительную поверхность детектора;
- Отсутствие темновых (ложных) срабатываний, т.е. срабатываний, когда чувствительная поверхность детектора закрыта;
- Отсутствия «мертвого» времени, т.е. времени на восстановление детектора после регистрации фотона;
- Отсутствие дрожания фазы или т.н. джиттера, т.е. неопределенности времени регистрации фотона;
- Удобство использования - работа при комнатной температуре, малые габариты, устойчивость к воздействиям внешней среды, низкая стоимость и т.д.;
- Опционально: различение числа фотонов при регистрации.

Стоит отметить, что идеального детектора одиночных фотонов не существует. Поэтому всегда стоит хорошо понимать, какие из приведенных выше характеристик наиболее важны в рамках того или иного эксперимента, а какими можно пренебречь.

3.2.1 Детектор одиночных фотонов на основе лавинного фотодиода

Данный детектор представляет собой полупроводниковую структуру, к которому подведено напряжение смещения. Таким образом, фотон, попадающий на поверхность детектора, выбивает электрон из решетки полупроводника, который ускоряется во внешнем поле вглубь полупроводника. Там происходит каскад столкновений ускоренного свободного электрона с другими электронами решетки. Последние также выбиваются, ускоряются и инициируют следующие столкновения. Таким образом рождается электронная лавина (схематично показана на рисунке 21), т.е. кратковременный скачок тока. По данному скачку тока и определяется регистрация фотона.

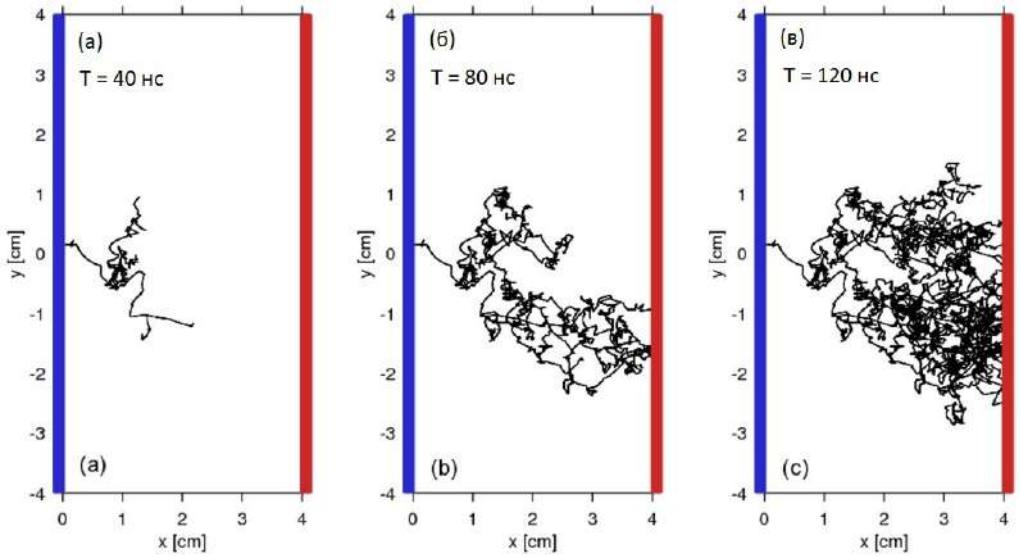


Рис. 21: Результат моделирования двумерной электронной лавины в лавинном фотодиоде, аналогичной лавине при регистрации фотона, рисунки соответствуют разным временам: (а) 40 нс, (б) 80 нс, (в) 120 нс

Данные детекторы обладают средними характеристиками. При этом мертвые времена довольно большие, т.к. детектору необходимо достаточно большое время (порядка единиц-десятков мс) для того, чтобы вторич-

ные лавины с меньшими амплитудами скачков тока сошли на нет. Тем не менее, простота и удобство в использовании, а также работа при комнатных температурах (сам полупроводник зачастую охлаждается пьезоэлементом) делают данный вид детекторов крайне широко распространенными.

3.2.2 Детектор, использующий сенсор, реагирующий на предельные переходы из проводящего режима в сверхпроводящий

Данный тип детекторов представляет из себя ультрачувствительный термометр, т.е. болометр, работающий при криогенных температурах порядка десятых Кельвина. В данном диапазоне температур материал болометра становится сверхпроводником, и установку настраивают таким образом, чтобы температура была слегка ниже предельного перехода (из проводящего режима в сверхпроводящий), а нагрева за счет поглощения одного фотона хватило бы для вывода сенсора из сверхпроводящего режима. Тогда при переходе ток уменьшается за счет увеличения сопротивления, а в параллельном подключении увеличивается, за счет чего и происходит регистрация фотона. На рисунке 22 показана типичная зависимость сопротивления от температуры в рассматриваемом сенсоре.

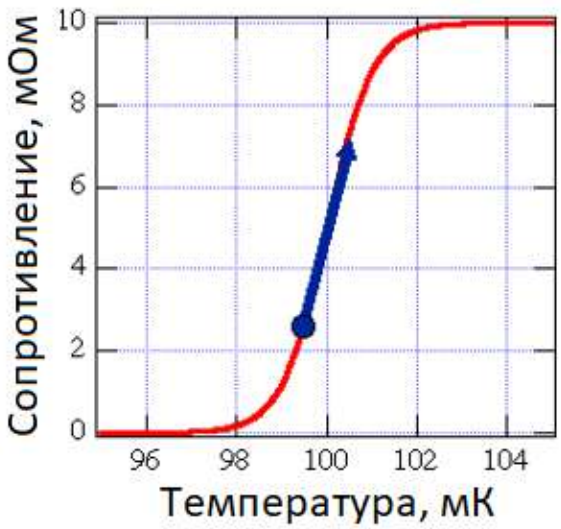


Рис. 22: Типичная зависимость сопротивления от температуры в сенсоре. Малое изменение температры дает значительное изменение сопротивления

Данный вид регистрации фотонов обладает высокой чувствительностью, тем не менее, очевидно, что обеспечение столь низких температур является отдельной довольно сложной инженерной задачей, в связи с чем данный вид детекторов является довольно специализированным.

3.2.3 Сверхпроводящий детектор, использующий туннельный эффект Джозефсона

Данный детектор представляет собой два сверхпроводника, разделенные тонким слоем диэлектрика, т.н. соединение Джозефсона, как показано на рисунке 23, где происходит одноименный эффект тунеллирования. Фотон, попадающий на поверхность элемента, разбивает сверхпроводящую куперовскую пару электронов на два свободных, которые и туннелируют через тонкий слой диэлектрика (куперовские пары не могут этого сделать). Таким образом, наблюдается небольшой ток в отсутствии внешнего напряжения, как показано на вольт-амперной характеристике на рисунке 24.

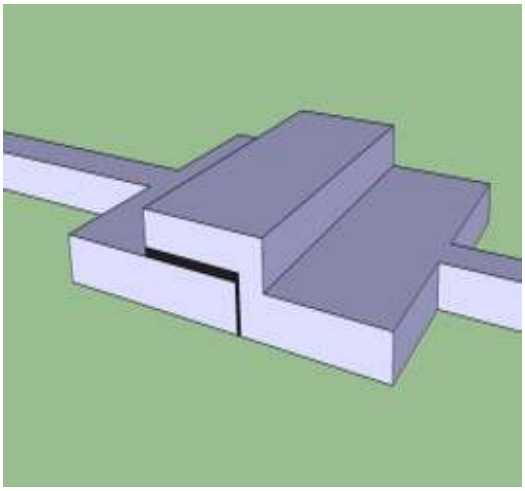


Рис. 23: Схематическое изображение соединения Джозефсона: серым показан сверхпроводник, черным – диэлектрик

Детектор, использующий туннельный эффект Джозефсона, имеет высокую скорость срабатывания, что позволяет обнаруживать фотоны, следующие с высокой частотой. Однако данный детектор дорогой и требует дорогостоящего обслуживания и сопутствующей техники, что может ограничить распространенность данного типа детекторов.

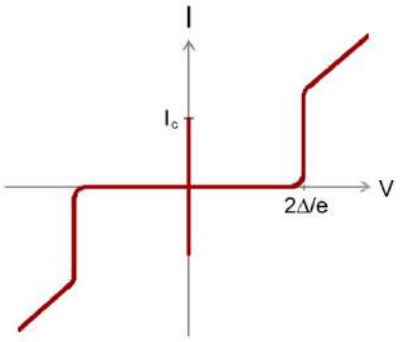


Рис. 24: Вольт-амперная характеристика Джозефсоновского соединения: наблюдается небольшой ток в отсутствии внешнего напряжения за счет тунеллировавших электронов, полученных за счет поглощения фотона куперовской парой

3.2.4 Детектор, основанный на квантово-точечном полевом транзисторе

Обычный полевой транзистор представляет из себя по сути обычный транзистор, в котором управляющий электрический вход заменен на световой, т.е. наличие или отсутствие света определяет уровень тока в транзисторе (рисунок 25). В отличие от обычного полевого транзистора, в данном случае световым управляющим входом является тонкий слой квантовых точек. Квантовая точка, поглощая фотон, сильно изменяет электрические свойства вокруг себя, действуя на соседние квантовые точки. Таким образом, по изменению тока в транзисторе можно определить регистрацию фотона.

С одной стороны, данный детектор работает с низкими энергозатратами, что делает его экономичным в обслуживании, а также имеет простые установку и управление, что делает его простым в использовании. Однако сам по себе детектор как продукт является достаточно дорогим, что может сделать его недоступным для некоторых приложений. Еще одним недостатком является ограниченный угол обзора, что существенно снижает его эффективность.

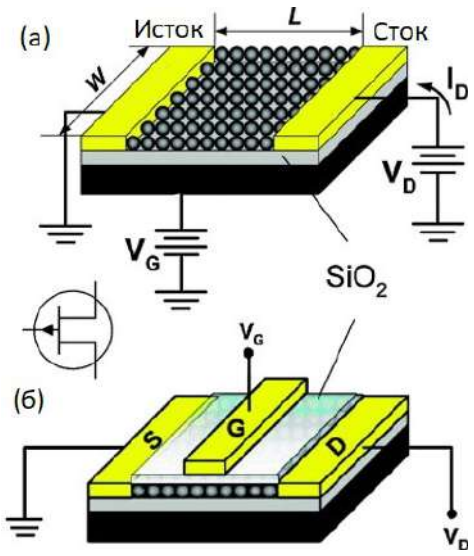


Рис. 25: Схематическое изображение квантово-точечного полевого транзистора, (а) без полевого контакта, где виден массив квантовых точек, (б) с полевым контактом, т.е. собранное устройство в конечном виде. На рисунке W - ширина массива квантовых точек, L - длина массива квантовых точек, I_D и V_D - ток и напряжение на стоке, V_G - напряжение на полевом контакте

3.2.5 Детектор одиночных фотонов, использующий сверхпроводящие наноразмерные волокна

Основным элементом данного детектора является уложенное «змейкой» волокно из нитрида ниобия (как показано на рисунке 26). Данный материал обладает сверпроводимостью при температурах ниже порядка $15K$ (зависит от состава примесей).

Принцип работы детектора схематично показан на рисунке 27. При попадании фотона на поверхность волокна там образуется «горячее пятно», вышедшее из сверхпроводящего режима. Плотность тока по бокам «горячего пятна» увеличивается, что также нагревает эти участки и выводит из сверхпроводящего режима. Таким образом, ток в волокне уменьшается, а в параллельно подключенной схеме – увеличивается. Через некоторое время (порядка десятков наносекунд) волокно снова охлаждается и входит в сверхпроводящий режим.

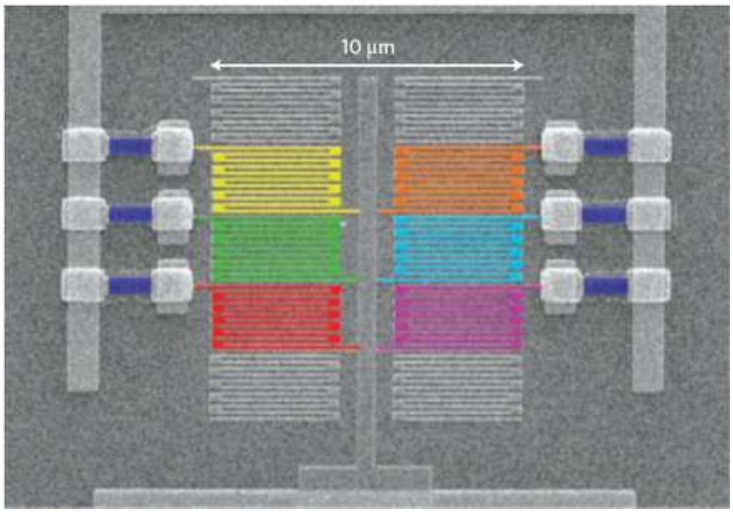


Рис. 26: Изображение регистрирующей поверхности детектора, полученное с помощью электронного микроскопа. Цветами выделены сверхпроводящие нановолокна — основной элемент детектора

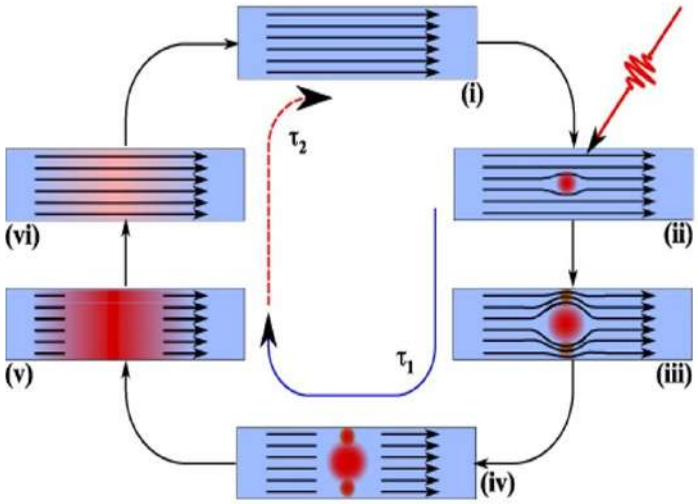


Рис. 27: Схематическое изображение работы детектора, использующего сверхпроводящие наноразмерные волокна, характерное время возбуждения τ_1 порядка единиц нс, характерное время релаксации τ_2 порядка десятков нс. Черными стрелками отображен электрический ток, красным отображены «горячие пятна», чем ярче цвет, тем выше температура

Стоит отметить, что мертвое время данного детектора значительно ниже, чем у лавинного фотодиода. Также данный детектор обладает высокой эффективностью, но необходимо охлаждение до криогенных температур (автоклав с жидким гелием). Тем не менее, характеристики волокон деградируют со временем, и средняя продолжительность службы такого детектора составляет 3-5 лет.

3.3 Контрольные вопросы

1. Математическое описание одиночного фотона.
2. Характеристики идеального источника одиночных фотонов.
3. Схема излучения одиночных фотонов в простейшей атомоподобной структуре.
4. Схема излучения одиночных фотонов в ансамблевой атомоподобной структуре.
5. Основные виды источников одиночных фотонов.
6. Характеристики атомоподобных источников одиночных фотонов.
7. Характеристики параметрических источников одиночных фотонов.
8. Характеристики квазиоднофотонных источников фотонов.
9. Характеристики идеального детектора одиночных фотонов.
10. Принцип работы детектора одиночных фотонов на основе лавинного фотодиода.
11. Принцип работы детектора, использующего сенсор, реагирующий на предельные переходы из проводящего режима в сверхпроводящий.
12. Принцип работы сверхпроводящего детектора, использующего тунельный эффект Джозефсона.
13. Принцип работы детектора, основанного на квантово-точечном полевом транзисторе.
14. Принцип работы детектора одиночных фотонов, использующего сверхпроводящие наноразмерные волокна.

4 Введение в квантовую теорию информации

4.1 Введение

Основной целью данной лекции является первичное знакомство с такой областью современной науки, как квантовая теория информации. Квантовая теория информации (КТИ) – новая дисциплина, которая изучает общие закономерности передачи, хранения и преобразования информации в системах, подчиняющихся законам квантовой механики. Как нетрудно догадаться из названия, основой для этой науки послужили классическая теория информации и квантовая механика. Математическими основами КТИ можно считать следующие концепции: матричный и операторный анализ, некоммутативная теория вероятностей и энтропийные (информационные) характеристики квантовых систем.

КТИ является активно развивающейся областью науки, которая объединяет как квантовые вычисления, так и квантовую коммуникацию. В частности, исследуются основные закономерности в теоретическом описании различных алгоритмов обработки квантовой информации, квантового распределения ключей, квантовой телепортации, сверхплотного кодирования и т.д. Помимо этого, оба эти направления объединены и другой областью КТИ, а именно изучением декогеренции. Декогеренция – процесс изменения свойств квантовых систем во времени вследствие взаимодействия с окружающей средой. Декогеренция является нагляднейшим проявлением неидеального реального мира, который влияет на работу абсолютно всех алгоритмов.

Основной единицей измерения в квантовой теории информации являются квантовые биты, или кубиты. Они являются прямым аналогом битов в классической теории информации. Классические биты могут принимать только два значения – либо 0, либо 1. Это понятие впервые ввел Клод Элвуд Шеннон (30 апреля 1916 года – 24 февраля 2001). Напротив, кубиты могут быть любой комбинацией нуля и единицы с различными вероятностями. Такое состояние называется суперпозиционным и является одним из наиболее важных принципов квантвой механики, используемых в КТИ. Хорошей иллюстрацией для описания этого принципа является мысленный эксперимент с котом Шрёдингера. Давайте рассмотрим более добрую версию эксперимента, представим, что в коробку залезла кошка и коробка закрылась. Пока мы не откроем коробку, для нас кошка как будто одновременно может как спать, так и бодрствовать с различными вероятностями – это квантовое представление, которое

и называется суперпозицией. И только, когда мы откроем коробку, мы увидим, в каком же действительно состоянии она пребывает, тем самым получив классическую информацию, разрушив суперпозицию двух противоположных состояний.

Основной мерой количества информации как в классической, так и в квантовой теории, принято считать энтропию. Этот термин применительно к информации был также впервые введён Шенноном и использовался для оценки количества информации. Помимо этого, Шеннон показал эквивалентность энтропии мере неопределённости информации в передаваемом сообщении. На основе этой введенной характеристики был получен один из величайших результатов Шеннона – он сформулировал понятие пропускной способности канала. Пропускной способностью канала принято называть предельное количество информации в пересчете на один бит, которое можно достоверно передать через канал связи. В отличие от классической теории информации, где пропускная способность имеет только один вид, пропускная способность в КТИ бывает различной и зависит от того, какой тип информации мы хотим передать с помощью квантовых систем.

Предельное количество квантовой информации, которое можно передать по квантовому каналу связи, тесно связано с наличием такого эффекта, как запутанность. Квантовой запутанностью (сцепленностью) называют квантовомеханическое явление, при котором квантовые состояния двух или большего числа объектов оказываются взаимосвязанными. Одними из первых, кто задумался о подобного рода эффектах, были трое ученых – Эйнштейн, Подольский и Розен. И, как им показалось, они даже усмотрели в существовании подобных систем некоторый парадокс. Данный парадокс заключался в следующем: если разнести две связанные (запутанные) частицы на любое расстояние и померить одну из них, то мы моментально узнаем состояние второй частицы. А это значит, что информация как будто передается быстрее скорости света, что порождает явный парадокс. Однако на деле никакого парадокса нет, информация в данном случае не передается быстрее скорости света, просто мы работаем не с двумя отдельными системами, а с одной, состоящей из двух частей.

Еще одним важным эффектом по сравнению с классической информацией является невозможность копирования неизвестного квантового состояния. В классическом случае копирование даже неизвестной информации реализуется достаточно просто. В случае с квантовой информацией вступает в дело теорема о запрете клонирования неизвестного квантового состояния. Математическая интерпретация данной теоремы будет дана далее.

4.2 Математика квантовой теории информации

4.2.1 Базовые определения

В данном разделе будут введены минимальные основные математические определения, необходимые для дальнейшего понимания материала курса.

Прежде всего необходимо рассмотреть простейший способ описания квантовых состояний. Принято считать, что квантовые состояния могут быть описаны с помощью векторов состояний, бра- и кет-векторов. Для этого необходимо определить пространство, в котором лежат векторы.

Пусть $\mathcal{H}$ – конечномерное векторное пространство над полем комплексных чисел с определенным скалярным произведением $\langle \cdot, \cdot \rangle : \mathcal{H} \times \mathcal{H} \to \mathbb{C}$, тогда $\mathcal{H}$ – гильбертово пространство. Двойственное пространство (сопряжённое пространство) к $\mathcal{H}$ – пространство линейных функционалов из $\mathcal{H}$ в $\mathbb{C}$. В данной работе использован формализм Дирака с бра– и кет–веторами для описания элементов пространства $\mathcal{H}$ и двойственного к нему, $\mathcal{H}^*$. Каждый кет–вектор, $|\psi\rangle \in \mathcal{H}$, имеет единственный соотвествующий ему двойственный(сопряженный) бра–вектор, $\langle\psi| \in \mathcal{H}^*$. Бра–вектор выражается через кет–ветор и скалярное произведение на гильбертовом пространстве как

$$\langle\psi| : |\varphi\rangle \mapsto \langle\psi|\varphi\rangle := \langle\langle\psi|, |\varphi\rangle\rangle. \tag{64}$$

Скалярное произведение в данном пространстве удовлетворяет следующим свойствам:

- скалярное произведение сопряженно-симметрично: $\langle\psi|\varphi\rangle = \langle\bar{\varphi}|\psi\rangle$;
- скалярное произведение положительно определено: $\langle\psi|\psi\rangle \geq 0$ ($\langle\psi|\psi\rangle = 0$ только если $|\psi\rangle = 0$)

Прежде всего, необходимо определить элементы, составляющие поле. Таким элементами будут являться комплексные числа $c = a + ib$, такие, что $c \in \mathbb{C}$, где $a, b \in \mathbb{R}$, $i = \sqrt{-1}$, тогда $c^* = a - ib$ – комплексно сопряженное к нему.

Определение № 1: Пусть кет-вектор, $|\cdot\rangle$, представляет собой d-размерный вектор-столбец в комплексном векторном пространстве $\mathbb{C}^d$, тогда бра-вектор, $\langle\cdot|$, — d-размерный вектор-строка, соответствующий комплексному сопряжению кет-вектора и имеющий вид $\langle\cdot| = ((|\cdot\rangle)^*)^T$, где *– комплексное сопряжение, а T – транспонирование.

Пример № 1: Пусть $|v\rangle \in \mathbb{C}^2$ – вектор в двумерном векторном пространстве, имеющий следующий вид

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

$$\langle v| = ((|0\rangle)^*)^T = \begin{pmatrix} 1^* \\ 0^* \end{pmatrix}^T = \begin{pmatrix} 1 & 0 \end{pmatrix}.$$

Определение № 2(абсолютное значение комплексного числа): Пусть $c \in \mathbb{C}$ –комплексное число и имеет вид $c = a + ib$, где $a, b \in \mathbb{R}$. Абсолютным значением, или модулем, с называют

$$|c| = \sqrt{c^* c} = \sqrt{a^2 + b^2} \tag{65}$$

Пример № 2:

$$c = 1 + i2 \Rightarrow |c| = \sqrt{1^2 + 2^2} = \sqrt{5}$$

Определение № 3(скалярное произведение): Пусть есть два d-размерных вектора

$$|v_1\rangle = \begin{pmatrix} a_1 \\ \vdots \\ a_2 \end{pmatrix}, |v_2\rangle = \begin{pmatrix} b_1 \\ \vdots \\ b_2 \end{pmatrix} \tag{66}$$

тогда скалярное произведение этих векторов есть не что иное как $\langle v_1|v_2\rangle := \langle v_1||v_2\rangle = \sum_{i=1}^{d} a_i^* b_i$. Необходимо отметить, что скалярное произведение двух векторов $|v_1\rangle, |v_2\rangle \in \mathbb{C}^d$ является в общем виде комплексным числом.

Пример № 3: Пусть есть два вектора

$$|v\rangle = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ i \end{pmatrix}, |w\rangle = \frac{i}{\sqrt{2}} \begin{pmatrix} 1 \\ 1 \end{pmatrix},$$

тогда

$$\langle v|w\rangle = \frac{i}{2} \begin{pmatrix} 1 & -i \end{pmatrix} \cdot \begin{pmatrix} 1 \\ 1 \end{pmatrix} = \frac{1+i}{2}, \quad \langle w|v\rangle = \frac{-i}{2} \begin{pmatrix} 1 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 \\ i \end{pmatrix} = \frac{1-i}{2},$$

$$\langle w|v\rangle = \overline{\langle v|w\rangle}.$$

Определение № 4(длина вектора): Пусть имеется вектор

$$|v\rangle = \begin{pmatrix} a_1 \\ \vdots \\ a_d \end{pmatrix},$$

тогда длина вектора имеет следующий вид

$$\||v\rangle\|_2 = \sqrt{\langle v|v\rangle} = \sqrt{\sum_{i=1}^{d} a_i^* \cdot a_i} = \sqrt{\sum_{i=1}^{d} |a_i|^2}. \tag{67}$$

Если $\||v\rangle\|_2 = 1$, то принято говорить, что вектор $|v\rangle$ имеет норму 1, или же просто нормирован.

Пример № 4: Пусть существует вектор $|v\rangle \in \mathbb{C}^2$, такой, что

$$|v\rangle = \frac{1}{2}\begin{pmatrix} 1+i \\ 1-i \end{pmatrix},$$

тогда его длина равна

$$\||v\rangle\|_2 = \sqrt{\frac{1}{4} \cdot 2 \cdot (1+i) \cdot (1-i)} = \sqrt{\frac{1}{2} \cdot 2} = 1.$$

Когда речь заходит о векторах, логично предположить, что возможно существование вектора следующего вида $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$. Подобное описание вектора есть не что иное, как представление **квантового бита (кубита)**. Вместо того, чтобы находиться строго в состоянии "0" либо строго в состоянии "1", кубит находится в *суперпозиционном состоянии*. Представляя биты в виде векторов, можно сказать, что квантовый бит может быть описан как $|v\rangle \in \mathbb{C}^2$.

Определение № 5(квантовый бит): Чистое состояние кубита может быть представлено как двумерный кет-вектор $|\psi\rangle \in \mathbb{C}^2$, имеющий вид $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$, где $\alpha, \beta \in \mathbb{C}$, и $|\alpha|^2 + |\beta|^2 = 1$. Условия на α, β говорят о том, что вектор $|\psi\rangle$ нормирован.

В предложенном представлении кубита предлагается использовать для описания классических бит векторы $|0\rangle$ и $|1\rangle$. Необходимо отметить, что данные векторы являются ортонормированными, что может быть выражено на квантовом языке как $\langle 1|0\rangle = 0$, тогда как $\langle 1|1\rangle = \langle 0|0\rangle = 1$. Таким образом, данные векторы, $|0\rangle$ и $|1\rangle$ составляют базис в $\mathbb{C}^2$, и любой вектор $|v\rangle \in \mathbb{C}^2$ может быть представлен как $|v\rangle = \alpha|0\rangle + \beta|1\rangle$, где α, β – некоторые комплексные коэффициенты.

Определение № 6(стандартный базис): Пусть $\mathbb{C}^2$ – двумерное комплексное векторное пространство, тогда стандартный базис (вычислительный базис) – $\mathscr{I} = \{|0\rangle, |1\rangle\}$ – является ортонормальным базисом этого пространства с базисными векторами

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

Безусловно, данный базис не является единственным, и можно подобрать бесконечно много других различных базисов.

4.3 Формализм матриц плотности

Хорошо известно, что квантовые состояния можно описывать с помощью векторов состояний. Тогда чистое состояние кубита может быть представлено как двумерный кет-вектор $|\psi\rangle \in \mathbb{C}^2$, имеющий вид $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$, где $\alpha, \beta \in \mathbb{C}$, и $|\alpha|^2 + |\beta|^2 = 1$. Условия на α, β говорят о том, что вектор $|\psi\rangle$ нормирован.

Начнем с исследования более общего формализма для записи квантовых состояний. Существуют две причины для его введения.

Представим, что у нас есть дискретная случайная переменная X, принимающая одно из значений алфавита $\mathscr{X}$ размера n. Тогда пусть $p(X)$ – распределение дискретной случайной величины X, $|X|$ – размерность алфавита, используемого в X, а $Prob(X = x)$ – вероятность того, что случайная величина принимает значение $x \in \mathscr{X}$. Иногда для упрощения будет использоваться $p_x = p(x) = Prob(X = x)$.

Распределение $p(X)$ определено набором неотрицательных вероятностей, а именно $\forall x \in \mathscr{X}$, $p_x \geq 0$. Более того, $p(X)$ должно быть нормированно, а значит $\sum_{x \in \mathscr{X}} p_x = 1$.

Важно понимать, что случайная величина X может быть скоррелирована со случайной величиной Y. Это значит, что у них есть совместное распределение $p(XY)$, которое в общем виде не обязательно является их прямым произведением $p_{xy} \neq p_x p_y$. Это подводит нас к понятию условной вероятности $P(X|Y)$, где $Prob(X = x|Y = y)$ — вероятность того, что случайная величина X принимает значение x, при условии что Y принимает значение y.

Однако подобного формализма недостаточно для описания квантовых состояний системы, а следовательно, требуется более общий подход. В частности, классическое описание вероятностей не позволяет нам описать такие состояния, как пары запутанных частиц, или же ситуации, когда состояние $|\psi_1\rangle$ выпадает с вероятностью p_1, а $|\psi_2\rangle$ с вероятностью p_2. Чтобы описать общее состояние точно, нам необходимо принять во внимание весь набор состояний и вероятностей $\{|\psi_i\rangle, p_i\}$. Для этого используется формализм матриц плотности.

Определение № 7 (матрица плотности): Состояние системы, связанной с гильбертовым пространством $\mathcal{H}$, задается оператором плотности, также называемым матрицей плотности, который является линейным оператором ρ на $\mathcal{H}$, удовлетворяющем следующим условиям

$$\rho \geq 0,$$
$$\mathrm{Tr}[\rho] = 1$$

Квантовые состояния, как мы их изначально определили, эквивалент-

ны операторам плотности вида $\rho = |\phi\rangle\langle\phi|$ и называются чистыми состояниями. Чистые состояния описываются матрицей ранга 1, она имеет только одно ненулевое собственное число (равное 1) с соответствующим собственным состоянием, и, следовательно, $\mathrm{Tr}\rho^2 = 1$.

Множество операторов плотности обозначим как $\mathcal{L}(\mathcal{H})$; обратите внимание, что такое множество является выпуклым. С помощью спектрального разложения мы всегда можем выразить ρ через собственные числа и собственные векторы как $\rho = \sum_k p_k |b_k\rangle\langle b_k|$; собственные значения образуют распределение вероятностей, поскольку оператор нормирован. Чистые состояния в таком множестве являются его крайними точками. Состояния с более чем одним ненулевым собственным числом называются *смешанными состояниями*, поскольку они представляют собой смеси (выпуклые комбинации) своих собственных векторов.

Рассмотрим квантовую систему $\mathcal{H}_A$, состояние которой зависит от классического значения (случайной величины) Z, и пусть $|\phi_z\rangle\langle\phi_z| \in \mathcal{L}(\mathcal{H}_A)$ - чистое состояние системы, обусловленное событием $Z = z$. Отметим, что состояния $|\phi_z\rangle$ не обязательно должны быть ортогональными. Кроме того, рассмотрим наблюдателя, который не имеет доступа к Z, то есть, с его точки зрения, Z может принимать разные значения, распределенные в соответствии с функцией вероятности P_Z. Тогда такая система описывается ансамблем состояний $\{P_Z(z), |\phi_z\rangle\}$.

Предположим теперь, что система $\mathcal{H}_A$ претерпевает изменение под действием произвольного оператора эволюции U_A с последующим измерением, описываемым положительной операторнозначной мерой $M_A = \sum_x \Pi_x$, где Π_x положительные полуопределенные операторы в гильбертовом пространстве. Тогда, согласно постулатам квантовой механики, функция плотности вероятности результатов измерения x, обусловленных событием $Z = z$, имеет следующий вид

$$P_{X|Z=z}(x) = \mathrm{Tr}[\Pi_x U_A |\phi_z\rangle\langle\phi_z| U_A^*]. \tag{68}$$

Следовательно, с точки зрения наблюдателя, незнакомого со значением Z, функция плотности вероятности X задается

$$P_X(x) = \sum_z P(z) P_{X|Z=z}(x). \tag{69}$$

Согласно свойству линейности это можно переписать в виде

$$P_X(x) = \mathrm{Tr}[\Pi_x U_A \rho_A U_A^*], \tag{70}$$

где неявно определено

$$\rho_A = \sum_z P_Z(z) |\phi_z\rangle\langle\phi_z|. \tag{71}$$

Одной из основных задач квантовой теории информации является передача классической информации с помощью квантовых состояний. Вследствие этого информация, содержащаяся в классической случайной величине Z, должна каким-то образом проявляться физически. Важной особенностью рассматриваемого математического каркаса является то, что Z можно также описать в формализме оператора плотности. Точнее, идея состоит в том, чтобы представить состояния классических значений Z взаимно ортогональными векторами в гильбертовом пространстве.

Определение № 8 (классическое состояние): Для случайной величины Z, распределенной согласно P_Z, соответствующая матрица плотности диагональна в пространстве состояний и имеет следующий вид

$$\rho_Z = \sum_z P_Z(z)|b_z\rangle\langle b_z|, \tag{72}$$

где, $\{|b_z\rangle\}$ – ортонормированный базис. В общем случае данное состояние является смешенным, так как коэффициентами перед слагаемыми является вероятность его выпадения, а не амплитуда вероятности.

Однако в задачах квантовой коммуникации мы часто будем сталкиваться с состояниями, которые частично классические, частично квантовые.

Определение № 9 (классически-квантовое состояние): Классически-квантовое состояние имеет вид

$$\rho_{ZQ} = \sum_z P_Z(z)|b_z\rangle\langle b_z|_Z \otimes \rho_z^Q. \tag{73}$$

Данное состояние имеет классический регистр Z и квантовый Q. Если квантовый регистр отсутствует, то это просто классическое состояние.

4.4 Каналы передачи информации

4.4.1 Общие свойства информационных каналов

Квантовая и, следовательно, классическая теории информации рассматривают взаимные переходы между различными информационными ресурсами. Ресурсы могут быть квантовыми или классическими, статическими или динамическими, с шумом и идеальными. Также ресурсы разделяются по количеству пользователей, чаще всего выделяют двухпользовательские, как самый простой случай (ресурсы одного пользователя считаются неограниченными). Введем обозначения для ресурсов: c — классический, q — квантовый, $\{\cdot\}$ — с шумом, $[\cdot]$ — идеальный, $\to$ — динамический.

Динамические ресурсы — это четыре вида каналов, определяемые квантовой/классической природой входных/выходных данных. Так, например, $\{c \to c\}$ — классический канал связи, определяемый произвольной стохастической матрицей, $\{q \to q\}$ — квантовый канал связи, определяемый произвольным полностью положительным отображением сохраняющим след, $\{c \to q\}$ — приготовление квантового состояния, используя произвольный квантовый алфавит (набор используемых состояний) $\{\rho_x\}$, $\{q \to c\}$ — обобщенное квантовое измерение с классическим результатом, задаваемое произвольной положительно определенной мерой. Замена фигурных скобок на квадратные дает соответственные идеальные каналы с единичной пропускной способностью (сохраняя соответствующую размерность бит/бит, бит/кубит, кубит/бит).

Существует три типа статических ресурсов: классические $\{cc\}$, квантовые $\{qq\}$ и смешанные квантово-классические $\{cq\}$. Первым типом является коррелированная пара случайных переменных X и Y, определенных на множестве $\mathcal{X} \times \mathcal{Y}$ и имеющих совместное распределение вероятностей $p(x, y) = Pr\{X = x, Y = y\}$. Квантовым типом $\{qq\}$ является двухчастичная квантовая система $\mathcal{AB}$, определенная на гильбертовом пространстве $\mathcal{H}_\mathcal{A} \otimes \mathcal{H}_\mathcal{B}$ и имеющая оператор плотности $\rho^{\mathcal{AB}}$. Ресурс $\{cq\}$ является гибридной квантово-классической системой $\mathcal{XQ}$, описываемая ансамблем $\{\rho_x, p(x)\}$, где $p(x)$ определено на множестве $\mathcal{X}$, а ρ_x является набором операторов плотности системы $\mathcal{Q}$ в гильбертовом пространстве $\mathcal{H}_\mathcal{Q}$. Состояние системы $\mathcal{Q}$ коррелировано со значением классической переменной X. Для описания ресурса $\{cq\}$ пользуются "расширенным гильбертовым пространством"(РГП), где под расширением понимается добавление подсистемы $\mathcal{A}$, которая описывает классическую переменную на квантовом языке. Таким образом, ансамбль $\{\rho_x, p(x)\}$ можно представить единым оператором плотности $\rho^{\mathcal{AQ}} = \sum_x p(x)|x\rangle\langle x|^\mathcal{A} \otimes \rho_x^\mathcal{Q}$, где $\{|x\rangle : x \in \mathcal{X}\}$ — ортонормальный базис в гильбертовом пространстве $\mathcal{H}_\mathcal{A}$ системы $\mathcal{A}$.

Идеальный ресурс $[cc]$ представляет собой полностью коррелированные случайные переменные, для которых справедливо $\mathcal{X} = \mathcal{Y}$ и $p(x, y) = p(x)\delta(x, y)$, где $\delta(\cdot, \cdot)$ – дельта-функция Дирака. Ресурс $[qq]$ является полностью запутанным состоянием $|\psi\rangle_\mathcal{AB} = \frac{1}{\sqrt{2}}(|0\rangle_\mathcal{A}|0\rangle_\mathcal{B} + |1\rangle_\mathcal{A}|1\rangle_\mathcal{B})$ системы $\mathcal{AB}$.

Таким образом, различные протоколы квантовой информатики можно представить в виде процессов преобразований ресурсов, например $\{qq\} + [cc] \Rightarrow [qq]$ — усиление запутанности, $\{c \to c\} \Rightarrow [c \to c]$ — теорема Шэннона, $[c \to c] + [qq] \Rightarrow [q \to q]$ — квантовая телепортация и т.п.. Протоколы квантовой коммуникации/криптографии, в свою очередь, можно представить в виде следующих последовательных преобразований ресур-

сов

$$\{c \to q\} + \{q \to q\} + \{q \to c\} + [c \to c] \Rightarrow [cc], \tag{74}$$

где $\{c \to q\}$ — приготовление Алисой состояний, $\{q \to q\}$ — распространение состояний по квантовому каналу, $\{q \to c\}$ — измерение состояний Бобом (и Евой), $[c \to c]$ — классическая постобработка "сырого"ключа и усиление секретности. Далее рассмотрим подробнее этап $\{q \to q\}$ и связанные с ним особенности.

4.4.2 Квантовые каналы

Что с математической, что с физической точек зрения квантовый канал - это квантовая операция, рассматриваемая как динамика открытой квантовой системы, а также средство для передачи квантовой или классической информации. Рассмотрим квантовый канал как линейное вполне положительное и сохраняющее след линейное отображение. На сегодняшний день существуют три основных подхода для их описания, представленные в статьях [5, 6, 7].

Пусть $\mathcal{A}, \mathcal{B}, \mathcal{E}$ – гильбертовы пространства Алисы, Боба и окружающей среды (Евы) соответственно. Тогда теорема Штайншпринга говорит о том, что для каждого квантового канала Φ всегда существует изометрия $U : \mathcal{A} \hookrightarrow \mathcal{B} \otimes \mathcal{E}$, следующего вида $U^\dagger U = \mathbb{I}$, делающая отображение состояний из системы $\mathcal{A}$ в совместную систему $\mathcal{B} \otimes \mathcal{E}$. В данном случае квантовый канал описывается путем взятия частичного следа по подсистеме $\mathcal{E}$ и имеет следующий вид

$$\Phi(\rho) = \mathrm{Tr}_{\mathcal{E}} U \rho U^\dagger, \tag{75}$$

где ρ принадлежит пространству сохраняющих след операторов на гильбертовом пространстве $\mathcal{A}$. При взятии частичного следа по подсистеме $\mathcal{B}$ вместо подсистемы $\mathcal{E}$ можно получить описание комплементарного квантового канала, $\tilde{\Phi}(\rho)$ соответственно

$$\tilde{\Phi}(\rho) = \mathrm{Tr}_{\mathcal{B}} U \rho U^\dagger, \tag{76}$$

Другими словами, квантовый канал показывает, как во времени изменяется матрица плотности, описывающая квантовое состояние, при взаимодействии с окружающей средой как показано на рис. 28.

4.4.3 Информационные характеристики

Чаще всего такое описание квантовых каналов используется для задач передачи информации. Подобные задачи реализуются в три этапа, как

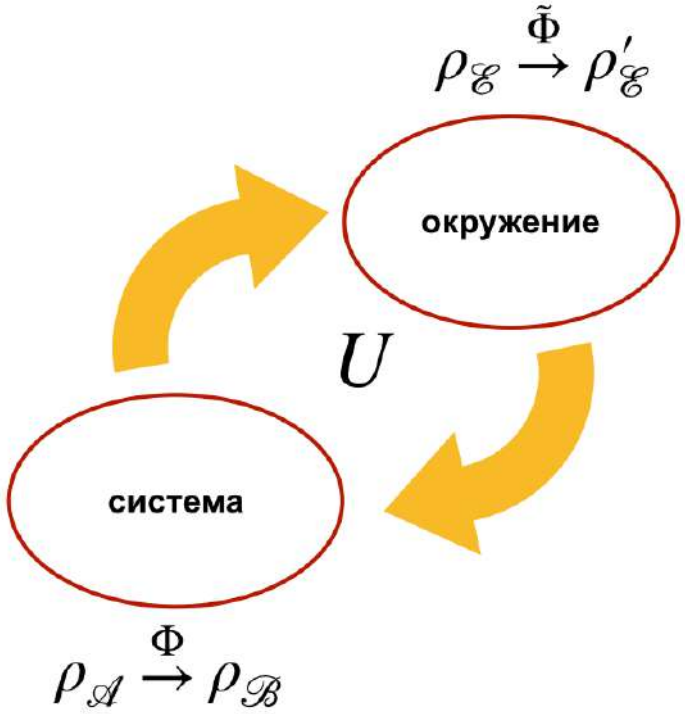


Рис. 28: Схематическое изображение взаимодействия квантовой системы с окружающей средой

показано на рис. 29: кодирование информации, передача через канал (чаще всего канал с шумом) и декодирование информации. Состояние, получаемое в результате кодирования классической информации в квантовую систему, может быть представлено как квантово-классическое состояние из уравнения 73. Распространение квантового состояния в канале описывается непосредственно с помощью уравнения 75. Описание методов декодирования информации из квантовых состояний остается за пределами данной главы.

Как и было сказано ранее, основной мерой оценки количества информации является энтропия. Информационная энтропия — мера неопределённости некоторой системы (в статистической физике или теории информации), в частности непредсказуемость появления какого-либо символа первичного алфавита. В последнем случае при отсутствии информационных потерь энтропия численно равна количеству информации на символ передаваемого сообщения. В классической теории информации чаще всего используется двоичная энтропия. Информационная двоич-

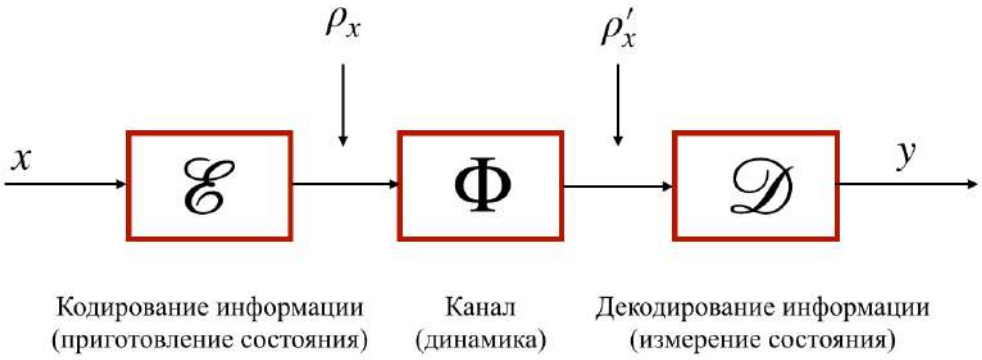


Рис. 29: Схематическое изображение передачи информации через квантовый канал

ная энтропия, при отсутствии информационных потерь рассчитывается по формуле Хартли

$$i = \log_2 N, \tag{77}$$

где N – мощность алфавита, i – количество информации в каждом символе сообщения. В общем виде, для произвольной случайной величины эта формула переходит в формулу Шеннона

$$H(x) = -\sum_{i=1}^{n} p_i \log p_i, \tag{78}$$

где p_i – распределения вероятностей.

Представим, что есть состояние $\rho_X = \sum_{x=0}^{d-1} p_x |x\rangle\langle x|$. Заметим, что это означает, что мы эффективно рассматриваем распределение вероятностей p_x по строкам x. Как возможно измерить присущую x неопределенность? Говоря о различных видах коммуникации, одной из важных мер является энтропия фон Неймана или Шеннона (78). Но является ли эта мера подходящей и достаточной для оценки в контексте, например, криптографии?

К сожалению, данная мера не может быть использована в разрезе криптографии, ввиду того, что здесь используется усреднение по всем возможным результатам, в то время как необходимо рассматривать худший из возможных сценариев. Однако на сегодняшний день существует альтернативная мера, которая может быть использована для этих целей.

Энтропией Реньи называется энтропия

$$H_\alpha(X) = \frac{1}{1-\alpha} \log \left(\sum_{i=1}^{n} p_i^\alpha \right), \tag{79}$$

являющаяся обобщением энтропии Шеннона, которое вводит параметр α, чтобы получить семейство мер неопределенности. Как и энтропия Шеннона, энтропия Реньи используется для описания степени неопределенности в алфавите сообщений, но ее использование может быть более удобным в некоторых приложениях, таких как физика и теория информации.

В данной работе рассматривается энтропия для любого распределения вероятностей $\{p_x\}_x$, когда параметр $\alpha \to \infty$, а именно *мин-энтропия*,

$$H_\infty(X) = H_{\min} = -\log \max_i p_i, \tag{80}$$

описывающая наихудший, а не усредненный случай, как это делают энтропии Шеннона и фон Неймана. Иными словами, $H_{\min}$ – мера неопределенности в случайной величине, которая характеризует минимальное количество бит, необходимых для представления этой величины в ее наиболее неопределенном состоянии. *мин-энтропия* широко используется в криптографии для оценки качества случайных чисел, используемых в качестве ключей шифрования, и для оценки сложности атак на системы шифрования.

В общем случае вероятность того, что мы угадаем всю битовую строку, оценивается как $P_{guess}(X) = \max_x p_x$. В таком случае

$$H_{\min}(X) = -\log P_{guess}(X).$$

Кроме того, возможно также количественно оценить неопределенность относительно X, учитывая некоторый дополнительный квантовый регистр E. Как и для энтропии фон Неймана, у мин-энтропии Реньи существует условный вариант $H_{\min}(X|E)$. Самый простой способ думать об условной мин-энтропии заключается в вероятности того, что Еве (злоумышленнику) удается угадать X, получив доступ к ее квантовому регистру E.

Рассмотрим двустороннее классически-квантовое состояние ρ_{XE}, где X – классический регистр. Тогда *условная мин-энтропия* $H_{\min}(X|E)$ может быть записана как

$$H_{\min}(X|E) := -\log P_{guess}(X|E),$$

где $P_{guess}(X|E)$ – вероятность того, что Ева угадает x, максимизированная по всем возможным квантовым измерениям. Её можно представить в виде

$$P_{guess}(X|E) := \max_{\{M_x\}} x \sum_x p_x[M_x \rho_x^E],$$

где ρ_x^E – матрицы плотности квантового регистра E, скоррелированного с классическим регистром X, а максимизация взята по всем возможным положительным операторнозначным мерам $\{M_x \geq 0 | \sum_x M_x = \mathbb{I}\}$, описывающим измерение. В данном контексте E называют сторонней информацией о X.

4.4.4 Пропускные способности квантовых каналов

В отличие от классических каналов связи, которые характеризуются только одним типом пропускной способности, квантовые каналы могут иметь целый ряд подобных характеристик. Прежде всего стоит отметить, что через квантовый канал можно передавать как классическую, так и квантовую информацию. Для большинства прикладных задач больший интерес представляет передача классической информации через квантовый канал. Способы оценки количества передаваемой квантовой информации останутся за скобками данного раздела. Оценка максимального количества классической информации, которая может быть передана через квантовый канал, может быть произведена двумя способами и зависит от интересующей задачи. В случае, когда необходимо оценить количество достоверно передаваемой информации, оптимальной мерой является классическая пропускная спосонбость квантового канала. Однако такой меры не всегда бывает достаточно. Например, задача может заключаться в том, чтобы передача информации была секретной, и тогда уже оптимальной мерой будет секретная (private) пропускная способность квантового канала.

Чтобы оценить максимально возможное количество классической информации, которую можно извлечь из квантовых состояний, необходимо вычислить границу Холево [8]. Она может быть оценена следующим образом:

$$\begin{aligned} I(\mathcal{A} : \mathcal{Q}_0) = S(\rho_{\mathcal{A}}) + S(\rho^{\mathcal{Q}_0}) - S(\rho_{\mathcal{A}}^{\mathcal{Q}_0}) = \\ = S(\rho^{\mathcal{Q}_0}) - \sum_x P(x) S(\rho_x^{\mathcal{Q}_0}), \end{aligned} \tag{81}$$

$$\rho_{\mathcal{A}}^{\mathcal{Q}_0} = \sum_x P(x) |a_x\rangle_{\mathcal{A}} \langle a_x| \otimes \rho_x^{\mathcal{Q}_0}, \tag{82}$$

где $\rho_{\mathcal{A}}$ – матрица плотности классической системы, $\rho^{\mathcal{Q}_0}$ – общее состояние квантового регистра после кодирования в него информации, $\rho_x^{\mathcal{Q}_0}$ – матрица плотности, описывающая состояние соответствующее закодированному биту информации, а $S(x)$ – энтропия фон Неймана.

В статьях [9, 10, 11, 12] дается определение максимального количества информации о сообщении, которое может быть восстановлено с помощью измерения пользователя $\mathcal{B}$, которое называется доступной информацией. Подходящей мерой восстановленной информации является взаимная информация, которая для пары случайных величин X, Z, принадлежащих подсистемам $\mathcal{A}, \mathcal{B}$, определяется как

$$I(\mathcal{A} : \mathcal{B}) = S(\rho_{\mathcal{A}}) + S(\rho_{\mathcal{B}}) - S(\rho_{\mathcal{AB}}). \tag{83}$$

Эта корреляционная мера лежит в основе классической оценки пропускной способности квантового канала. В случае распутанных состояний его можно оценить следующим образом:

$$C(\mathcal{N}) = \max_{p_i, \rho_i} I(\mathcal{A} : \mathcal{B}), \tag{84}$$

где $\mathcal{N}$ обозначает действие квантового канала, а $\{p_i, \rho_i\}$ – ансамбль квантовых состояний в канале.

Однако эта мера не подходит для безопасной передачи данных или проблем квантового распределения ключей. Эта проблема требует оценки трехсторонних корреляций, поскольку в качестве третьей подсистемы следует рассматривать злоумышленника (Еву). В этом случае следует рассматривать секретную (private) пропускную способность [13], которая описывает максимальную скорость, с которой можно передавать классическую информацию по каналу надежно и конфиденциально (то есть без какой-либо утечки информации об исходном сообщении для подслушивателя). Следовательно, однобуквенная секретная пропускная способность может быть рассчитана следующим образом:

$$P^{(1)}(\mathcal{N}) = \max_{p_i, \rho_i} (I(\mathcal{A} : \mathcal{B}) - I(\mathcal{A} : \mathcal{E})) \tag{85}$$

4.5 Контрольные вопросы

1. Что такое квантовая теория информации?
2. Какая основная единица измерения в квантовой теории информации?
3. Какая основная мера количества информации используется в квантовой теории?
4. Что такое пропускная способность канала?
5. Что такое квантовая запутанность (сцепленность)?
6. Почему невозможно копировать квантовое состояние?
7. Как могут быть описаны квантовые состояния?
8. Какие состояния называются смешанными состояниями?
9. Как описывается классически-квантовое состояние?
10. Какие типы статических ресурсов существуют?
11. С помощью какого уравнения описывается распространение квантового состояния в канале?
12. В чем отличие пропускной способности квантовых каналов от классических?

5 Квантовые коммуникации в свободном пространстве и в космосе

5.1 Первый эксперимент по передаче квантовых ключей через атмосферный канал связи

Стоит отметить, что исторически первый эксперимент по передаче квантовых ключей был проведен именно в открытом пространстве в 1989 году. В работе [14] были представлены результаты по передаче квантовых ключей на лабораторном столе на расстояние 32 см. На рисунке 30 представлена фотография эксперимента. Устройство отправителя состояло из зеленого светодиода, луч которого из 25 мкм отверстия был коллимирован в объектив с фокусным расстоянием 25 мм, затем прошел через 550 нм фильтр и горизонтальный поляризатор. Ячейки Поккельса у отправителя преобразовывали горизонтальную поляризацию в произвольную последовательность четырех состояний поляризации (горизонтальной, вертикальной, лево-круговой и право-круговой) в соответствии с протоколом BB84. Среднее число фотонов в импульсе на выходе из устройства отправителя составило 0,1. После прохождения квантового сигнала по открытому пространству на 32 см луч попадал в устройство получателя. Здесь ячейка Поккельса преобразовала линейную поляризацию в круговую, и наоборот. Затем призма Волластона разбивала пучок света на горизонтально- и вертикально-поляризованные компоненты, которые регистрировались с помощью фотоэлектронных умножителей A и B соответственно.

Квантовая эффективность фотоэлектронных умножителей составляла 9%, при темновых отсчетах порядка 200 в секунду или около 10^{-4} на 500 нс временном окне. При использовании среднего числа фотонов в импульсе $\mu = 0,1$ теоретически рассчитанный коэффициент квантовых ошибок составил около 2%; фактический коэффициент ошибок составил около 4%, что было обусловлено несовершенством используемых ячеек Поккельса.

5.2 Квантовая коммуникация по атмосферному каналу связи в условиях прямой видимости

Большое количество работ о квантовой коммуникации в открытом пространстве посвящено лабораторным исследованиям таких систем [15, 16, 17, 18, 19]. В таких работах передача квантовых ключей по атмосферному каналу связи осуществляется на небольшие расстояния в пределах

лабораторий, подобно эксперименту, описанному в предыдущем разделе. Однако в ряде работ квантовая коммуникация по атмосферному каналу связи в пределах прямой видимости была осуществлена между отдельно стоящими зданиями на значительные расстояния.

В 2008 году в рамках проекта создания европейской квантовой сети SECOQC в качестве одного из каналов связи между узлами сети был использован атмосферный лазерный канал. Узлы располагались в пределах прямой видимости (80 м). На рисунке 31 представлена фотография атмосферной линии связи и схема устройства квантовой коммуникации. В блоке передатчика импульсы восьми лазерных диодов объединяются с использованием специальной конструкции конических и пирамидальных зеркал в пространственный фильтр. Диоды управляются в соответствии со случайным выбором четырех состояний поляризации $-45°$, $0°$, $45°$ и $90°$ со средним числом фотонов в импульсе μ=0.3. Далее ослабленные импульсы попадали в атмосферный канал связи. Атмосферный канал связи был реализован при помощи линзовых телескопических систем диаметром 25 мм. В блоке получателя сигнал после фильтрации попадал на систему из светоделителей и пластинок $\lambda/4$, в которой случайным образом анализировалось его поляризационное состояние ($-45°$, $0°$, $45°$ и $90°$). Далее фотоны регистрировались на лавинных фотодиодах. Узлы работали в тестовом режиме в течение месяца при различных погодных условиях с использованием поляризационного протокола BB84 с состояниями-ловушками. Среднее значение скорости генерации просеянных квантовых ключей составило 50 кбит/с при уровне квантовых ошибок порядка 2,3%.

В работе [20] исследовалась высокоскоростная передача квантовых ключей в городских условиях на расстояния до 300 м по атмосферному каналу связи между зданиями. Фотографии и схемы устройств отправителя и получателя представлены на рисунке 32. Для достижения высокой скорости передачи квантовых бит отправитель генерировал сигнал с тактовой частотой 1 ГГц, используя два высокоскоростных лазерных диода на длине волны λ=848 нм и два высокопоглощающих поляризатора для генерации двоичных логических состояний «1» и «0». Среднее число фотонов в импульсе было равно 0,2. Оба состояния объединялись на специальной призме и передавались через атмосферный квантовый канал связи получателю. Получатель состоял из 25-миллиметрового телескопа Шмидта-Кассегрена и оптических компонентов, необходимых для распознавания логических состояний «1» и «0».Предельная скорость обмена квантовыми ключами составляла 1 Мбит/с (ночью). В условиях яркого дневного света система работала со средней скоростью передачи квантовых ключей 0,5 Мбит/с при среднем коэффициенте квантовых ошибок

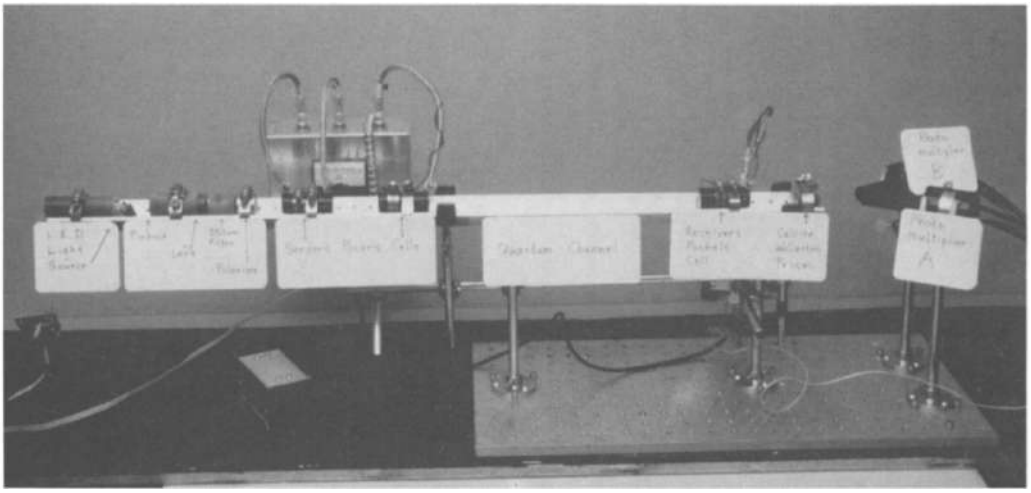


Рис. 30: Первый экспериментальный стенд системы квантовой коммуникации

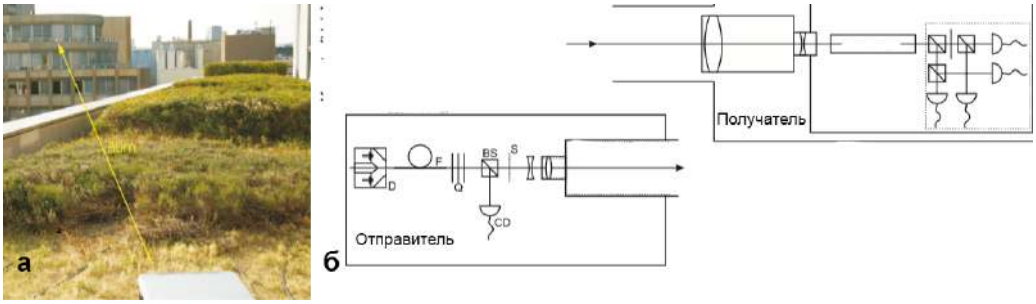


Рис. 31: а. Вид на атмосферную линию связи, б. Оптическая схема устройства квантовой коммуникации

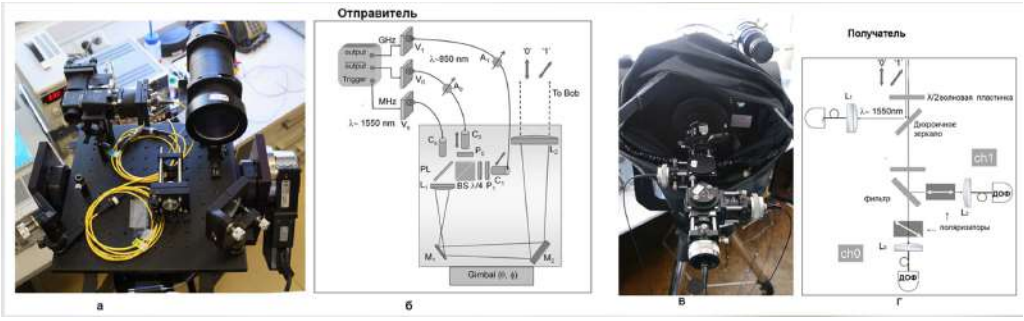


Рис. 32: Фотография устройства отправителя (а) и его оптическая схема (б). Фотография устройства получателя (в) и его оптическая схема (г)

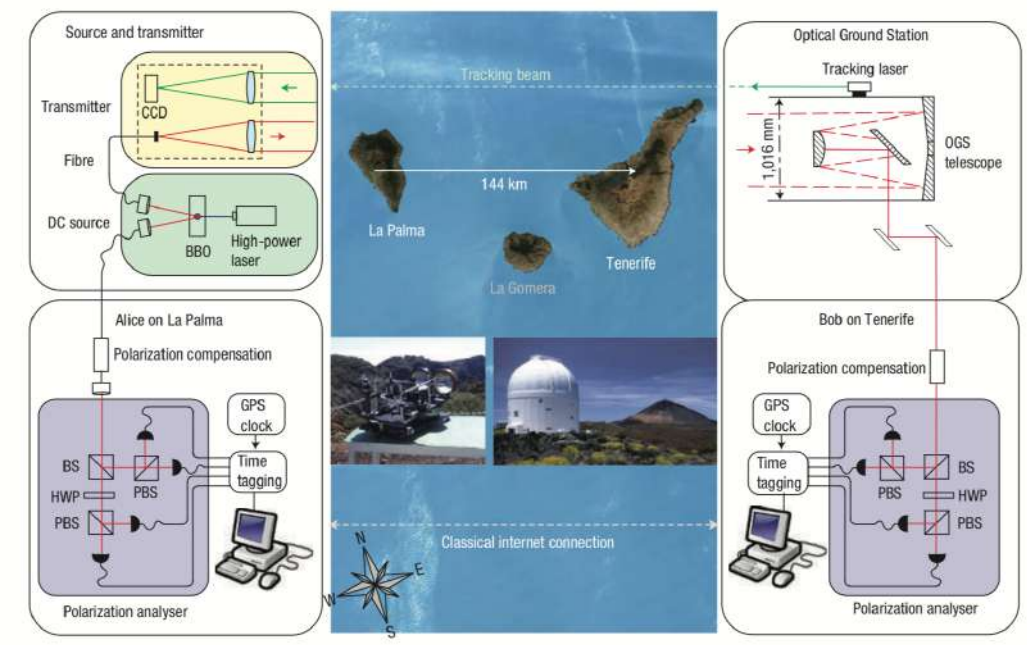


Рис. 33: Схема эксперимента по передаче запутанного квантового состояния на 144 км по атмосферному каналу между островами Ла Пальма и Тенерифе

порядка 4,5%. Система была протестирована на безотказную работу в течение 24 часов.

5.3 Передача запутанных фотонных пар по атмосферному каналу связи на 144 км

В работах [21, 22] экспериментально продемонстрировано распределение квантовых ключей на расстояние 144 км. На сегодняшний день этот эксперимент является рекордным для передачи квантового состояния света на земле через атмосферный канал связи. Данная работа являлась важным шагом на пути к спутниковой квантовой коммуникации и экспериментальным испытаниям квантовой физики в космосе (рисунок 33). Поляризованные запутанные пары фотонов были получены с помощью спонтанного параметрического рассеяния II типа накачкой кристалла β-бората-бария (BBO) с помощью мощного ультрафиолетового лазера. Один фотон измерялся локально на Ла-Пальме; другой был отправлен через 15-сантиметровый приемо-передатчик по атмосферной оптической линии длиной 144 км на телескоп с диаметром апертуры 1 м оптической

наземной станции на острове Тенерифе. Связь активно стабилизировалась путем анализа направления пучка слежения (532 нм), отправленного из Ла-Пальмы, который был получен во второй линзе, фокусирующей ее на ПЗС. В квантовом канале оптических перекрестных помех не было, поскольку следящий лазер был направлен в противоположном направлении; дополнительно использовались интерференционные фильтры. Обе стороны использовали четырехканальные поляризационные анализаторы, состоящие из делителей пучков 50/50 (BS), полуволновой пластины (HWP) и поляризационных делителей пучка (PBS). Всего в эксперименте была передана квантовая битовая последовательность длиной 178 бит, т.е. передавался один фотон приблизительно за 75 секунд.

5.4 Квантовая коммуникация между движущимся и наземным объектами

В 2013 году группа исследователей из Германии впервые продемонстрировала [23] возможность квантовой коммуникации между самолетом и наземной станцией.

Устройство передатчика было установлено на самолет Dornier 228. Передача квантовых ключей осуществлялась в темное время суток во время облета самолетом по дуговой траектории приемного телескопа (рисунок 34). Расстояние между самолетом и приемной станцией составляло 20 км. При передаче ключей использовался протокол BB84 с кодированием поляризационных состояний фотона.

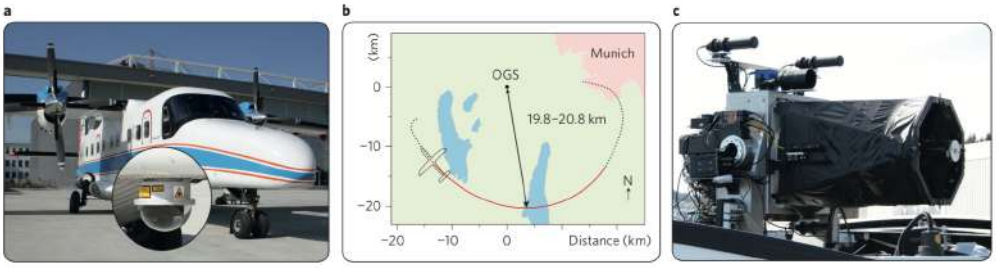


Рис. 34: a, Самолет The Dornier 228, использованный в эксперименте. Вставка: оптический купол с CPA. b, траектория полета самолета, с красной секцией, обозначающей позиции во время передачи квантовых ключей. c телескоп OGS

Скорость генерации просеянных ключей составила 145 бит/с с коэффициентом квантовых ошибок 4,8%. Высокий уровень ошибок в первую

очередь был связан с высоким темновым шумом приемника одиночных фотонов. В общей сложности в результате одного облета самолета вокруг приемного телескопа было получено около 80 кбит секретного квантового ключа.

В 2017 году канадские ученые реализовали квантовый канал связи для распределения секретных ключей шифрования между летящим самолетом в качестве получателя и наземной станцией в качестве отправителя [24]. В работе была продемонстрирована возможность квантового распределения ключа между летящим самолетом и наземной станцией. Для приема и передачи фотонов физики использовали пару телескопов. Приемник был установлен на самолете, облетавшем наземную станцию, как показано на рисунке 35, на высоте 1,6 километра. Протяженность линии связи колебались от 3 до 10 километров. В установке были предприняты методы защиты от простейших атак на системы квантовых коммуникаций, например, против атаки типа «Троянский конь».

Рис. 35: Траектория полета самолета вокруг наземной станции (обозначена звездой), желтым и синим показаны траектории, во время которых осуществлялся сеанс квантовой связи

Самолет выполнил 14 полетов вокруг наземной станцией со скоростью около 200 - 250 километров в час. Из них 7 раз удалось установить квантовый канал связи и в 6 из них – сгенерировать квантовый ключ. Время квантовой связи колебалось от 30 секунд до четырех с половиной минут, максимальный размер секретного ключа составил 867 килобит.

5.5 Квантовая коммуникация между наземными и низкоорбитальными летательными объектами

Искусственные спутники, летающие на околоземной орбите, могут использоваться в качестве доверительных узлов для передачи квантовых ключей на большие расстояния, так как на данный момент ограниченная дальность передачи квантовых ключей по волоконным линиям связи является одной из важнейших проблем. На сегодняшний день существует два основных подхода для её увеличения. Первый — использование квантовых повторителей. Этот вариант является самым очевидным, однако имеет один существенный недостаток — реализация подобных элементов сети в полной мере так и не осуществлена на сегодняшний день, несмотря на то, что некоторые технологические компоненты, необходимые для их создания, уже разработаны и исследуются в лабораторных условиях. Второй — использование доверенных узлов. Доверенный узел представляет собой схему, соединяющую две разнесенные квантовые сети, либо две линии квантовой коммуникации, построенные по принципу “точка-точка”, в одну. Подобный узел, несмотря на то, что между блоками отправителя и получателя происходит классическая передача информации, является доверенным, в связи с тем, что обмен информацией происходит в пределах одного устройства, куда у нелегитимного пользователя нет доступа, благодаря одному из основных требований к системам КРК. Как показано на рисунке 36, данный доверенный узел включает в себя два модуля отправителя (А1 и А2). На земле же находятся два модуля получателя (Б1 и Б2), разнесенные географически. Таким образом, в доверенном узле образуются два ключа от каждой из сторон, которые складываются по модулю два, а результат этой операции отправляется в приемный модуль второй стороны. Затем в приемном модуле второй стороны производится сложение по модулю два данной последовательности с ключом, сгенерированным в этом участке сети. Данная операция позволяет получить одинаковые ключи на обоих участках сети, что позволяет таким образом увеличить дальность передачи ключа.

Далее рассмотрим работы, посвященные созданию спутников для квантовой связи.

Первой работой по передаче квантовой информации в виде одиночных фотонов с орбитального спутника на земную станцию является работа 2008 года Антона Цайленгера и его исследовательской группы. В работах [25, 26] ими были представлены результаты первого в мире успешного эксперимента по устойчивой передаче и детектированию однофотонных импульсов между Землей и спутником на высокой орбите. В работе была показана возможность защиты средствами квантовой коммуникации ка-

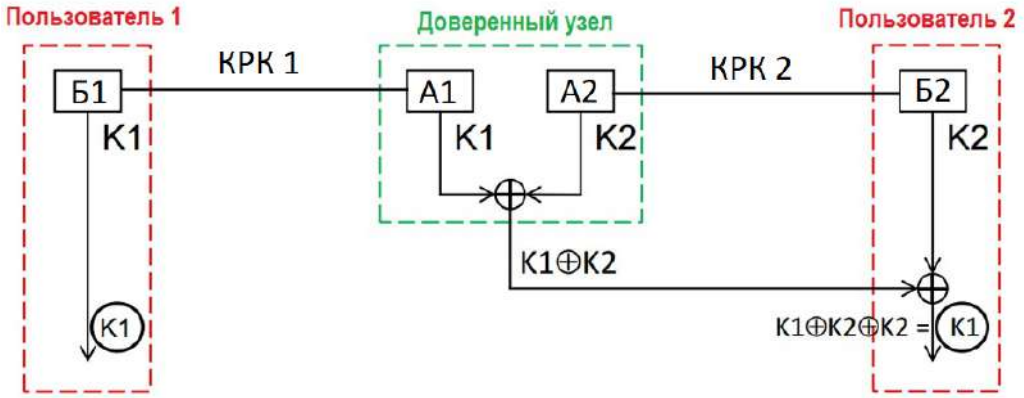


Рис. 36: Схема устройства доверенного узла в системах квантовой коммуникации. K1, K2 - ключи, генерируемые отправителем и получателем на линиях КРК1 и КРК2, соответственно

налов спутниковой связи, телеметрической и разведывательной информации, даже для спутников, находящихся на высокой орбите.

В эксперименте использовалось стандартное оборудование лазерной станции Матера итальянского космического агентства и геодезический спутник Аджасти японского космического агентства (минимальное расстояние от орбиты до земли составляло 1485 км). Этот спутник представляет собой покрытую угловыми отражателями сферу. Контроль орбиты спутника осуществляется методами лазерной локации с помощью телескопа станции Матера с апертурой 1,5 м. В эксперименте использовались лазерные импульсы со следующими характеристиками: длина волны $\lambda = 532$ нм, продолжительность импульс $t = 700$ пс, мощность $P = 490$ нДж, частота повторения $F = 17$ кГц. Детектирование отраженных спутником сигналов осуществлялось при помощи узкополосного лавинного фотодиода.

Основными ограничивающими факторами передачи квантовой информации от спутника к земной станции были атмосферные искажения, которые приводили к искажению фронта волны, атмосферное поглощение, потери сигнала из-за нестабильности установки лазерного локатора на наземной станции вследствие сейсмических колебаний. Расчеты показали, что лазерный импульс проходил на пути к спутнику и обратно в атмосфере расстояние, эквивалентное дистанции 8 км на уровне моря. Помимо спутника Аджасти, подобные эксперименты (рисунок 37) были проведены также со спутниками Лагос (минимальное расстояние от орбиты до земли 5625 км), Посейдон (минимальное расстояние от орбиты

до земли приблизительно 1350 км) и Бикон-С (минимальное расстояние от орбиты до земли 927 км), также оснащенными уголковыми отражателями. Эксперимент показал возможность осуществления закрытой передачи данных со спутника и на спутник с использованием существующих средств лазерной спутниковой связи. В 2013 г. научная группа Цзяньвэя Паня из Научно-технического университета в Шанхае (КНР) представила работу, в которой было показано отражение одиночного фотона от спутника, вращающегося вокруг Земли, и регистрация его обратного прихода на планету. В эксперименте использовались два телескопа в бинокулярной формации, которую направили на спутник, вращающийся на высоте 400 км. Аппарат покрыт отражателями, способными отражать лазерные пучки назад к Земле, а точнее – почти к тому же месту, откуда они вышли. В сравнении с работой [25] авторы уверяют, что получили гораздо большее отношение «сигнал-шум» — 16:1 против 1:1 в работе [25]. Поскольку атмосфера Земли поглощает довольно большую часть фотонов, отправляемых с поверхности, в каждом импульсе, посылаемом с Земли, количество фотонов должно было быть примерно равно $1.5 * 10^9$, чтобы до спутника долетел хотя бы один фотон. Далее этот фотон отражался и направлялся от спутника к Земле. Однако и этот фотон мог быть поглощён атмосферой, поэтому передача повторялась несколько миллионов раз в секунду, и лишь примерно 600 раз в секунду на приемном модуле детектировались одиночные отражённые фотоны. Для эксперимента использовался немецкий спутник CHAMP, запущенный в 2000 году и ушедший с орбиты в 2010-м. Далее в 2016 году сотрудниками этой лаборатории был запущен первый спутник в мире, предназначенный для квантовой передачи информации на Землю. Спутник получил названия «Мо-Цзы» и Quantum Sciense Sattelite (QSS). QSS является проектом Китайской академии наук при участии Австрийской академии наук. Общая стоимость проекта оценивается около 100 млн долларов. Вес спутника составляет более 600 кг.

В 2017 году были представлены первые научные результаты миссии квантового спутника связи. Аппарат обеспечил распределение запутанных фотонов на рекордно большое расстояние, свыше 1200 километров — это в 12 раз больше, чем в предыдущих экспериментах. Эксперимент вновь подтверждает нарушение локальности запутанными частицами. В дальнейшем в планах миссии реализация квантовой спутниковой линии связи между Веной и Пекином, где спутник будет выступать в роли доверительного узла и эксперименты по квантовой телепортации.

С помощью космического аппарата «Мо-Цзы» физикам удалось распределить запутанные фотоны между парами обсерваторий, находившихся на расстоянии до 1203 километров [27, 28, 29]. Эксперимент был

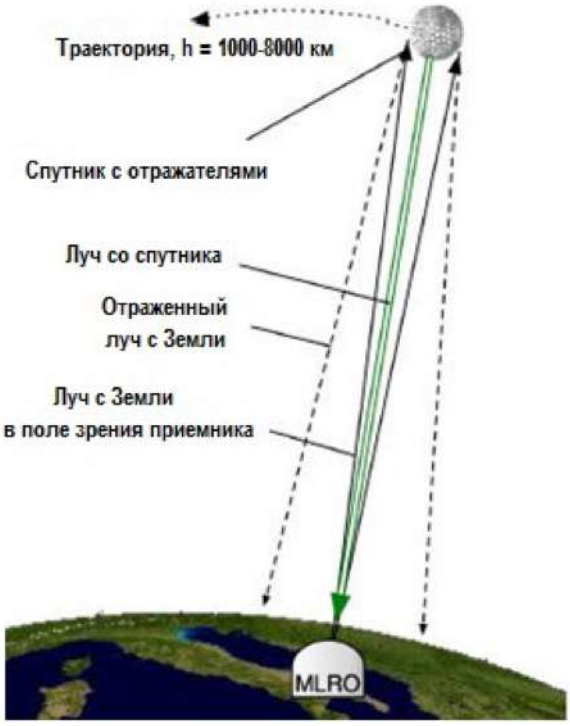


Рис. 37: Схема однофотонной локации спутника

устроен следующим образом. На космическом аппарате был установлен яркий источник запутанных фотонов — кристалл, в котором происходило спонтанное параметрическое рассеяние — превращение одного фотона в два с уменьшенной энергией. Источник формировал около шести миллионов пар запутанных фотонов в секунду. Затем фотонные пары отправляли с помощью двух телескопов к наземным обсерваториям (рисунок 38): Дэлинха (Тибет), Наньшань (Урумчи) и Гаомеигу (Юньнань). Как телескопы спутника, так и телескопы-приемники требовали высокой точности наведения — «Мо-Цзы» двигался по орбите со скоростью около восьми километров в секунду. По словам авторов, наибольшие потери одиночных фотонов происходят в нижних 10 километрах атмосферы Земли. Расстояния от спутника до наземных станций по прямой составляли от 500 до 1700 километров. В таких условиях физикам удалось собрать свыше 1000 событий, когда оба фотона запутанной пары достигали наземной обсерватории — примерно одно событие на шесть миллионов отправленных фотонных пар. Для проверки запутанности и нарушения локальности ученые анализировали взаимную поляризацию пар фотонов. Со статистической значимостью в четыре стандартных отклонения

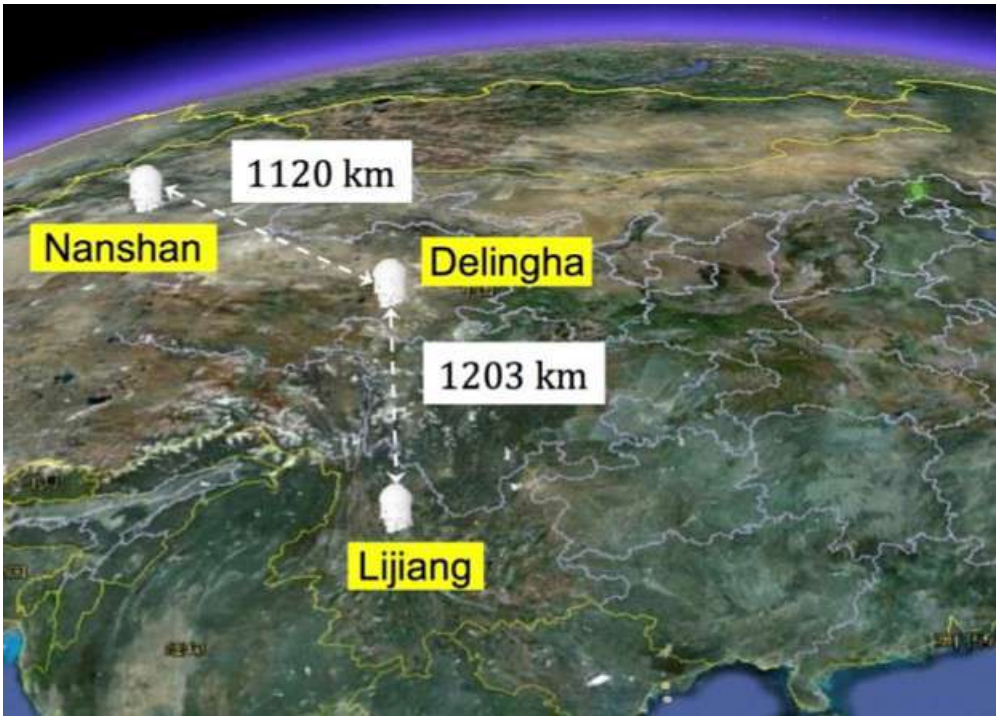


Рис. 38: Расположение наземных станций

исследователи показали, что поляризация частиц оказывалась взаимно перпендикулярной чаще, чем того можно было ожидать в предположении локальности.

5.6 Квантовая коммуникация с использованием фотонов, обладающих орбитальным угловым моментом

Для преодоления проблемы расхождения поляризационных базисов в работе [30, 31] был предложен уникальный способ кодирования кубитов с использованием "закрученного"света (рисунок 39). В таких системах базис квантовых ключей можно описать гибридными состояниями, связанными с орбитальными и спиновыми угловыми моментами:

$$|1\rangle_L = |R\rangle_p |l\rangle_o,$$
$$|0\rangle_L = |L\rangle_p |l\rangle_o.$$

Первые экспериментальные исследования систем квантовой коммуникации в открытом пространстве на основе этого метода были представлены в работе [32].

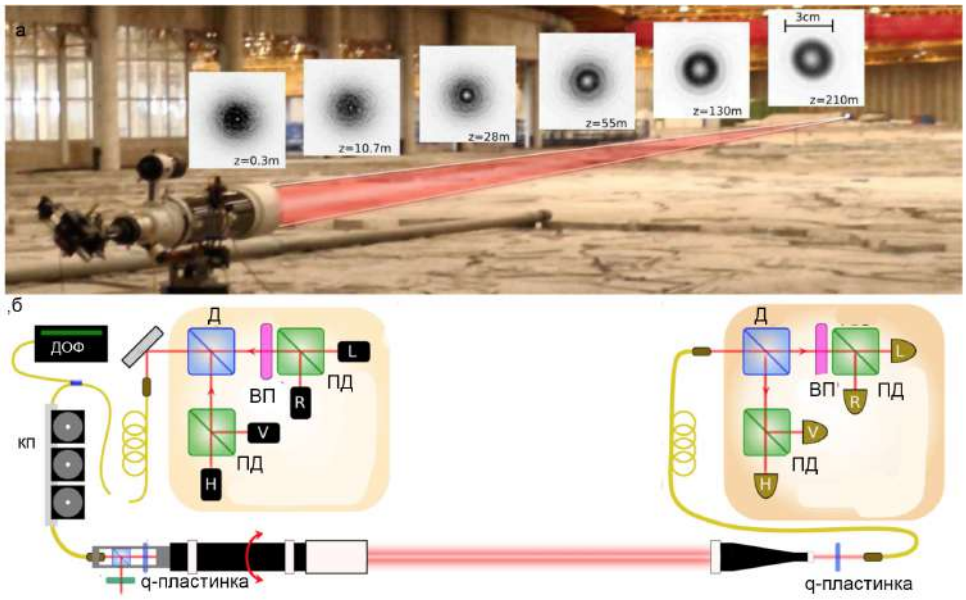


Рис. 39: Экспериментальное исследование системы квантовой коммуникации с использованием "закрученного"света. а. Изображение экспериментального стенда. Телескоп отправителя находится слева, телескоп получателя - справа. Профиль луча в зависимости от расстоянием распространения z от телескопа показан в квадратных рамках. б. Оптические схемы установок отправителя и получателя

Устройство отправителя состояло из четырех лазеров (с длиной волны λ=850 нм) с четырьмя различными поляризациями: горизонтальной H, вертикальной V, левосторонней L и правосторонней R [L и R получены комбинацией поляризации лазера и $\lambda/4$ волновой пластины (ВП)]. Квантовые ключи отправлялись блоками из 2880 бит. Программируемая логическая интегральная схема (ПЛИС) управляла четырьмя лазерами с частотой 2,5 МГц. Из-за ограничений с передачей данных ПЛИС скорость передачи ключей составляла 30 кбит/ с. Фотоны были соединены в одномодовое волокно, затем на делителе (Д) 95% сигнала отправлялись к телескопу передатчика и 5% к однофотонному детектору (ДОФ), используемому для оценки среднего числа фотонов на импульс. В телескопической системе разделитель пучка (Д) доставляет половину фотонов на поляризатор, а другую половину на q-пластинку с топологическим зарядом $q = 1/2$. Поляризатор вместе с контроллером поляризации (КП) позволяет устройству отправителя корректировать поляризованные вращения, вызванные волокном. Q-пластинка превращает кубиты, закодированные поляризационными состояниями (H и V), в кубиты, закодиро-

ванные в гибридных поляризационных состояниях с угловыми моментами (L и R). После q-пластинки фотоны попадают в 12-сантиметровый апертурный телескоп с фокусным расстоянием f 1/4 900 мм (увеличение 12 $\times$) и отправляются на приемную станцию. Увеличение было выбрано для того, чтобы иметь почти коллимированный луч между передатчиком и приемником. На приемной стороне был использован телескоп с апертурой большей, чем диаметр пучка, чтобы свести к минимуму дифракционные эффекты. Телескоп установлен на ступени вращения, что обеспечивает жесткий поворот всего передающего устройства. На приемном устройстве 5-сантиметровый апертурный телескоп принимал фотоны (с потерями на дифракции порядка 2%), а вторая q-пластинка декодировала гибридные кубитные состояния в поляризационные кубиты. Затем сигнал собирался в одномодовое волокно и доставлялся в измерительное устройство, состоящее из делителя луча (Д), $\lambda/4$ волновой пластины (ВП) и двух поляризационных делителей (ПД). Четыре разных однофотонных детектора были связаны с четырьмя поляризационными состояниями H, V, R и L. Длина линии связи составляла 210 м.

В работах [33, 34] было продемонстрирована передача квантовых ключей на расстояние 300 м между зданиями в Оттаве (Канада). Для кодирования квантовых состояний использовались как свободные, так и орбитальные угловые моменты одиночных фотонов. Такая комбинация оптических угловых моментов позволила авторам создать 4-мерное квантовое состояние, в котором, используя известный протокол BB84, коэффициент квантовых ошибок составил 11% с соответствующей скоростью передачи 0,65 бит на фотон. Для сравнения, для случая 2-мерных структурированных фотонов достигается частота ошибок 5% со скоростью 0,43 бит на фотон. Таким образом, в работе было продемонстрировано, что использование 4-мерных состояний фотонов с орбитальным угловым моментом, помимо инвариантности к повороту к телескопическим приемно-передающим системам, обеспечивает более высокие скорости передачи квантовых бит.

5.7 Контрольные вопросы

1. На какое рекордное расстояние была экспериментально продемонстрирована передача квантового состояния света на земле через атмосферный канал связи?

2. Какие два подхода применяются для решения проблемы ограниченной дальности передачи квантовых ключей по волоконным линиям связи?

3. Что представляет собой схема доверенного узла?

4. С какой целью был предложен уникальный способ кодирования кубитов с использованием "закрученного"света?

5. Что является основными ограничивающими факторами передачи квантовой информации от спутника к земной станции?

6 Квантовые генераторы случайных чисел

6.1 Генерация случайных чисел и сферы её применения

Случайные числа используются во множестве отраслей. Например, в криптосистемах степень непредсказуемости ключа для шифрования информации во многом зависит от качества генератора случайных чисел, используемого в данной системе. В схемах квантовой криптографии случайным образом могут выбираться базис, а также состояние фотона. В классической криптографии роль случайных чисел тоже велика. Случайные числа также используются для проверки подлинности пользователя при предоставлении ему доступа к каким-либо данным, то есть для осуществления процедуры аутентификации.

В различных отраслях науки для моделирования сложных систем разработаны методы, опирающиеся на использование случайных чисел. Эти методы имеют большое значение для современного численного моделирования (метод Монте-Карло, методы имитационного моделирования и т. д.). Также генерация случайных чисел используется в лотереях и теории игр для гарантии одинаковой вероятности выигрыша. Однако несмотря на то, что случайные числа используются повсеместно, и мы к ним давно уже привыкли, не может не возникнуть вопрос: «Почему мы считаем некоторые числа случайными, а некоторые – нет?».

Могут быть даны различные определения случайности, но общий смысл заключается в том, что случайные числа — это числа, порожденные процессом, исход которого непредсказуем и который не может быть надежно воспроизведен впоследствии. Цифры, символы или биты в случайной последовательности не должны быть связаны между собой, чтобы информация об одном из элементов последовательности не несла информации о других и не могла быть использована в прогнозировании. При этом если перед нами лишь одно число, то мы не можем абсолютно ничего сказать про степень его случайности. Для последовательности бесконечной длины мы уже можем вынести вердикт о её случайности (последовательность является случайной, если количество информации, содержащейся в ней, бесконечно), но в реальности мы никогда не можем встретить бесконечно длинную последовательность. Для реальной генерации случайных чисел может использоваться численная характеристика значений некоторой зарегистрированной в заданный момент времени случайной величины. И мы можем только сравнить её статистические свойства со статистическими свойствами идеальных случайных последовательностей.

На данный момент наиболее распространенными подходами к генерации случайных чисел являются два класса систем: основанные на программном обеспечении (алгоритмические или псевдослучайные генераторы случайных чисел (ГСЧ)) и ГСЧ, основанные на физических процессах (физические или аппаратные ГСЧ).

Так как компьютер является детерминированной системой, то алгоритмический ГСЧ, используя в качестве источника одинаковый набор данных, всегда будет выдавать одинаковый результат генерации. Полученная последовательность может успешно пройти несколько статистических тестов на случайность, но её всегда можно воспроизвести, то есть она является предсказуемой. Именно поэтому алгоритмические генераторы не являются генераторами истинно случайных чисел, такие генераторы называются генераторами псевдослучайных чисел. Никакой детерминированный алгоритм не может генерировать полностью случайные числа, он может только аппроксимировать некоторые их свойства. Однако псевдослучайные числа можно использовать для тех приложений, которые не требуют абсолютной непредсказуемости случайной последовательности, например, для математического моделирования сложных физических систем.

Если использование псевдослучайных чисел не является приемлемым (при проведении электронных коммерческих операций, шифровании персональных данных, в криптографических или иных системах, где необходим высокий уровень конфиденциальности данных), требуется использование аппаратного ГСЧ, основанного на доверенном источнике энтропии. Такие ГСЧ работают на основе измерения параметров сложного и непредсказуемого физического процесса, который можно описать при помощи уравнений классической или квантовой физики. На сегодняшний день разработаны ГСЧ на основе различных физических процессов, например, электрических шумов тока в резисторе, радиоактивного распада, турбулентности атмосферы, космического излучения, фотоэффекта и различных квантовых явлений.

Одним из недостатков физических генераторов случайных чисел является возникновение смещенных последовательностей (в подобных последовательностях определенная комбинация чисел, символов или битов повторяется чаще других). Такое смещение возникает из-за сложности в разработке и реализации точно сбалансированных физических схем генерации случайных чисел. Однако для удаления подобного смещения существуют алгоритмы последующей обработки. Традиционно для создания ГСЧ использовались макроскопические процессы (это связано с их простотой и доступностью), которые могут быть описаны при помощи уравнений классической физики. К этому подтипу принадлежит

один из простейших и древнейших ГСЧ — бросание монеты. Последовательности случайных чисел, полученные при помощи физических генераторов случайных чисел, основанных на использовании макроскопических процессов, являются детерминированными, но их предсказание является трудновыполнимой задачей. Если макроскопические процессы можно охарактеризовать при помощи уравнений классической физики, то для квантовых процессов не используется полностью детерминированное описание движения отдельных частиц, в связи с тем, что природа данных процессов является вероятностной. Вероятностная природа квантового случайного процесса позволяет выбрать его в качестве источника энтропии для построения генератора истинно случайных чисел. Подобные системы называются квантовыми генераторами случайных чисел (КГСЧ).

6.2 Системы квантовой генерации случайных чисел

Наибольшее распространение получили два основных класса систем квантовой генерации случайных чисел:

- КГСЧ, использующие детекторы одиночных фотонов или детекторы одиночных фотонов с возможностью определения числа фотонов в импульсе;
- КГСЧ, использующие фотодетекторы.

Для каждого из них характерны свои особенности, далее они будут рассмотрены более подробно.

6.3 Квантовые генераторы случайных чисел, использующие детекторы одиночных фотонов или детекторы одиночных фотонов с возможностью определения числа фотонов в импульсе

В квантовых генераторах случайных чисел для регистрации сигналов используются детекторы одиночных фотонов (ДОФ), что позволяет производить точные измерения однофотонных импульсов для различных КГСЧ. Устройства данного класса можно условно разделить на несколько типов:

- КГСЧ, основанные на пространственном разделении излучения [35, 36]

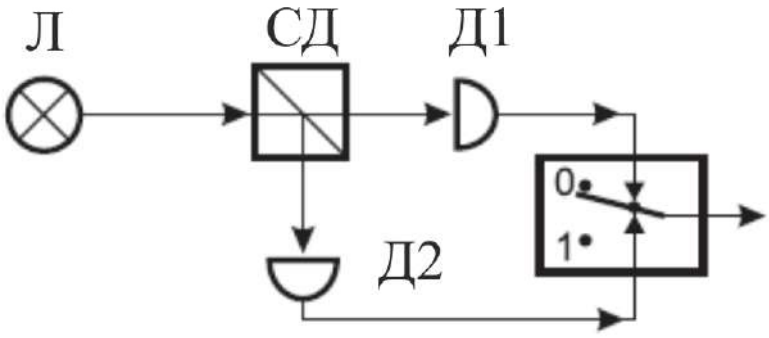


Рис. 40: Схема КГСЧ, который основан на разделении пути следования одиночных фотонов при помощи оптического светоделителя СД с коэффициентом деления 50/50 с использованием двух детекторов[35]

- КГСЧ, основанные на использовании массива из детекторов одиночных фотонов [37, 38]
- КГСЧ, основанные на времени детектирования фотонов [39, 40]
- КГСЧ, основанные на явлении квантовой запутанности [41, 42]
- КГСЧ, основанные на определении числа фотонов в импульсе [43, 44]

6.3.1 Квантовые генераторы случайных чисел, основанные на пространственном разделении излучения

Этот подход стал первым, примененным для КГСЧ в связи с простотой используемых в нем схем генерации случайных последовательностей. Реализации подобных КГСЧ используют прохождение фотонов через оптический светоделитель [35] или волоконный разветвитель [36], прохождение поляризованных фотонов через поляризационный делитель [35].

Работа системы, предложенной в статье [35], заключается в следующем: лазер (Л) испускает фотон, который после попадания на оптический светоделитель (СД) идет с равной вероятностью по первому или второму оптическому пути, итоговый сигнал регистрируется на одном из двух детекторов одиночных фотонов (рисунок 40).

Если срабатывает детектор одиночных фотонов Д1, то в последовательность случайных битов записывается бит «1», в случае срабатывания детектора одиночных фотонов Д2 записывается бит «0». Если от источника исходит более одного фотона и происходит срабатывание на обоих

детекторах, то запись бита случайной последовательности не производится. Скорость генерации на данных устройствах достигает порядка 1 Мбит/с. В данной схеме можно также использовать поляризационный светоделитель. Основным отличием является использование поляризованного излучения при генерации СЧ. Процесс генерации случайных последовательностей состоит в следующем: лазер (Л) испускает фотон, который после прохождения через поляризатор (П) приобретает поляризацию 45°, далее он поступает на поляризационный светоделитель (ПСД), который пропускает на один выход излучение, поляризованное под углом 0°, а на другой – излучение, поляризованное под углом 90°, таким образом вероятность попадания излучения с поляризацией 45° на каждый из двух выходов одинакова и составляет 50%, итоговый сигнал регистрируется на детекторах одиночных фотонов (рисунок 41).

Процесс преобразования сигналов с детекторов Д1 и Д2 в итоговую последовательность случайных битов аналогичен указанному для предыдущей схемы.

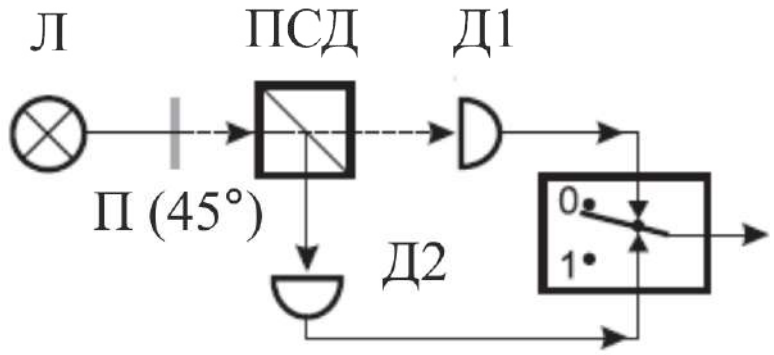


Рис. 41: Схема КГСЧ, реализуемая при помощи поляризационного делителя пучка с коэффициентом деления 50/50 в случае, когда падающий свет поляризован на 45º относительно ПСД

Для экономии могут также использоваться квантовые генераторы случайных чисел, основанные на разделении пути следования фотонов при помощи оптического светоделителя и использующие один детектор одиночных фотонов. Схема системы КГСЧ, использующей задержку по времени на одном из путей, по которым проходят одиночные фотоны [36], приведена на рисунке 42.

Ослабленное до уровня одиночных фотонов излучение исходит от светоизлучающего диода (СИД), излучение от которого поступает в одномодовое волокно. Далее фотон поступает в одно из двух многомодовых волокон, время задержки между ними составляет 60 нс. Время регистра-

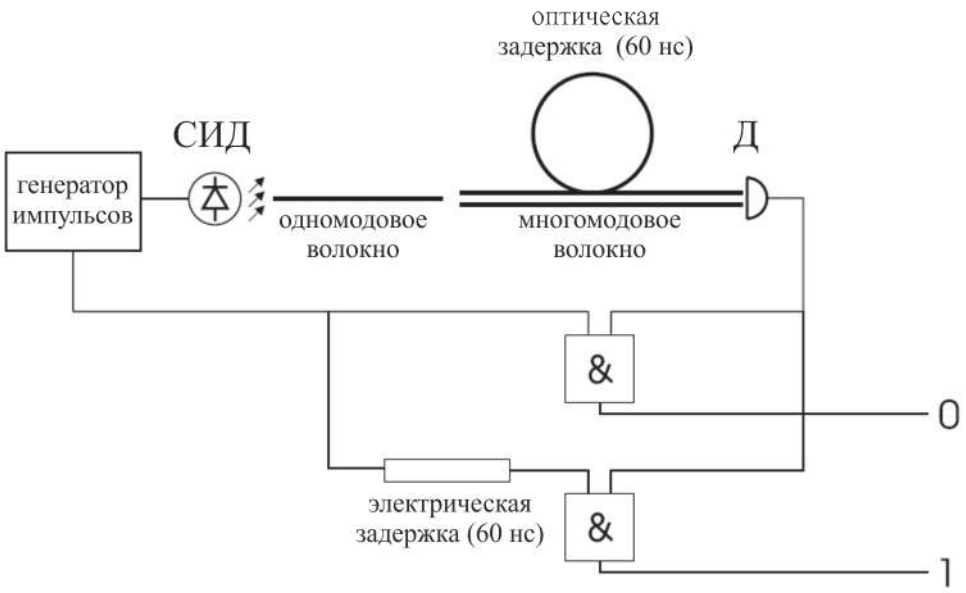


Рис. 42: Схема КГСЧ, основанного на разделении пути следования одиночных фотонов и использующая один детектор [36]

ции фотона при детектировании определяет, по какому из двух возможных путей он прошел. Обозначив битом «0» короткий путь, а длинный – битом «1», получим итоговую последовательность случайных битов. В такой схеме используется только один детектор, но подобный подход приводит к потерям в скорости генерации, к тому же вероятности получения во время генерации единиц и нулей не в точности равны из-за различия оптических путей, проходимых фотонами. Скорость генерации составляет примерно 100 Кбит/с [36].

В целом КГСЧ на основе детектирования одиночных фотонов после разделения путей их следования просты, но обладают существенным недостатком: в случае попадания на светоделитель одновременно нескольких фотонов процесс генерации происходит некорректно. Эффективный однофотонный источник, имеющий большое значение для схем с разделением пути следования одиночных фотонов, еще не существует, поэтому на практике схемы осуществляются на ослабленных лазерных импульсах, в связи с этим практическая реализация в этом случае не может быть исполнена корректно. Также несовершенством систем квантовой генерации случайных чисел, основанных на разделении излучения, является асимметрия схемы: вероятности получения в процессе генерации нулей и единиц не в точности равны из-за различия проходимых фотонами путей, а в схемах, где используются два или более детекто-

ра, различными являются также квантовые эффективности детекторов. Помимо прочего, детекторы одиночных фотонов очень чувствительны к флуктуациям напряжения или к изменению температуры окружающей среды. Поэтому необходимо стремиться к тому, чтобы детекторы обладали именно такой эффективностью, которая могла бы компенсировать различие путей следования фотонов, а также сохраняли эту эффективность постоянной. КГСЧ данного типа должны быть очень точно настроены перед использованием. Существуют также проблемы со стабильностью настройки данных устройств во время длительного использования.

6.3.2 Квантовые генераторы случайных чисел, основанные на использовании массива из детекторов одиночных фотонов

Чтобы иметь возможность кодировать более чем один бит за время одного отсчета, применяются КГСЧ, основанные на использовании пространственного кодирования при помощи массивов из детекторов одиночных фотонов. Квантовая генерация случайных чисел, основанная на пространственной регистрации фотонов, была продемонстрирована с использованием схемы детектирования, использующей мультипиксельный массив детекторов одиночных фотонов [37], как показано на рисунке 43.

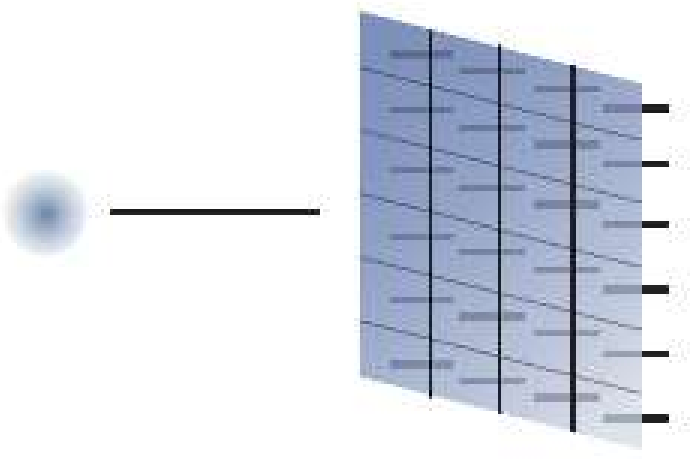


Рис. 43: Иллюстрация процесса детектирования в схеме КГСЧ, использующей массив однофотонных детекторов [45]

В этой схеме испускаемый лазером фотон может быть зарегистрирован любым детектором одиночных фотонов из массива. В зависимости

от того, какой именно из детекторов зарегистрирует фотон, в последовательность случайных битов записываются закодированные координаты (каждой координате соответствует свой код из нескольких битов) сработавшего детектора. В данном случае последовательность случайных битов зависит не только от пространственного распределения интенсивности света, но и от соотношения характеристик ДОФ, входящих в массив детекторов. В описываемой выше системе КГСЧ на пути фотона от источника до массива детекторов одиночных фотонов не было установлено никаких дополнительных устройств. Ниже приведен пример системы, в которой для наилучшего пространственного разделения пути следования фотонов оптический путь фотонов изменяется при помощи дополнительных элементов схемы, такими элементами могут быть разветвители излучения с одним входным и несколькими выходными портами, а также призмы или дифракционные решетки. На рисунке 44 представлена схема квантового генератора случайных чисел, использующего отражение фотонов от дифракционной решетки под различными углами с последующей регистрацией угла отклонения [38].

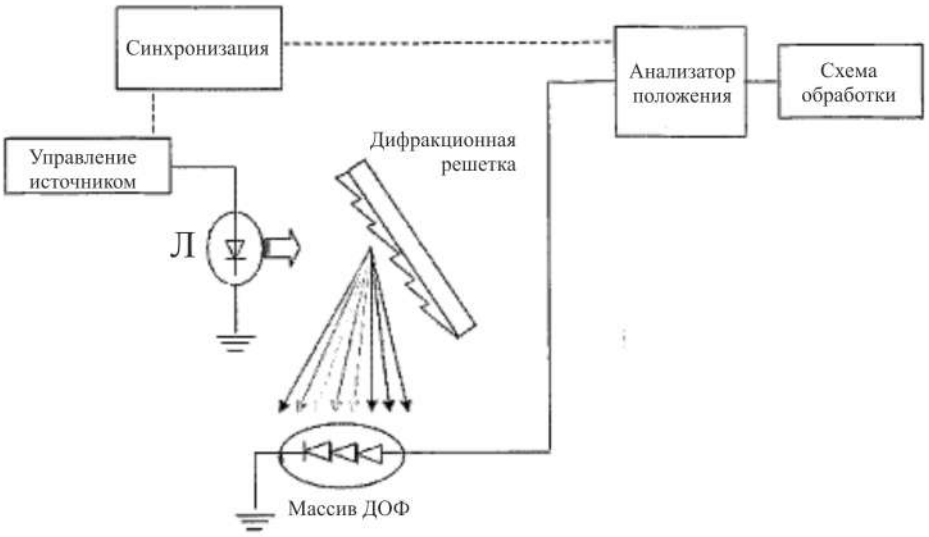


Рис. 44: Схема квантового генератора случайных чисел, использующего дифракционную решетку [38]

Некогерентным лазерным источником (Л) создаются одиночные фотоны, которые, попав на дифракционную решетку, отражаются от нее на

некоторый случайный угол относительно нормали в зависимости от длины волны (за счет чего происходит пространственное разделение пути следования фотонов) и попадают на массив ДОФ. Генерация итогового случайного сигнала зависит от расположения детектора, зарегистрировавшего фотон. Схемы КГСЧ, основанные на использовании массивов из детекторов одиночных фотонов, позволяют кодировать события одного отсчета при помощи нескольких битов итоговой последовательности. Из-за наличия в схеме нескольких ДОФ необходима точная калибровка детекторов для того, чтобы их параметры были максимально схожи, и не возникало статистического смещения. Также с увеличением числа детекторов возрастает стоимость устройства.

6.3.3 Квантовые генераторы случайных чисел, основанные на регистрации времени детектирования фотонов

В предыдущих разделах главным образом рассматривалось прохождение одиночными фотонами по одному из нескольких возможных путей распространения излучения, регистрировались пространственные координаты. В КГСЧ, рассматриваемых в данном разделе, главную роль играет время регистрации фотонов. На данный момент разработаны несколько типов схем, использующих случайность эмиссии и последующего обнаружения фотонов при помощи фотоэффекта [39, 40]. В них в качестве источника излучения обычно применяется низкоэффективный светоизлучающий диод (СИД). При использовании достаточно низкой мощности диод испускает независимые друг от друга фотоны, при этом их испускание может быть охарактеризовано при помощи случайного пуассоновского процесса. Когда каждый фотон достигает фотокатода, есть некоторая вероятность, что из-за фотоэлектрического эффекта произойдет излучение электрона. Создание фотоэлектрона является, таким образом, истинно случайным событием. Такая система производит пуассоновские случайные события в виде последовательности цифровых импульсов. Суть одного из методов извлечения случайных битов [40] заключается в последовательном рассмотрении пар неперекрывающихся случайных промежутков времени (t1, t2), которые определены при помощи последовательности случайных событий, и генерации бита «0», если выполняется условие $t1<t2$, или бита «1», когда данное условие не выполняется. Недостатком данного метода является ограничение скорости генерации, обусловленное тем, что после обнаружения фотона детектор становится неспособным к регистрации фотонов в течение некоторого периода времени. В квантовом генераторе случайных чисел, используемом в работе [39], эффекты нечувствительности детекторов, связанные с осо-

бенностями работы фотоумножителей, использовались для того, чтобы избежать необходимости последующей обработки данных. События регистрации фотонов подсчитывались в течение некоторого интервала времени выборки и фиксировались как бит «0» для четного номера отсчета и бит «1» — для нечетного. Достоинствами систем квантовой генерации случайных последовательностей на основе времени детектирования фотонов являются отсутствие необходимости контроля числа испускаемых фотонов, а также возможность кодировать несколькими битами события одного отсчета. Основным недостатком систем подобного типа является наличие времени нечувствительности у ДОФ, ограничивающего скорость генерации.

6.3.4 Квантовые генераторы случайных чисел, основанные на явлении квантовой запутанности

Реализации схем, основанных на явлении квантовой запутанности [41, 42], имеют преимущество в том, что становится возможным подавление большей часть паразитного шума при использовании схемы совпадений на детекторах. КГСЧ данного типа, описанный в работе [41], использует поляризационно-запутанные фотонные пары (рисунок 45). Для реализации этой схемы необходимо поддержание чистоты поляризации запутанных состояний, что является нетривиальной экспериментальной задачей, также возникает необходимость квантовой томографии состояний.

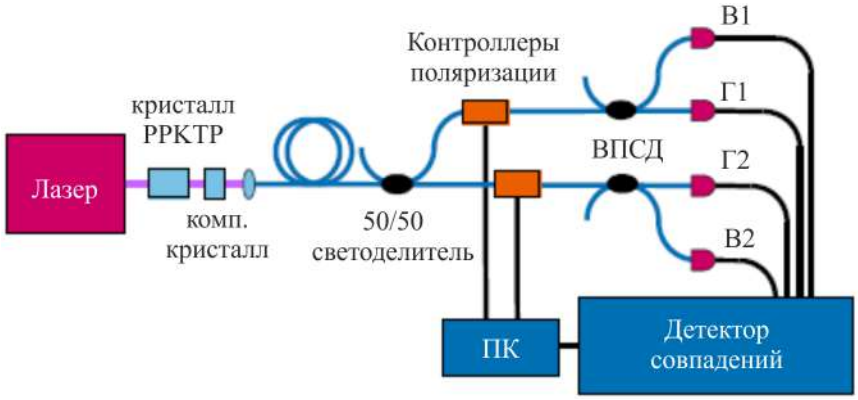


Рис. 45: Схема КГСЧ, основанного на поляризационно-запутанных фотонных парах [41]

Поляризационно-запутанные фотоны, произведенные при помощи спонтанного параметрического рассеяния (СПР) в кристалле PPKTP, после разделения на светоделителе с коэффициентом деления 50/50 поступа-

ют на контроллеры поляризации, затем на волоконные поляризационные делители пучка (ВПСД), после прохождения которых анализируются при помощи детекторов одиночных фотонов (детекторы Г1 и Г2 регистрируют горизонтально поляризованные фотоны, детекторы В1 и В2 — вертикально поляризованные). Детектирование совпадений регистрации фотонов на Г1+В2 записывается в итоговую последовательность как «0», на В1+Г2 – «1». Скорость генерации для данной схемы составляет 5.3 Кбит/с. Явление квантовой запутанности также используется в работе [42], но обработка получаемых данных происходит иным образом. В данном случае генерация СЧ основана на состоянии квантовой запутанности фотонов, подготовленных путем двухфотонной квантовой интерференции на светоделителе (рисунок 46).

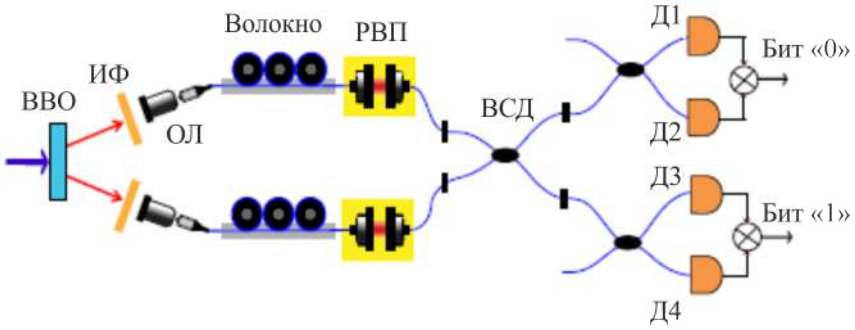


Рис. 46: Схема КГСЧ, использующего запутанные фотоны, подготовленные путем двухфотонной квантовой интерференции на светоделителе [42]

Для генерации одиночных фотонов используется ослабленное излучение диодного лазера, далее на кристалле ВВО в процессе СПР из одного исходного фотона генерируется пара фотонов с меньшей энергией. Два интерференционных фильтра (ИФ) используются для сокращения нежелательного шума, после этого фотоны попадают при помощи линз (ОЛ) в одномодовое оптическое волокно, а затем в волоконный светоделитель (ВСД) с коэффициентом деления 50/50. Контроллеры поляризации волокна (ПК) используются для обеспечения одинакового состояния поляризации фотонов, а регулируемые воздушные промежутки (РВП) предназначены для управления разницей в регистрации прибытия фотонов в ВСД. Когда пара полученных при помощи СПР идентичных фотонов прибывает одновременно в ВСД через различные входные порты, то имеет место квантовая двухфотонная интерференция, в результате которой два фотона всегда выходят из ВСД через один порт. Случайность совпадения регистрации на детекторах Д1+Д2 или на детекторах

Д3+Д4 является равновероятной квантовомеханической случайностью. Эти совпадения можно использовать, чтобы выделить итоговую битовую последовательность. Совпадения времени регистрации фотонов на детекторах Д1+Д2 и на детекторах Д3+Д4 происходят беспорядочно из-за запутанного состояния фотонов. В случае совпадения времени регистрации фотонов на детекторах Д1+Д2 или на детекторах Д3+Д4 в итоговую последовательность битов дописываются значение бита «0» или «1» соответственно. В случае, когда имеются более одного такого события в пределах временного отсчета, фиксируется ошибка. Для использования данного типа измерений необходимо гарантировать, что измеряется именно запутанное состояние (для этого необходимо удерживать воздушный промежуток в нулевой позиции задержки и при этом постоянно контролировать совпадение на детекторах Д1+Д3). В противном случае результат на выходе будет характеризоваться как классический случайный процесс из-за многократного деления пути следования фотонов и последующего измерения совпадений. Скорость генерации в данной системе составляет 668 Кбит/с. Достоинствами схем квантовой генерации случайных последовательностей, основанных на явлении квантовой запутанности, является возможность проверить, что имеют место именно квантовые эффекты, так как при ложных срабатываниях ДОФ биты в итоговую последовательность случайных чисел не записываются. Недостатком подобных систем является сложность их реализации и настройки.

6.3.5 Квантовые генераторы случайных чисел, использующие детекторы одиночных фотонов с возможностью определения числа фотонов в импульсе

Случайные последовательности могут быть получены не только посредством измерения однофотонных состояний, но также и измерением состояний, в которые входят несколько фотонов[43, 46, 44]. Например, когерентное состояние $|\alpha\rangle$ является суперпозицией состояний с различным числом фотонов $|n\rangle$ определяется выражением (57) Таким образом, измеряя число фотонов в когерентном лазерном импульсе при помощи детекторов одиночных фотонов с возможностью определения числа фотонов в импульсе, можно получить случайные числа, которые могут быть охарактеризованы при помощи пуассоновского распределения. Схемы КГСЧ, построенные на детектировании одиночных фотонов с возможностью определения числа фотонов в импульсе, являются чувствительными как к распределению числа фотонов, излучаемых источником, так и к эффективности детектирования, что требует точной настройки. Схе-

мы состоят только из источника и детектора, и позволяют кодировать в одном отсчете несколько битов. Данные КГСЧ также являются ограниченными по скорости в связи с использованием детекторов одиночных фотонов.

6.4 Квантовые генераторы случайных чисел, использующие классические фотодетекторы

Основным недостатком всех схем, использующих ДОФ, является ограничение по скорости генерации, вызванное нечувствительностью детекторов после срабатывания, также заметна зависимость характеристик ДОФ от изменения температуры окружающей среды или от флуктуаций напряжения. Таким образом, возникает необходимость точной настройки и стабильности данных устройств во время длительного использования. Для решения этих проблем были предложены схемы квантовой генерации случайных чисел, в которых используются классические фотодетекторы. В этом разделе будут рассмотрены КГСЧ данного класса, основанные на фазовых или амплитудных шумах лазера [46, 47] и основанные на флуктуациях вакуума [48].

6.4.1 Квантовые генераторы случайных чисел, основанные на лазерных шумах

Схема КГСЧ, основанного на измерении квантового фазового шума одномодового полупроводникового лазера, который работает на ослабленной интенсивности излучения вблизи порога лазерной генерации была представлена в работе [47] (рисунок 47). Источником фазового шума лазера является спонтанное излучение: каждый случайным образом испускаемый фотон имеет свою фазу, которая вносит случайное колебание фазы в общее электрическое поле, вследствие чего происходит уширение спектральной линии. Спонтанная эмиссия фотонов и соответствующий ей фазовый шум имеют квантовомеханическое происхождение. Скорость генерации случайных чисел в данной схеме может достигать 500 Мбит/с.

Одномодовый непрерывный диодный лазер, работающий на длине волны 1.5 мкм, с распределенной обратной связью используется в качестве лазерного источника. Симметричные волоконные разветвители создают собой волоконный интерферометр Маха-Цендера (ИМЦ) с расхождением длин плеч L. Интерференционные сигналы от ИМЦ поступают в два канала обнаружения: один из них запускает фотодетектор (Д1) и быструю карту сбора данных (КСД1) для генерации случайных чисел. Другой поступает на 1 МГц фотоприемник (Д2) для контроля

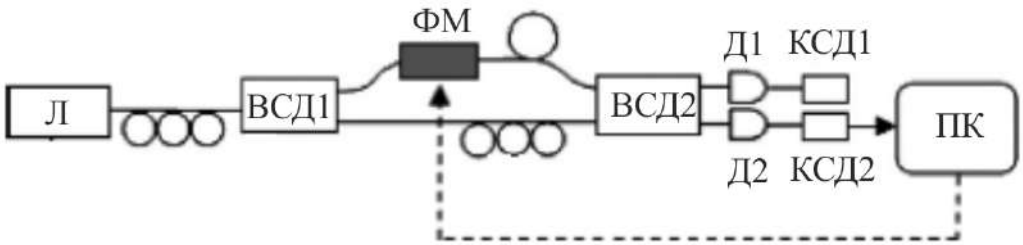


Рис. 47: Схема установки, основанной на измерении квантового фазового шума [47]. Л – лазер, ВСД1, ВСД2 – симметричные волоконные светоделители, Д1 – фотодетектор, КСД1 –карта быстрого сбора данных, Д2 – 1 МГц фотоприемник, КСД2 –карта медленного сбора данных, ФМ – фазовый модулятор

медленного фазового дрейфа ИМЦ из-за температурных колебаний и медленную карту сбора данных (КСД2), которая обеспечивает отправку сигнала управления обратной связи на фазовый модулятор (ФМ) внутри ИМЦ. Для создания последовательностей случайных битов производится сравнение полученного в момент времени ti результата выборки S(ti) и среднего значения S0, если S(ti) больше S0, то биту присваивается значение «1», если S(ti) меньше S0 , то биту присваивается значение «0». Для генерации случайных последовательностей в работе [46] используется интенсивность колебаний хаотического полупроводникового лазера. Преобразование хаотических колебаний в случайную последовательность бит может быть осуществлено при помощи программного обеспечения или при помощи аппаратных средств. Рисунок 48 демонстрирует схему установки.

В схеме в качестве источника излучения используется полупроводниковый многомодовый лазер. Зарегистрированный лазерный сигнал дискретизируется при помощи 8-битового аналого-цифрового преобразователя (АЦП) и далее используется для формирования битовой последовательности: цифровой сигнал запоминается, и при помощи программного обеспечения находится разность между последовательными значениями, некоторое число m<8 младших двоичных разрядов от этой разности значений запоминаются как следующие m бит в итоговой последовательности СЧ. Скорость генерации случайных чисел в данной схеме, таким образом, достигает m битов за один отсчет АЦП, и m может варьироваться в пределах зависящего от разрешения АЦП максимального значения. Скорость генерации в установке [46] составляет 12.5 Гбит/с. Достоинствами систем квантовой генерации случайных чисел, основан-

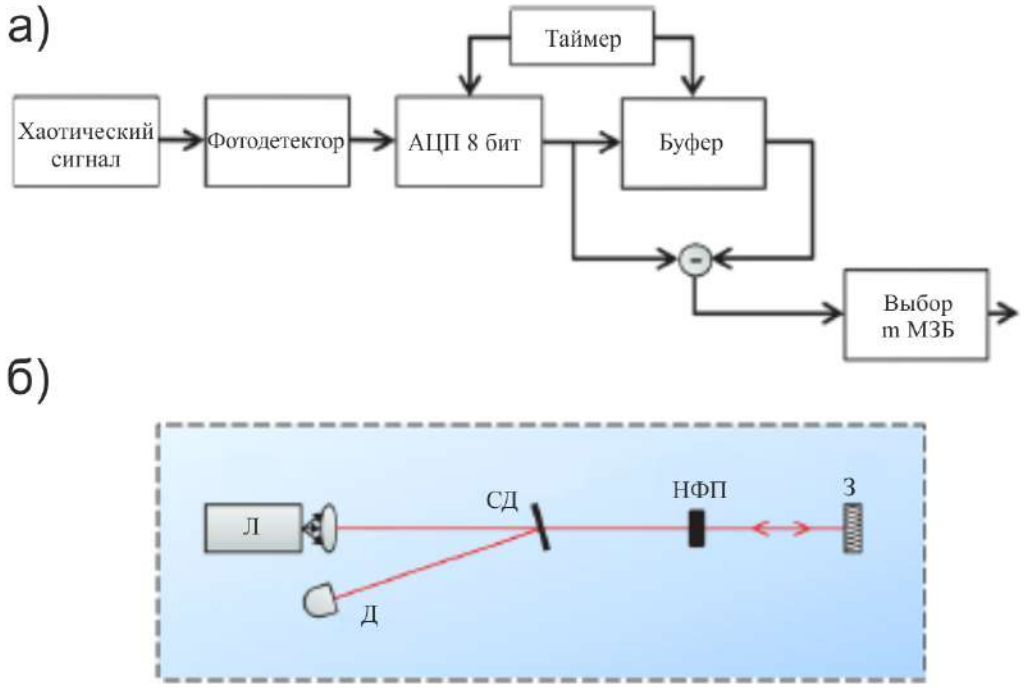


Рис. 48: (а) Схема КГСЧ, основанного на интенсивности колебаний хаотического полупроводникового лазера [46], (б) Лазерная реализация: лазерный диод (Л), делитель пучка (СД), нейтральный фильтр плотности (НФП), высокоскоростной фотодетектор (Д), зеркало (З)

ных на фазовых или амплитудных шумах лазера, являются простота исполнения и высокая скорость генерации, недостатком является невозможность проверить, является ли измеряемый шум квантовым, или же он обусловлен классическими эффектами.

6.4.2 Квантовые генераторы случайных чисел, основанные на флуктуациях вакуума

Принципом работы КГСЧ этого типа является извлечение случайности из квантового шума, получаемого после вычитания на балансном детекторе сигналов, полученных с выходов светоделителя. На один из входов светоделителя при помощи лазера (Л) подается когерентное состояние, а на второй — вакуум, на светоделителе (СД) эти сигналы смешиваются, а затем сигналы с его выходов поступают на балансный детектор (состоящий из фотодиодов Д с одинаковыми характеристиками и вычитателя), где сигналы вычитаются друг из друга, а затем переводятся в цифро-

вой формат при помощи АЦП (рисунок 49). Итоговый сигнал является квантовым шумом, который можно при помощи последующей обработки (ПО) преобразовать в случайную последовательность битов. Основным преимуществом такой схемы [48] является измерение квантовых состояний при помощи классических детекторов за счет использования гомодинного детектирования. Скорость генерации в этой системе составила 2 Гбит/с. В работе [48] были использованы два метода обработки квантового шума (один из них – с защитой от постороннего вмешательства).

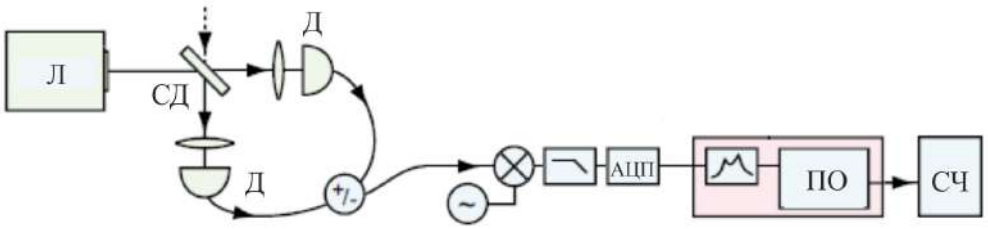


Рис. 49: Схема КГСЧ, основанного на флуктуациях вакуума [48]

Устройства квантовой генерации случайных чисел, основанные на флуктуациях вакуума, позволяют получать истинно-случайные последовательности, используя классические фотодетекторы, а также обладают высокой скоростью генерации, надежным источником энтропии и, соответственно, высокой степенью случайности генерируемых последовательностей, также они устойчивы к внешнему воздействию. [38]

6.5 Контрольные вопросы

1. Почему алгоритмические генераторы случайных чисел не являются генераторами истинно случайных чисел?

2. На чем основаны аппаратные генераторы случайных чисел?

3. Недостатки физических генераторов случайных чисел?

4. Какие системы называются квантовыми генераторами случайных чисел?

5. Приведите и поясните принцип работы схемы квантового генератора случайных чисел, основанного на пространственном разделении излучения.

6. Недостаток квантового генератора случайных чисел на основе детектирования одиночных фотонов после разделения путей их следования?

7. Для чего применяются квантового генератора случайных чисел, основанные на использовании пространственного кодирования при помощи массивов из детекторов одиночных фотонов?

8. Приведите и поясните принцип работы схемы квантового генератора случайных чисел, использующего дифракционную решетку.

9. Преимущество схем, основанных на явлении квантовой запутанности?

10. Приведите и поясните принцип работы схемы квантового генератора случайных чисел, основанного на измерении квантового фазового шума.

11. Приведите и поясните принцип работы схемы квантового генератора случайных чисел, основанного на флуктуациях вакуума.

7 Спонтанное параметрическое рассеяние

7.1 Введение

Процесс спонтанного параметрического рассеяния был предсказан в работах российского ученого и профессора МГУ Давида Николаевича Клышко [49] в 1967 году в результате активных исследований и разработок в области квантовой и нелинейной оптики. В течение нескольких последующих лет ряд экспериментальных групп подтвердили существование данного явления на практике [50, 51, 52]. Впоследствии явление СПР активно исследовалось как с теоретической, так и с практической точек зрения и на сегодняшний день является неотъемлемой частью квантовой физики и применяется во многих исследованиях, часть из которых будет рассмотрена в данном пособии.

7.2 Математическое описание

Воспользовавшись уравнениями Максвелла, получим систему связанных дифференциальных уравнения для трёхчастотного взаимодействия, чем и является параметрическая генерация [53]:

$$\begin{aligned}
\frac{dA_p}{dz} &= -i\frac{2\pi\omega_p^2}{k_p c^2}\chi^{(2)} A_s A_i e^{-i(k_p-k_i-k_s)z} \\
\frac{dA_s}{dz} &= -i\frac{2\pi\omega_s^2}{k_s c^2}\chi^{(2)} A_p A_i^* e^{-i(k_p-k_i-k_s)z} \\
\frac{dA_i^*}{dz} &= -i\frac{2\pi\omega_i^2}{k_i c^2}\chi^{(2)} A_p A_s^* e^{i(k_p-k_i-k_s)z}
\end{aligned} \tag{86}$$

Для решения системы необходимо выполнение следующих условий:

$$\omega_p = \omega_s + \omega_i \tag{87}$$

$$\overrightarrow{k}_p = \overrightarrow{k}_s + \overrightarrow{k}_i \tag{88}$$

где $\omega = \frac{c}{\lambda}$ – частота излучения, c – скорость света в вакууме, λ – длина волны излучения, $k = \frac{2\pi n}{\lambda}$ – волновой вектор, n – показатель преломления, s,i,p – соответствуют сигнальному и холостому излучениям и излучению накачки. Условие (87) называется уравнением баланса частот и представляет собой закон сохранения энергии. Выражение (88) является условием фазового синхронизма. Выполнение этих двух условий приводит к наиболее эффективной реализации процесса параметрической ге-

нерации. В противном случае разность между волновым вектором волны накачки с сигнальным и холостым волновыми векторами является величиной, отличной от нуля. Такую величину называют фазовой расстройкой и обозначают как Δk.

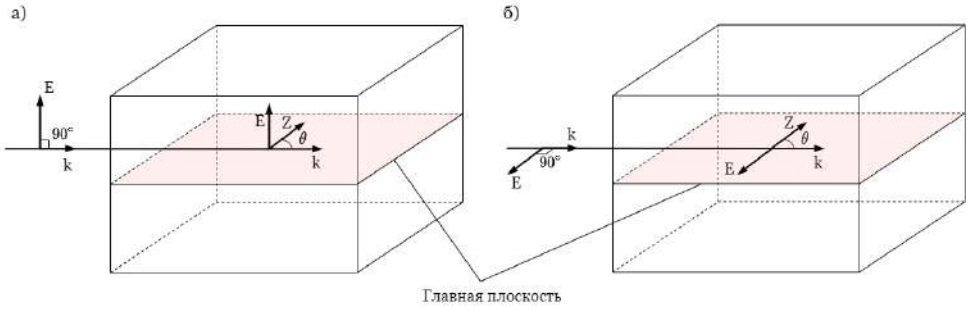


Рис. 50: Главная плоскость кристалла и обыкновенный луч (а), необыкновенный луч (б)

В общем случае выполнение приведённых выше условий невозможно. Однако, существует возможность их выполнения в анизотропных кристаллах с отличной от нуля нелинейной восприимчивостью второго порядка. В таких кристаллах показатель преломления зависит от плоскости поляризации волны (рис. 50). Волну, плоскость поляризации которой перпендикулярна плоскости, образуемой главной осью кристалла и волновым вектором (которую также называют главной плоскостью), называют обыкновенной. Если же плоскость поляризации волны лежит в представленной плоскости, то такую волну называют необыкновенной [54].

Показатель преломления необыкновенной волны зависит от направления распространения внутри кристалла. На рисунке (51) представлены индикатрисы показателей преломления для различных кристаллов. В случае, когда показатель преломления необыкновенной волны больше либо равен показателю преломления обыкновенной волны, такой кристалл называется положительным. В противном случае – отрицательным.

Зависимость показателя преломления необыкновенной волны от направления распространения внутри кристалла описывается следующим выражением [55]:

$$n_e^{eff}(\lambda,\theta) = \left[\frac{\cos^2\theta}{n_o^2(\lambda} + \frac{\sin^2\theta}{n_e^2(\lambda}\right]^{-\frac{1}{2}}, \tag{89}$$

где n_e^{eff} – эффективный показатель преломления необыкновенного луча,

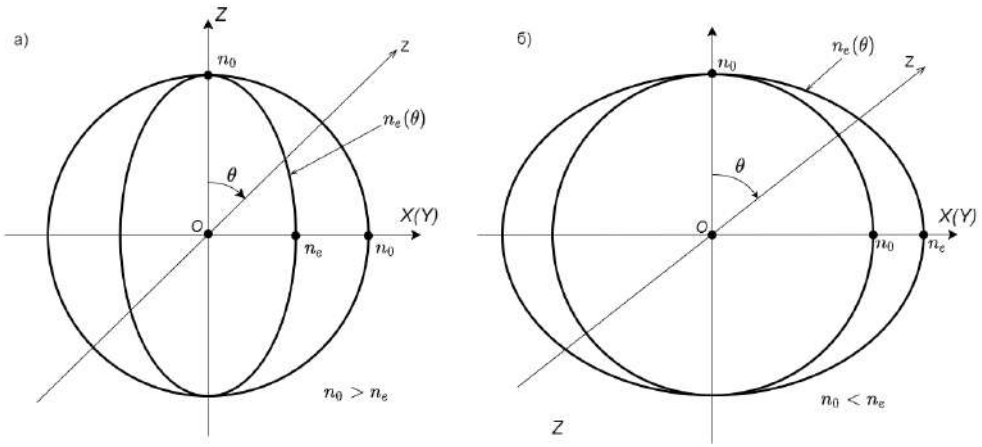


Рис. 51: Индикатрисы показателей преломления а) индикатрисы показателей преломления для отрицательного кристалла б) индикатрисы показателей преломления для положительного кристалла

θ – угол между направлением распространения излучения и оптической осью, n_0 – показатель преломления обыкновенного луча, n_e – показатель преломления необыкновенного луча (здесь важно различать эффективный и обычный показатель преломления необыкновенного луча, которые имеют следующее соотношение $n_e^{eff}(\lambda, 90°) = n_e$).

Показатели преломления кристаллов возможно описать при помощи уравнения Сельмаера. При этом стоит понимать, что данные описания для различных кристаллов отличаются и их значения можно определить экспериментально, найти в публикациях или справочниках.

Исходя из вышеописанного, можно выделить несколько возможных реализаций условий фазового синхронизма, которые называются типами: I-тип и II-тип. Стоит обратить внимание, что реализовать условия синхронизма в анизотропных кристаллах возможно только для волн с определённой поляризацией.

Для I-типа синхронизма плоскость поляризации волны накачки ортогональна плоскостям сигнального и холостого излучений, что можно обозначить как $e \to oo$ или $o \to ee$, выбор зависит от того, положительный или отрицательный кристалл используется. Обозначение о соответствует обыкновенной волне (ordinary), а е – необыкновенной (extraordinary). II-типу соответствует случай, при котором плоскости поляризации генерируемого излучения ортогональны, что можно записать как $e \to eo$ или $o \to eo$.

Другим способом реализации условий, необходимых для параметрической генерации и спонтанного параметрического рассеяния может слу-

жить реализация условий квазисинхронизма [56]. В таком случае фазовая расстройка Δk не равна нулю и компенсируется за счёт вектора обратной решётки $\overrightarrow{G}$. В таком случае уравнение (88) примет вид

$$\overrightarrow{k}_p = \overrightarrow{k}_s + \overrightarrow{k}_i + \overrightarrow{G} \tag{90}$$

Такой тип синхронизма возможно реализовать в периодически поляризованных кристаллах за счёт чередования значения коэффициента нелинейной эффективности при росте кристалла. В таком случае модуль вектора обратной решётки будет равен

$$G = \frac{2\pi m}{\Lambda}, \tag{91}$$

где Λ – период чередования доменов, соответствующих противоположным по знаку значениям коэффициента нелинейной эффективности, m – целое число. Пользуясь данным подходом, возможно реализовать условия квазисинхронизма 0-типа, при котором поляризации всех волн, участвующих во взаимодействии одинаковы ($o \to oo$ и $e \to ee$).

Учитывая, что условия синхронизма и баланса частот выполняются выражения (86) можно переписать следующим образом:

$$\begin{aligned} \frac{dA_s}{dz} &= -i\frac{g}{2}A_i^* \\ \frac{dA_i^*}{dz} &= i\frac{g}{2}A_s \end{aligned} \tag{92}$$

Данная система имеет аналитическое решение следующего вида:

$$\begin{aligned} A_s(z) &= A_1(0)ch\left(\frac{g}{2}z\right) - iA_2^*(0)sh\left(\frac{g}{2}z\right) \\ A_i^*(z) &= A_1(0)ch\left(\frac{g}{2}z\right) + iA_2^*(0)sh\left(\frac{g}{2}z\right) \end{aligned} \tag{93}$$

Анализируя решения системы связанных дифференциальных уравнений, важно обратить внимание на необходимость наличия ненулевых амплитуд сигнального и холостого излучения на входе в кристалл. В эксперименте это соответствует отличным от нуля интенсивностям сигнального и холостого излучений, которые также называются затравочными. Однако было продемонстрировано, что генерация излучения возможна даже без затравочного излучения [57]. Другим важным результатом является зависимость интенсивности генерируемого излучения от интенсивности излучения накачки. Данная зависимость в предельном случае

является экспоненциальной, что, однако, не соответствует экспериментальным данным. Такой случай соответствует спонтанному параметрическому рассеянию.

Для теоретического описания процесса спонтанного параметрического рассеяния в отсутствии затравочного излучения можно воспользоваться гейзенберговским описанием.

Для простоты понимания возможно использовать аналогию с представленными ранее связанными дифференциальными уравнениями. Для этого нужно произвести замену комплескных амплитуд соответствующих волн на операторы рождения и уничтожения, а производную по направлению на производную по времени. В таком случае можно получить следующие уравнения:

$$\begin{aligned} \frac{d\hat{a}_s}{dt} &= -i\frac{s}{2}\hat{a}_i^\dagger \\ \frac{d\hat{a}_i^\dagger}{dt} &= i\frac{s}{2}\hat{a}_s \end{aligned} \tag{94}$$

Данные уравнения позволяют определить временную зависимость используемых операторов, что свойственно для гейзенберговского представления. Решения уравнений будут иметь следующий вид:

$$\begin{aligned} \hat{a}_s(t) &= \hat{a}_s(0)ch\left(\frac{s}{2}t\right) - i\hat{a}_i^\dagger(0)sh\left(\frac{s}{2}t\right) \\ \hat{a}_i^\dagger(t) &= \hat{a}_s(0)ch\left(\frac{s}{2}t\right) + i\hat{a}_i^\dagger(0)sh\left(\frac{s}{2}t\right) \end{aligned} \tag{95}$$

В таком случае число фотонов в моде можно записать следующим образом:

$$\bar{n}_s(t) = n_{10}ch^2\left(\frac{s}{2}t\right) + (1+n_{20})sh^2\left(\frac{s}{2}t\right) \tag{96}$$

Важно заметить, что даже в случае равенства нулю операторов рождения и уничтожения в начале процесса присутствует член, не зависящий от исходного состояния, который имеет квантово-оптическую природу.

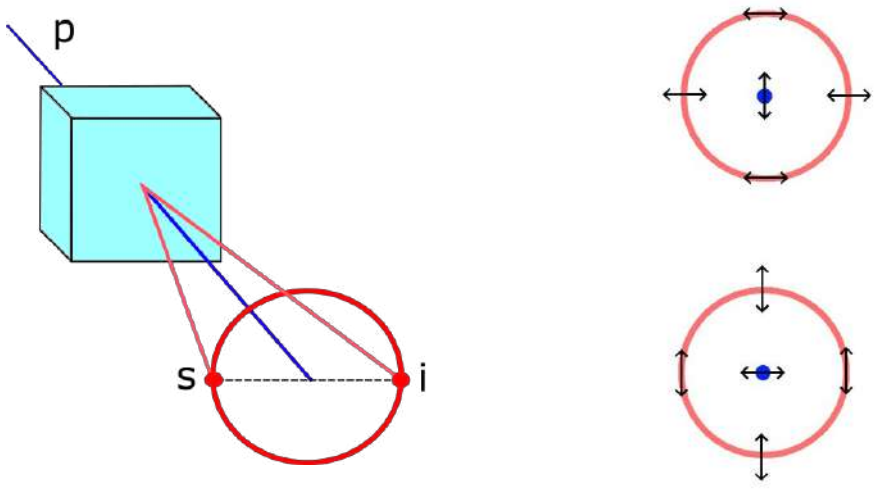
7.3 Схемы СПР

Рассмотрев типы синхронизма в нелинейных одноосных кристаллах, применим данные обозначения с ранее введенной нотацией пучков излучения (p – накачка, s – сигнальный луч, i – холостой луч) к процессу СПР.

Таким образом, можно определить два типа синхронизма (далее предполагаем, что кристалл является отрицательным – показатель преломления обыкновенной волны больше необыкновенной). При первом типе синхронизма излучение накачки падает на кристалл с необыкновенной поляризацией (параллельной главной плоскости кристалла), в результате чего происходит генерация сигнального и холостого пучка с обыкновенной поляризацией

$$\overrightarrow{k}_p^e = \overrightarrow{k}_s^o + \overrightarrow{k}_i^o \tag{97}$$

При визуальном рассмотрении данный эффект проявляется в виде одного расходящегося конуса, выходящего из кристалла совместно с излучением накачки. Если взять сечение выходной волны, то получится более привычное кольцо, как показано на рисунке (52а). Угол расходимости полученного кольца будет зависеть от угла падения излучения накачки относительно перпендикуляра к плоскости кристалла или, что более точно, волнового вектора накачки к оптической оси кристалла. При этом поляризация полученного конуса излучения во всех точках будет одинаковой и ортогональной к лучу накачки, что изображено на рисунке (52б).



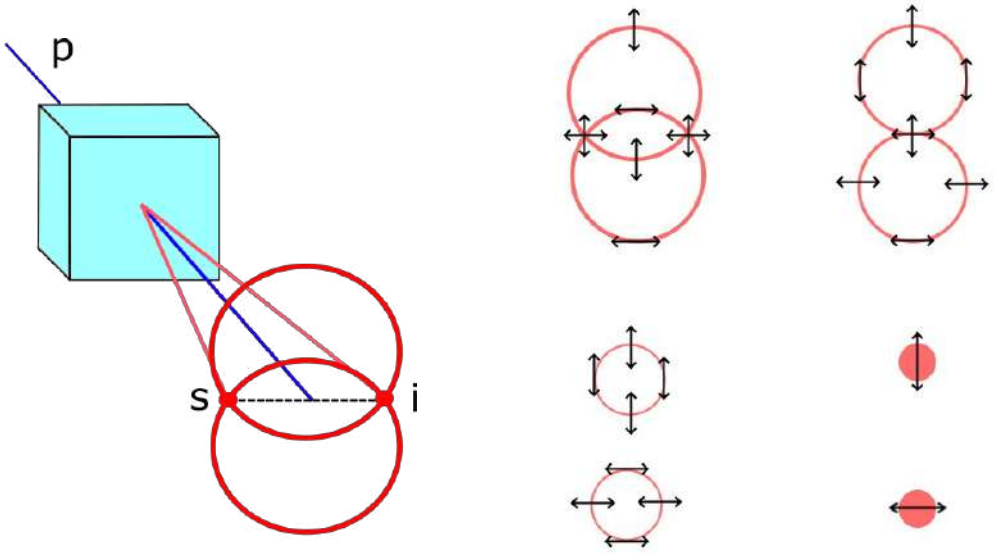
а) б)

Рис. 52: Процесс СПР при первом типе синхронизма (а), поляризация выходного излучения при первом типе синхронизма (б)

В свою очередь, при втором типе синхронизма излучение накачки все так же падает на кристалл с необыкновенной поляризацией, однако теперь сигнальный и холостой лучи имеют противоположную поляризацию:

$$\overrightarrow{k}_p^e = \overrightarrow{k}_s^o + \overrightarrow{k}_i^e \text{или } \overrightarrow{k}_p^e = \overrightarrow{k}_s^e + \overrightarrow{k}_i^o \tag{98}$$

Визуально это проявляется в виде двух расходящихся конусов: один соответствует сигнальному излучению с обыкновенной поляризацией, второй – холостому с необыкновенной, что показано на рисунке (53а). При этом угол их расхождения все так же зависит от угла между волновым вектором накачки и оптической осью кристалла, и при определенном диапазоне значений в определённой точке пространства происходит их пересечение, что соответствует паре запутанных по поляризации фотонов. В данном случае поляризация излучения в пределе каждого конуса в заданный момент времени остается постоянной, однако между собой они являются ортогональными, как показано на рисунке (53б).



а) б)

Рис. 53: Процесс СПР при втором типе синхронизма (а), поляризация выходного излучения при втором типе синхронизма (б)

Одним из важнейших применений процесса СПР является генерация запутанных фотонов, в частности состояний Белла:

$$|\Phi\rangle_{\pm} = \frac{1}{\sqrt{2}}(|HH\rangle \pm |VV\rangle) \tag{99}$$

$$|\Psi\rangle_{\pm} = \frac{1}{\sqrt{2}}(|HV\rangle \pm |VH\rangle) \tag{100}$$

Данные квантовые состояния являются чрезвычайно важными объектами в квантовой физике и применяются в теоретических исследованиях и в практических приложениях. Например, данные состояния используются для квантовой телепортации [58], протоколах квантового распределения ключа [59, 60], исследовании концепции локального реализма [61].

Схема генерации состояний Белла на процессе СПР первого типа [62] представлена на рисунке (54). В качестве среды для генерации используют два совмещенных кристалла, один из которых повернут относительного другого на 90°. В качестве луча накачки используют излучение с диагональной поляризацией. Таким образом, входное состояние можно представить следующим образом:

$$|D\rangle_{\pm} = \frac{1}{\sqrt{2}}|H\rangle + \frac{1}{\sqrt{2}}|V\rangle \tag{101}$$

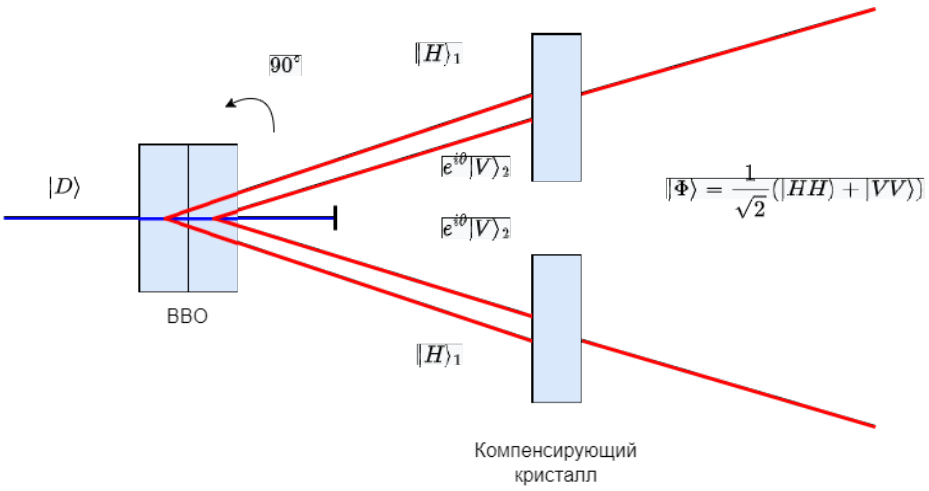


Рис. 54: Принципиальная схема генерации состояния Белла на СПР первого типа

В результате горизонтальная составляющая входного пучка $|H\rangle$ будет генерировать вертикальные выходные состояния $|VV\rangle$ на первом кристалле, а вертикальная составляющая входного пучка $|V\rangle$ будет генерировать горизонтальные выходные состояния $|HH\rangle$ на втором кристалле.

Важно обратить внимание, что одновременная генерация двух выходных состояний невозможна от одного входного. При этом выбор выходного состояния происходит случайным образом. В заключение, выходное состояние после двух кристаллов можно определить как

$$|\Phi(\theta)\rangle = \frac{1}{\sqrt{2}}(|HH\rangle_1 + e^{i\theta}|VV\rangle_2) \tag{102}$$

Тем не менее представленная схема содержит в себе несколько критических недостатков, которые приводят к тому, что вертикальные и горизонтальные выходные состояния становятся различимы между собой, что снижает запутанность таких состояний и разрушает состояние Белла. Первая причина кроется в фазовой задержке вертикальных состояний от горизонтальных вследствие разного времени рождения фотонов. Так как первый кристалл находится впереди второго, рождённые на нем фотоны, проходя через второй кристалл, претерпевают отличный фазовый набег от фотонов, рожденных на втором кристалле, ввиду различных состояний поляризации и анизотропии кристалла. Вторая причина заключается в различии выходных траекторий вертикального и горизонтального состояний вследствие разных пространственных точек рождения фотонов и анизотропии кристаллов. Данные различия двух выходных состояний можно преодолеть, расположив два дополнительных нелинейных кристалла после системы генерации запутанных фотонов на траекториях сигнального и холостого излучения, что скомпенсирует расхождение как в траекториях, так и в фазе. В результате данная схема позволит сгенерировать следующую пару состояний Белла:

$$|\Phi\rangle = \frac{1}{\sqrt{2}}(|HH\rangle + |VV\rangle) \tag{103}$$

Как уже было упомянуто ранее, в результате процесса СПР второго типа при выполнении определенных условий происходит генерация сигнального и холостого конусов излучения, на месте пересечения которых происходит формирование двух запутанных фотонов. Тем не менее, вследствие анизотропии кристалла вертикальное и горизонтальное состояние на выходе будут иметь фазовый сдвиг, что делает данные состояния различимыми и разрушает запутанность:

$$|\Psi(\theta)\rangle = \frac{1}{\sqrt{2}}(|H\rangle \otimes e^{i\theta_2}|V\rangle + e^{i\theta_1}|V\rangle \otimes |H\rangle) \tag{104}$$

Как и в случае СПР первого типа, данный эффект можно скомпенсировать, поставив после кристалла СПР второй компенсирующий

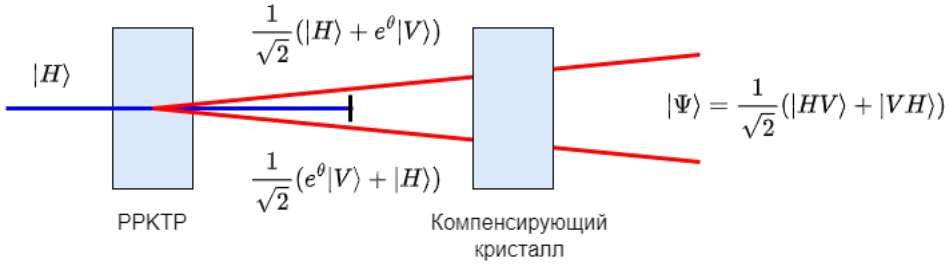


Рис. 55: Принципиальная схема генерации состояния Белла на СПР второго типа

кристалл, который позволит ликвидировать фазовый сдвиг между двумя состояниями поляризации [63]. Оптическая схема данного процесса представлена на рисунке (55). В результате выходное состояние такой системы можно представить как

$$|\Psi\rangle = \frac{1}{\sqrt{2}}(|HV\rangle + |VH\rangle) \tag{105}$$

На сегодняшний день один из самых популярных способов генерации запутанных фотонов является процесс СПР второго типа в схеме поляризационного интерферометра Саньяка [64], представленного на рисунке (56). В представленной схеме линейно поляризованное излучение проходит через одномодовое волокно, которое обеспечивает модовую фильтрацию, и далее выводится в открытое пространство, после чего проходит через систему полуволновой и четвертьволновой пластины, которые задают определенное состояние поляризации и фазовой задержки, и далее отражается от дихроичного зеркала, которое служит для разделения сигнального/холостого луча от излучения накачки на выходе интерферометра. Таким образом, входное состояние на входе интерферометра можно представить как

$$\overrightarrow{E}_p = E_H \hat{e}_H + e^{i\phi_p} E_V \hat{e}_V, \tag{106}$$

где $\hat{e}_H$ и $\hat{e}_V$ – единичные векторы состояния поляризации, а ϕ_p – разность фаз между вертикальной и горизонтальный поляризациями. Далее полученное состояние направляется на поляризационный светоделитель, где вертикальная и горизонтальная составляющие разделятся на два пути, каждый из которых мы рассмотрим отдельно.

Горизонтальная составляющая входного состояния проходит интерферометр по пути A, как показано на рисунке (57a). Отражаясь от зеркала, излучение накачки падает на нелинейный кристалл, генерируя в

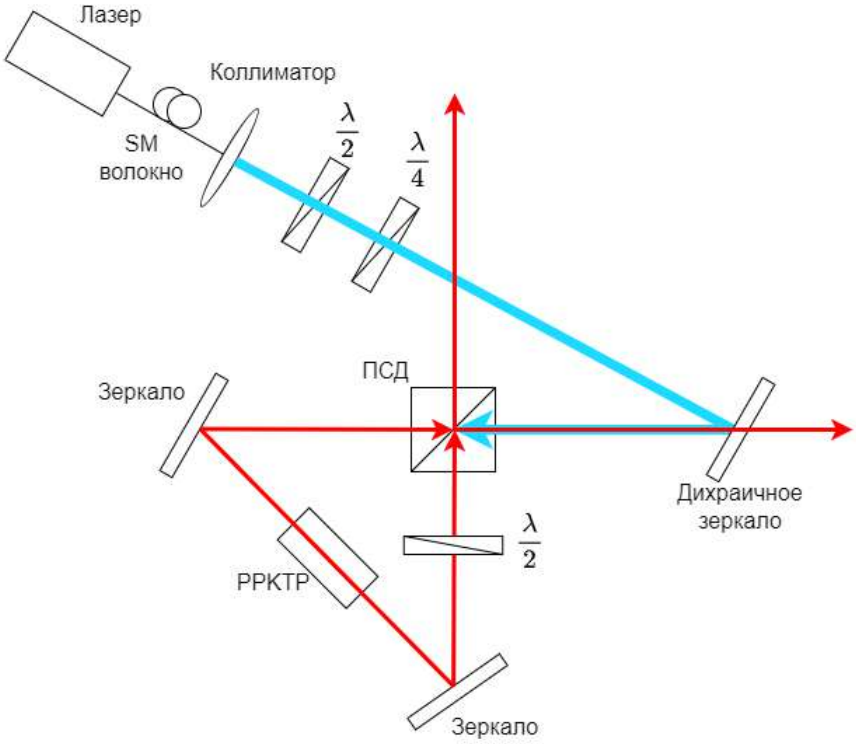


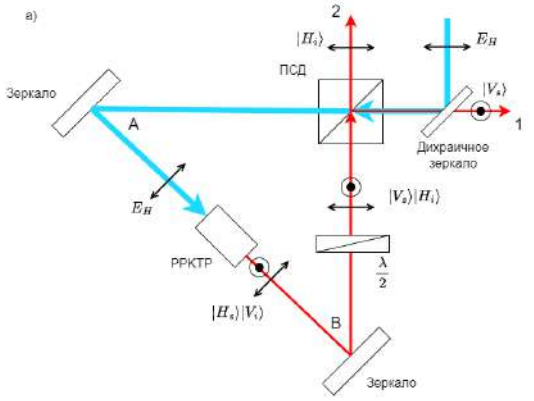
Рис. 56: Оптическая схема генерации запутанных фотонов на основе процесса СПР в поляризационном интерферометре Саньяка

результате пару запутанных фотонов с ортогональными поляризациями, после чего общее состояние на выходе кристалла, отражаясь через зеркало, проходит через вторую полуволновую пластину и затем направляется на поляризационный светоделитель. Таким образом, выходное состояние интерферометра для горизонтального входного состояния можно представить как

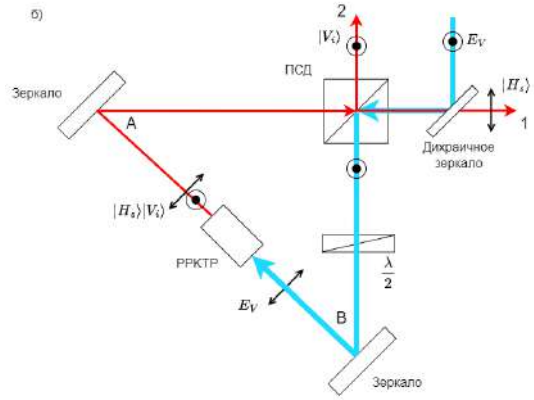
$$|\Psi_H\rangle = e^{i[k_p L_A + (k_s+k_i)L_B + \theta_s + \theta_i]} \eta_H E_H |V_s\rangle_1 |H_i\rangle_2, \tag{107}$$

где 1 и 2 – выходы на поляризационном светоделителе, θ_s и θ_i – фазовая задержка сигнального и холостого фотонов на полуволновой пластине, η_H – эффективность генерации.

В свою очередь, вертикальная составляющая входного состояния проходит интерферометр по пути B, что изображено на рисунке (57б). Отражаясь от зеркала, излучение накачки проходит через полуволновую пластину, таким образом меняя поляризацию на горизонтальную. Далее, попадая на кристалл, накачка разделяется на сигнальный и холостой



а)



б)

Рис. 57: Ход лучей горизонтальной (а) и вертикальной (б) составляющей излучения накачки в процессе СПР в поляризационном интерферометре Саньяка

фотоны, которые направляются на поляризационный светоделитель. В результате выходное состояние для вертикальной поляризации накачки можно представить в виде

$$|\Psi_H\rangle = e^{i[\phi_p + k_p L_B + \theta_p + (k_s + k_i) L_A]} \eta_H E_V |H_s\rangle_1 |V_i\rangle_2, \tag{108}$$

где θ_p – фазовая задержка излучения накачки на полуволновой пластине. Таким образом, общее состояние на выходе интерферометра можно представить как

$$|\Psi\rangle \propto (|H_s\rangle_1 |V_i\rangle_2 + e^{i\phi} \beta |V_s\rangle_1 |H_i\rangle_2), \tag{109}$$

где $\phi = \theta_s + \theta_i - \theta_p - \phi_p$ и $\beta = \frac{\eta_H E_H}{\eta_V E_V}$. Таким образом, контролируя соотношение между вертикальной и горизонтальной составляющими поляризации и фазовой задержкой излучения накачки, с помощью полуволновой и четвертьволновой пластины можно контролировать получаемые запутанные состояния, в том числе генерировать состояния Белла. Данная схема является наиболее простой, компактной и стабильной из рассмотренных в данном разделе и в настоящее время используется в большинстве теоретических и экспериментальных работ.

7.4 Применение спонтанного параметрического рассеяния

Существуют различные применения СПР-излучения, которые основываются на использовании свойств фотонных пар. Основным способом использования данных свойств являются корреляционные измерения. В основе таких измерений лежит факт одновременности рождения пар фотонов. При проведении измерений это выражается в одновременном срабатывании детекторов одиночных фотонов, которые регистрируют фотонные пары, в пределах заданного временного окна. К таким реализациям можно отнести бифотонную спектроскопию [65], квантовые фантомные изображения [66, 67] и некоторые реализации протоколов квантовой криптографии [68, 69].

Другой особенностью излучения, генерируемого в процессе спонтанного параметрического рассеяния, является возможность реализации различных неклассических состояний света. Так, при помощи источников на основе СПР возможно реализовать генерацию одиночных фотонов [70]. Одиночные фотоны, в свою очередь, могут использоваться в системах квантового распределения ключа для увеличения защищённости подобных систем. Однако стоит отметить, что подобные источники не получили широкого распространения ввиду несоответствия некоторых их свойств требованиям к параметрам идеальных источников одиночных фотонов. Одно из таких свойств кроется в названии процесса СПР: поскольку процесс спонтанен, невозможно генерировать одиночные фотоны по требованию, что накладывает ограничения на их использование в реальных системах. Тем не менее, потенциально интересным примером применения источника одиночных фотонов на основе СПР-излучения является генерация случайных чисел. Существует несколько подходов с использованием запутанных фотонов, которые позволяют генерировать случайные числа. При одном используется ранее описанный источник одиночных фотонов [70]. Другой способ подразумевает использование

запутанных фотонов при их прохождении через светоделители с последующей регистрацией детекторами фотонов в схеме счёта одновременных срабатываний [71].

СПР-излучение также является источником сжатых состояний, что находит своё применение в метрологии, когда возникает необходимость проведения более точных измерений. Примером использования таких состояний может послужить квантовый гироскоп. Существует два основных способа увеличения точности измерений в волоконно-оптических гироскопах: увеличение площади интерферометра или уменьшение длины волны. Альтернативным же способом является использование так называемых NOON-состояний, которые позволяют обойти ограничения, связанные с длиной волны за счёт своих свойств [72].

Другим примером использования свойств СПР-излучения можно назвать реализацию логических операций за счёт использования эффекта группировки и антигруппировки фотонов, которая была продемонстрирована в эксперименте с интерферометром Хонга-Оу-Менделя [73]. Подобные операции могут послужить основой для реализации квантового компьютера [74]. Однако в данном случае стоит отметить, что, хотя существует возможность реализации отдельных операций с увеличением числа подобных операций, падает эффективность реализации всей схемы, что негативно сказывается на потенциальной масштабируемости.

Запутанные фотоны могут быть использованы для реализации протоколов квантовых коммуникаций. Среди таких протоколов можно выделить [68, 69]. Для протокола E92, после распределения случайной битовой последовательности происходит оценка S-параметра, который позволяет определить, вмешивался ли нарушитель в процесс распределения ключа.

7.5 Контрольные вопросы

1. Какими уравнениями описывается параметрическая генерация?
2. Уравнение баланса частот.
3. Уравнение, описывающее условие фазового синхронизма.
4. Что такое фазовая расстройка?
5. Какая волна называется обыкновенной?
6. Какая волна называется необыкновенной?
7. Какой анизотропный кристалл называется положительным?
8. Какой анизотропный кристалл называется отрицательным?
9. Каким выражением описывается зависимость показателя преломления необыкновенной волны от направления распространения внутри кристалла?
10. Какие виды фазового синхронизма бывают?
11. Как выглядят индикатрисы показателей преломления положительного и отрицательного кристаллов?
12. Приведите и поясните принцип работы схемы генерации состояний Белла на процессе спонтанного параметрического рассеяния первого типа.
13. Недостатки схемы генерации состояний Белла на процессе спонтанного параметрического рассеяния первого типа.
14. Приведите и поясните принцип работы схемы генерации состояний Белла на процессе спонтанного параметрического рассеяния второго типа.
15. Принцип работы оптической схемы генерации запутанных фотонов на основе процесса спонтанного параметрического рассеяния второго типа в поляризационном интерферометре Саньяка.
16. Приведите примеры применения спонтанного параметрического рассеяния СПР-излучения.

8 Фантомная визуализация

8.1 Введение

От первобытного общества до современной цивилизации человек стремился запечатлеть и неким образом зафиксировать окружающую его действительность. Начиная от наскальных рисунков первобытного человека и настенных изображений древних цивилизаций, продолжая изобразительными полотнами средневековья и эпохи Возрождения и заканчивая современными фотографическими средствами, смысл и функция изображения постоянно расширялись. В настоящее время изображение может служить напоминанием об ушедшем прошлом и приятных воспоминаниях, предметом искусства, способом идентификации и борьбы с преступниками и нарушителями закона, методом передачи информации и множеством других функций.

Последним крупным достижением в области получения изображения стало изобретение фотографического аппарата (далее под этим термином понимается большой класс современных регистрирующих устройств, при помощи которых возможно получать изображения, а не только привычные нам фотоаппараты). Если опустить все технические особенности и детали, то принцип действия данного устройства можно описать следующим образом. Свет от источника излучения (Солнца или лампы) попадает на объект, часть излучения от которого отражается и через систему линз попадает на регистрирующую среду (светочувствительную пленку или ПЗС-матрицу). Таким образом, происходит формирования изображения объекта.

За последние полтора столетия фотографические аппараты прошли большой путь развития и на сегодняшний день удовлетворяют практически всем современным требованиям. Тем не менее, с развитием научной мысли, и квантовой механики в частности, учеными был предложен новый способ регистрации изображений, который получил название «Фантомные изображения» (ФИ), который основан на пространственных корреляциях двух пучков оптического излучения. Данный метод не подразумевает замену современным фотографическим аппаратам, а скорее позволяет преодолеть физические ограничения и расширить функциональные возможности последних.

Цель данной главы – дать читателю понимание об общих принципах технологии ФИ и современном ее состоянии. Данная глава содержит в себе общие принципы формирования ФИ, необходимый минимум математического аппарата и современные модификации и применения. При необходимости более детального понимания изложенного здесь матери-

ала мы просим читателей обратиться к списку литературы.

8.2 Общие принципы

Впервые метод ФИ был представлен в работах российских и американских ученых [75, 76] в конце прошлого столетия. Обобщенная оптическая схема их эксперимента представлена на рисунке 58.

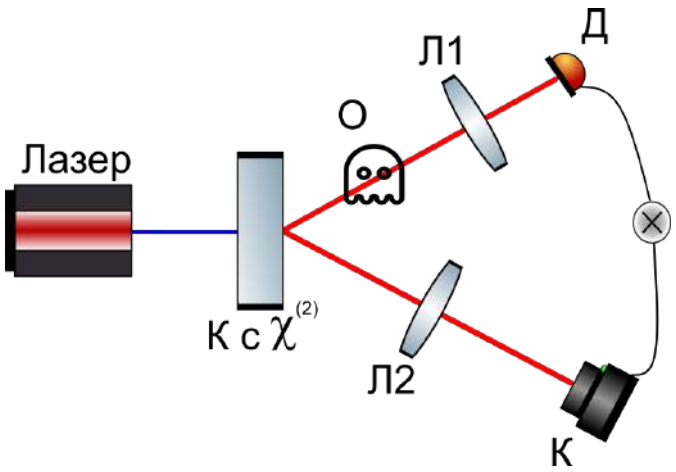


Рис. 58: Принципиальная схема квантовых ФИ, где К – кристалл с квадратичной нелинейностью, О – объект, Л – линза, Д – однопиксельный (собирающий) детектор, К – многопиксельная камера

Лазерное излучение накачки направляется на кристалл с квадратичной нелинейностью, где в результате реализации процесса спонтанного параметрического рассеяния (СПР) рождается пара запутанных фотонов. Первый фотон данной пары направляется в так называемое «зондирующее плечо», где взаимодействует с изучаемым объектом (проходит или отражается/поглощается) и далее регистрируется однопиксельным детектором с помощью фокусирующей линзы или большим собирающим детектором, который фиксирует общую интенсивность. В общем случае считается, что объект представляет собой двумерный трафарет или маску, через которую фотон либо проходит, либо отражается/поглощается. В то же время второй фотон изначальной пары направляется в «воспроизводящее плечо», где, никак не провзаимодействовав с изучаемым объектом, регистрируется многопиксельной камерой или движущимся (сканирующим) однопиксельным детектором, который должен быть пространственно согласован со вторым фотоном (второй случай на рисунке не отображен). Системы регистрации в воспроизводящем плече отличаются лишь тем, что в случае однопиксельного сканирующего детектора

необходимо дополнительно фиксировать его положение в пространстве, тогда как многопиксельная камера позволяет сразу получать координаты прилетевшего фотона по сработанному элементу матрицы. Далее, проведя несколько итераций данного процесса, последовательно меняя угол разлета фотонов так, чтобы в итоге весь объект был освещен, мы получаем ряд (одномерную матрицу) интенсивностей однопиксельного детектора или набор многомерных матриц многопиксельной камеры (в случае сканирующего однопиксельного детектора будет одномерная матрица, где каждому элементу соответствует координата детектора в данный момент времени в пространстве). По отдельности полученные данные не позволяют нам получить изображение изучаемого объекта; однако, воспользовавшись тем, что пара запутанных фотонов обладает идеальной пространственной и временной корреляцией, мы можем восстановить изображение объекта, используя временное совпадение прилетов пары фотонов.

Рассмотрим подробнее процесс формирования изображения. Представленная оптическая схема собрана таким образом, что фотон в «воспроизводящем плече» всегда регистрируется детектором (напомним, что в случае сканирующего однопиксельного детектора он всегда должен быть пространственно сориентирован так, чтобы на него пришел фотон). В этом случае, при условии идеальной корреляции пары запутанных фотонов, наличие совпадения между детектором в первом плече и камерой во втором плече может произойти только тогда, когда фотон в «зондирующем плече» прошел через объект. Таким образом, восстановление изображения изучаемого объекта происходит попиксельно: есть совпадение – «ставим» 1 в соответствующей точке пространства, нет совпадения – «ставим» 0. Данные условия считаются идеальными, что выражается в отсутствии холостых срабатываний детектора и его 100 эффективности. В действительности для каждого положения разлета фотонов необходимо проводить несколько итераций для получения точного результата.

После своего открытия технология ФИ считалась исключительно квантовым явлением, однако через несколько лет было продемонстрировано, что данный эффект можно получить и в классическом приближении [77]. На сегодняшний день ФИ разделяют на квантовые и псевдотепловые (классические). Далее подробно рассмотрим последний случай, обобщенная оптическая схема которого представлена на 59. Пучок лазерного излучения направляется на рассеивающую среду (например, матовое зеркало), в результате чего образуется случайная спекл-структура, характерный вид которой представлен на 60. Далее процесс формирования фантомного изображения в каком-то виде совпадает с квантовым случаем. С помощью светоделителя полученная спекл-структура разде-

ляется на две части, первая из которых направляется в «зондирующее плечо», где в результате взаимодействия с объектом часть спеклов отражается/поглощается, а оставшаяся часть регистрируется с помощью линзы (не представлена на рисунке) собирающим детектором, который фиксирует суммарную интенсивность прошедших через объект спеклов.

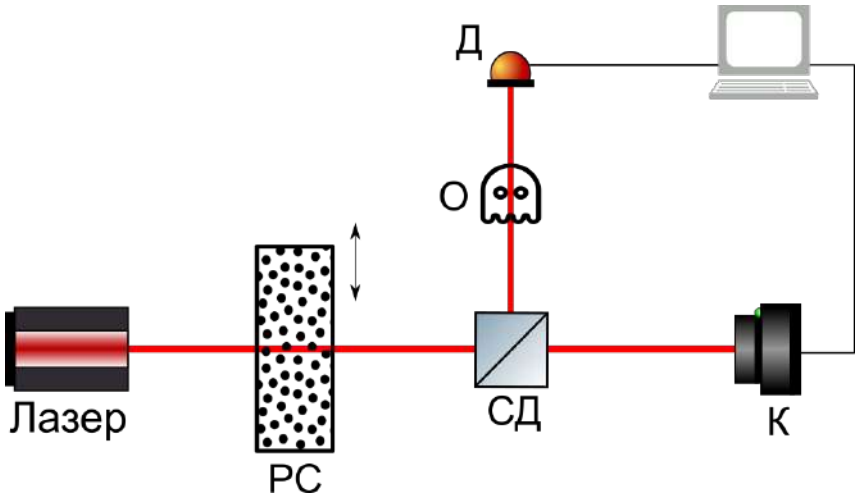


Рис. 59: Принципиальная схема псевдотепловых ФИ, где РС – рассеивающая среда, СД – светоделитель, О – объект, Д – однопиксельный (собирающий) детектор, К – многопиксельная камера

В свою очередь, вторая часть изначальной спекл-структуры направляется в «воспроизводящее плечо», где фиксируется многопиксельной камерой. Как и в квантовом случае, проведя некоторое количество итераций, в каждой из которых обязательно должно происходить изменение спекл-структуры (например, в результате освещения разных участков матового зеркала), мы обладаем рядом суммарных интенсивностей прошедших через объект спеклов для каждой итерации и набором матриц, отражающих пространственное распределение полученных спекл-структур для каждого случая. Аналогично, по отдельности полученные данные не позволяют нам восстановить изображение исследуемого объекта, однако, применив к ним в данном случае функцию корреляции интенсивностей, мы получаем изображение нашего объекта.

Общий вид функции корреляции интенсивностей представлен выражением

$$G(x, y) = \langle S \cdot I(x, y) \rangle - \langle S \rangle \cdot \langle I(x, y) \rangle, \tag{110}$$

где S – интенсивность собирающего детектора, $I(x, y)$ – пространственное

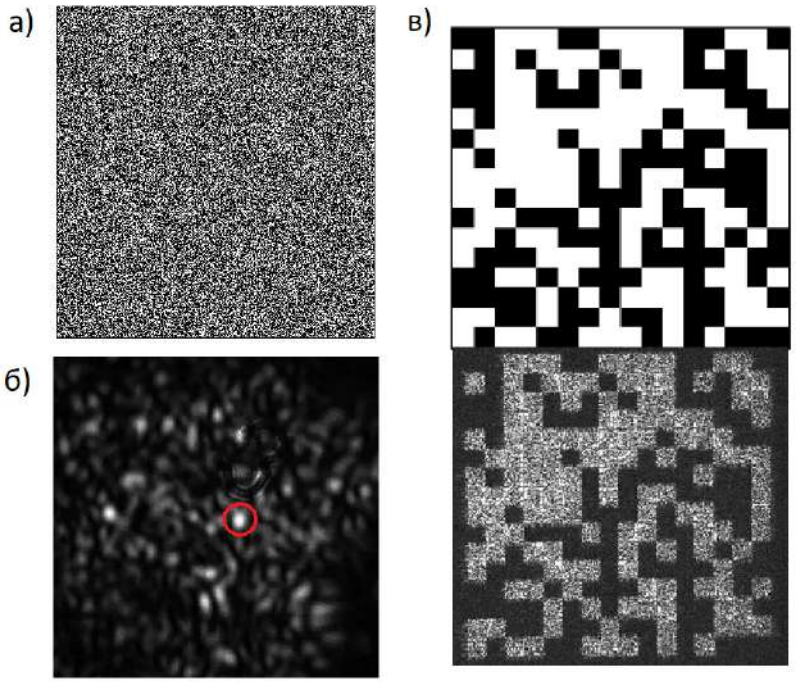


Рис. 60: Спекл-структура: а) сгенерированная на компьютере , б) полученная экспериментально с помощью матового стекла, где красным выделен один спекл, в) полученная экспериментально с помощью SLM (снизу)(см. раздел «Модификации фантомных изображений и практическое применение») по заданной модели (сверху)

распределение интенсивностей зарегистрированной спекл-структуры, $\langle\cdot\rangle = \frac{1}{N}\sum \mathrm{r}$ – усреднение по всем N реализациям. Исходя из формулы (110), основная идея псевдотепловых ФИ заключается в том, что чем больше спеклов пройдет через объект в данной итерации, тем больший «вес» будет у заданной спекл-структуры (в формуле (110) это слагаемое $\mathrm{S}\cdot\mathrm{I}(\mathrm{x},\mathrm{y})$). Таким образом, в процессе расчета корреляционной функции (можно сказать, что это грубый аналог усредненной спекл-структуры) те спеклы, которые как бы находились в области объекта и проходили через него чаще других, дадут больший вклад в финальное рассчитанное изображение. В итоге, на полученном изображении область объекта будет ярче по сравнению с остальной частью.

Пример фантомного изображения, полученного с помощью псевдотеплового метода, представлен на рисунке 61 (в квантовом случае изображение будет иметь схожий вид). Здесь важно уточнить, что для предотвращения искажения изображения объекта необходимо соблюдать опре-

делённое соотношение расстояний в плечах: равенство длин плеч в квантовом случае и равенство расстояний от светоделительной пластинки до объекта в «зондирующем плече» и от светоделительной пластинки до камеры во «воспроизводящем плече». Первое условие гарантирует совпадение двух фотонов для квантового случая, а второе идентичность и, как следствие, пространственную корреляцию зарегистрированной и падающей на объект спекл-структуры для псевдотеплового случая. При невыполнении данных условий в оптической схеме необходимо предусмотреть систему линз в обоих плечах [78, 79, 80]. Также стоит заметить, что в большинстве лабораторных установок по ФИ используется схема, построенная на пропускании, вследствие своего удобства; однако, при практическом использовании её также можно собрать схему, работающую на отражение [81, 82]. Помимо прочего, стоит обратить внимание, что в большинстве исследований полученное фантомное изображение имеет двумерную структуру и черно-белую палитру, однако ведутся исследования как по передаче цвета [83], так и объема [84].

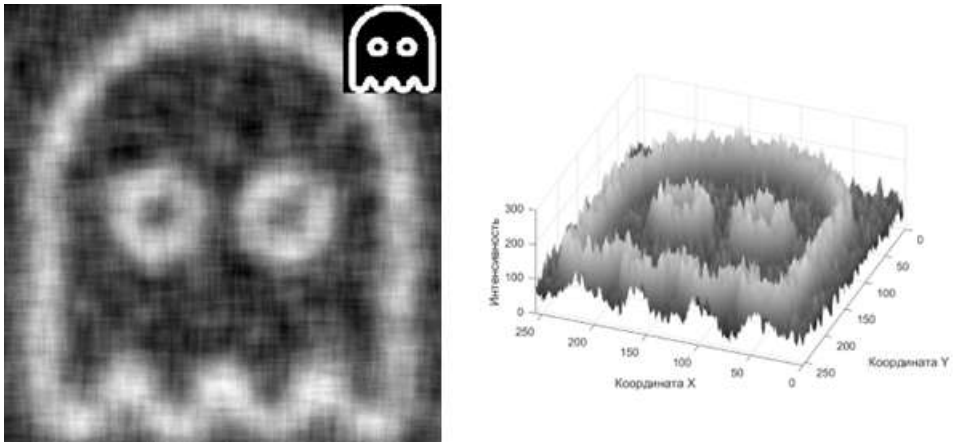


Рис. 61: Пример восстановленного фантомного изображения псевдотепловым методом

Подробнее остановимся на различии квантового и псевдотеплового ФИ. Одним из основных отличий, как уже было сказано при подробном рассмотрении оптических схем, является использование запутанных одиночных фотонов в квантовом методе и спекл-структур в псевдотепловом. Соответственно, само изображение восстанавливается с помощью счёта совпадений или корреляционной функции. Здесь стоит обратить внимание, что формально для квантового метода можно также применить корреляционную функцию, что будет показано в следующем разделе. На сегодняшний день большей популярностью пользуются схемы на псев-

дотепловых ФИ вследствие своей простоты, дешевой элементной базы и возможностью дополнительной настройки параметров (данное отличие будет раскрыто в последующих разделах). В свою очередь, квантовые ФИ более устойчивы к шумам и имеют более высокие характеристики соотношения сигнал шум; однако, вследствие большой сложности и дорогой компонентной базы, не так сильно распространены.

Основными параметрами при восстановлении фантомного изображения являются соотношение сигнал-шум и контрастность, представленные следующими выражениями соответственно:

$$\mathrm{SNR} = 10 \cdot \log_{10}\left(\frac{\langle \mathrm{I_o} \rangle}{\langle \mathrm{I_b} \rangle}\right), \tag{111}$$

$$\mathrm{C} = \frac{\langle \mathrm{I_o} \rangle - \langle \mathrm{I_b} \rangle}{\langle \mathrm{I_o} \rangle}, \tag{112}$$

где $\langle \mathrm{I_o} \rangle$, $\langle \mathrm{I_b} \rangle$ – среднее значение интенсивностей объекта и фона, соответственно. Стоит заметить, что расчет данных характеристик возможен только при заранее известном изображении объекта и подходит скорее для научных исследований. При практическом использовании технологии ФИ можно воспользоваться гистограммой полученного изображения, которая будет иметь два гауссовых распределения: сигнала и шума – по их пикам и производится расчет указанных параметров.

При использовании псевдотеплового метода также важно обратить внимание на количество итераций и размер генерируемых спекл структур. Интуитивно понятно, что при увеличении числа итераций качество изображения будет улучшаться, так как «вес» проходящих через объект спекл будет становиться больше. Данная зависимость продемонстрирована на рисунке 62.

С размером спеклов все несколько сложнее. Также понятно, что чем больше размер отдельно взятого спекла, тем быстрее будет восстанавливаться изображение, так как эти спеклы будут покрывать большую часть объекта; однако, если их размер будет превосходить минимально различимый элемент объекта (например, если в качестве объекта выступает щель, то ее минимально различимый элемент – это ширина этой самой щели), то восстановленное изображение будет деформировано или вовсе не будет восстановлено.

Данные соотношения отражены на рисунке 63. Исходя из них, можно сделать вывод, что наилучшее восстановление происходит в случае, когда размеры щели и минимально различимого элемента совпадают (представленное отношение в настоящем пособии названо размерным соотношением).

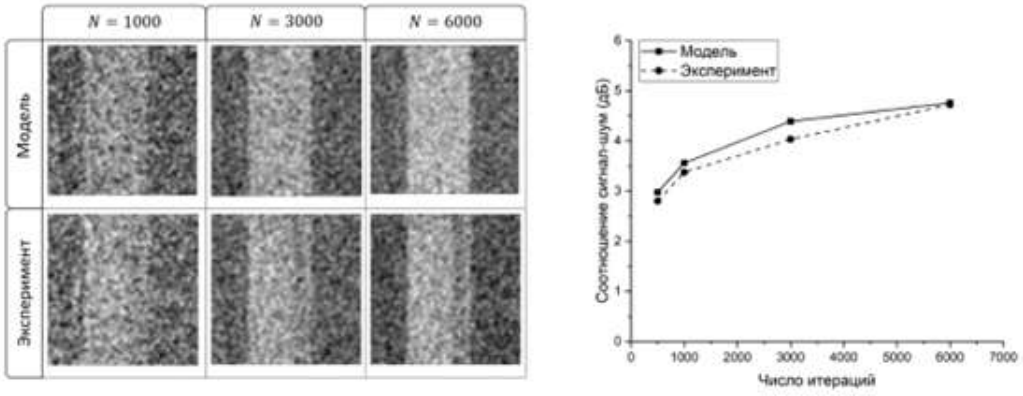


Рис. 62: Восстановленные изображения щели для численного моделирования и экспериментальной установки при различном числе итераций (слева) и зависимость соотношения сигнал-шум от числа итераций для щели (справа)

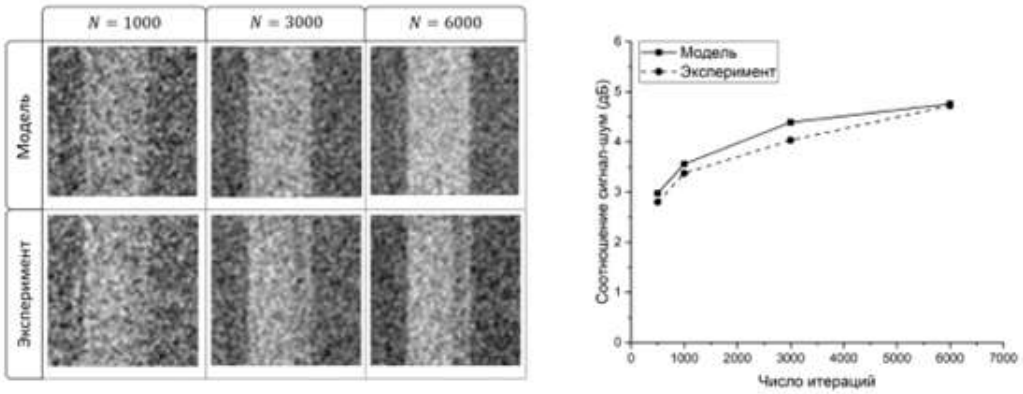


Рис. 63: Восстановленные изображения щели для численного моделирования и экспериментальной установки при 3000 итераций при различных размерных соотношениях (слева) и зависимость соотношения сигнал-шум от размерного соотношения для щели (справа)

8.3 Математическое описание

Данный раздел будет посвящен математическому описанию процесса получения фантомных изображений. Будет рассмотрен общий вывод как для квантового, так и для псевдотеплового случая. Все математические выкладки данной главы основаны на учебном пособии [85]. Математическое описание и общие положения технологии ФИ также представлены

в работах [86, 87]. Начнем наше рассмотрение с квантового случая и для начала определим соотношение "вход-выход" через преобразование Н.Н. Боголюбова для спонтанного параметрического рассеяния на кристалле по формуле

$$\hat{a}_{i,out}(\boldsymbol{q}) = U_i(\boldsymbol{q})\hat{a}_{i,in}(\boldsymbol{q}) + U_i(\boldsymbol{q})\hat{a}^{\dagger}_{j,in}(-\boldsymbol{q}) \qquad i \neq j = 1, 2, ..., \tag{113}$$

где i и j – моды излучения; U и V – коэффициенты, удовлетворяющие следующим условиям: $|U(\boldsymbol{q})|^2 + |V(\boldsymbol{q})|^2 = 1$ и $U_1(\boldsymbol{q})V_2(-\boldsymbol{q} = U_2(-\boldsymbol{q})V_1(\boldsymbol{q})$; $\boldsymbol{q}$ – компоненты волнового вектора.

Тогда поля в плоскости детектирования записываются в виде выражения

$$\hat{c}_i(x_i) = \int dx'_i h_i(x_i, x'_i)\hat{a}_{i,out}(x_i) + \hat{L}_i(x_i), \qquad i = 1, 2, ..., \tag{114}$$

где $\hat{L_1}, \hat{L_2}$ отвечают за возможные потери при распространении полей, а $h_1(x_1, x'_1), h_2(x_2, x'_2)$ – функции импульсного отклика оптических путей.

Оператор плотности потока фотонов для i-ой волны определяется выражением

$$\hat{I}_i(z, x, t) = \hat{a}^{\dagger}_i(z, x, t)\hat{a}_i(z, x, t). \tag{115}$$

Информация об объекте извлекается из анализа пространственной корреляционной функции интенсивностей, измеряемых детекторами в зависимости от положения x_2 пикселя второго детектора,

$$\langle\hat{I}_1(x_1)\hat{I}_2(x_2)\rangle = \langle\hat{c}^{\dagger}_1(x_1)\hat{c}_1(x_1)\hat{c}^{\dagger}_2(x_2)\hat{c}_2(x_2)\rangle. \tag{116}$$

В этом случае полная информация об объекте содержится в корреляционной функции флуктуаций интенсивности

$$G(x_1, x_2) = \langle\hat{I}_1(x_1)\hat{I}_2(x_2)\rangle - \langle\hat{I}_1(x_1)\rangle\langle\hat{I}_2(x_2)\rangle, \tag{117}$$

где $\langle\hat{I}_i(x_i) = \langle\hat{c}^{\dagger}_i(x_i)\hat{c}_i(x_i)$– средняя интенсивность i-го пучка. На основе изложенных выше выкладок выражение (117) можно привести к следующему виду:

$$\begin{aligned} G(x_1, x_2) = \int dx'_1 \int dx''_1 \int dx'_2 \int dx''_2 h^*_1(x_1, x''_1)h_1(x_1, x'_1)\times \\ \times h^*_2(x_2, x''_2)h_2(x_2, x'_2)[\langle\hat{a}^{\dagger}_{1,out}(x''_1)\hat{a}_{1,out}(x'_1)\hat{a}^{\dagger}_{2,out}(x''_2)\hat{a}_{2,out}(x'_2)\rangle - \\ -\langle\hat{a}^{\dagger}_{1,out}(x''_1)\hat{a}_{1,out}(x'_1)\rangle\langle\hat{a}^{\dagger}_{2,out}(x''_2)\hat{a}_{2,out}(x'_2)\rangle \end{aligned} \tag{118}$$

Применив факторизацию к первому члену квадратной скобки

$$\begin{aligned}\langle \hat{a}^{\dagger}_{1,\mathrm{out}}(x''_1)\hat{a}_{1,\mathrm{out}}(x'_1)\hat{a}^{\dagger}_{2,\mathrm{out}}(x''_2)\hat{a}_{2,\mathrm{out}}(x'_2)\rangle = \\ = \langle \hat{a}^{\dagger}_{1,\mathrm{out}}(x''_1)\hat{a}_{1,\mathrm{out}}(x'_1)\rangle\langle \hat{a}^{\dagger}_{2,\mathrm{out}}(x''_2)\hat{a}_{2,\mathrm{out}}(x'_2)\rangle + \\ + \langle \hat{a}^{\dagger}_{1,out}(x''_1)\hat{a}^{\dagger}_{2,out}(x''_2)\rangle\langle \hat{a}_{1,out}(x'_1)\hat{a}_{2,out}(x'_2)\rangle \end{aligned} \quad (119)$$

получим корреляционную функцию флуктуаций интенсивности для параметрического рассеяния в следующем виде:

$$G_{PDG}(x_1, x_2) = |\int dx'_1 \int dx'_2 h_1(x_1, x'_1)h_2(x_2, x'_2)\langle \hat{a}_{1,out}(x'_1)\hat{a}_{2,out}(x'_2)\rangle|^2 \quad (120)$$

Принимая во внимание, что $\hat{a_{2,\mathrm{out}}}$ находятся в вакуумном состоянии, получим

$$\langle \hat{a}_{1,\mathrm{out}}(x'_1)\hat{a}_{2,\mathrm{out}}(x'_2)\rangle = \int \frac{dq}{(2\pi)^2} e^{iq\cdot(x'_1 - x'_2)} U_1(\boldsymbol{q})V_2(-\boldsymbol{q}) \quad (121)$$

Для псевдотеплового случая соотношение "вход-выход" на светоделителе можно записать следующим образом:

$$\hat{b}_1(x) = r\hat{a}(x) + t\hat{\nu}(x); \quad (122)$$

$$\hat{b}_2(x) = t\hat{a}(x) - r\hat{\nu}(x), \quad (123)$$

где t и r – комплексные коэффициенты пропускания и отражения зеркала; $\hat{a}$ – тепловое поле; $\hat{\nu}$ – вакуумное поле. Если мы считаем, что тепловое состояние $\hat{a}(x)$ характеризуется гауссовой статистикой поля, при которой любая корреляционная функция произвольного порядка выражается через корреляционную функцию второго порядка

$$\Gamma(x, x') = \langle \hat{a}^{\dagger}(x)\hat{a}(x')\rangle = \int \frac{dq}{(2\pi)^2} e^{iq\cdot(x-x')}\langle n(q)\rangle_{\mathrm{th}} \quad (124)$$

где $\langle n(q)\rangle_{\mathrm{th}}$- среднее число фотонов в моде q теплового состояния. В результате по аналогии с квантовым случаем для функции флуктуаций интенсивности для теплового излучения получим

$$G_{\mathrm{th}}(x_1, x_2) = |tr|^2| \int dx'_1 \int dx'_2 h^*_1(x_1, x'_1)h_2(x_2, x'_2)\langle \hat{a}^{\dagger}(x'_1)\hat{a}(x'_2)\rangle|^2 \quad (125)$$

Таким образом, в данном разделе был получен общий вид функции флуктуации интенсивностей для квантового G_{PDG} и псевдотеплового случаев G_{th}. Дальнейший вид полученных выражений зависит от конкретной оптической схемы и определяется как функциями импульсного отклика, так и выходными полями.

8.4 Модификации фантомных изображений и практическое применение

С момента своего появления ФИ получили множество модификаций. Так, одной из самых значимых стали вычислительные ФИ [88], обобщённая оптическая схема которых представлена на 64. Как и псевдотепловые ФИ, данная модификация основана на генерации случайной спекл-структуры, однако вместо рассеивающей среды используется пространственный модулятор света (англ. SLM – spatial light modulator), на который загружено случайное фазовое распределение (фазовая маска). Данная особенность позволяет обходиться лишь «зондирующим плечом», процессы в котором идентичны описанным в псевдотепловом случае. В свою очередь, «воспроизводящее плечо» является «виртуальным»: по имеющийся случайной фазовой маске, загруженной на SLM, и падающей на него интенсивности с помощью пропагатора Френеля-Гюйгенса можно рассчитать пространственное распределение интенсивностей на заданном расстоянии. Другими словами, зная расстояние между SLM и изучаемым объектом, можно заранее рассчитать, какая именно по форме спекл-структура попадет на объект при заданной фазовой маске, а ее вид будет с высокой степенью точности совпадать с реальной. Дальнейший процесс восстановления фантомного изображения будет идентичен описанному в псевдотепловом ФИ, только теперь в функции корреляции интенсивностей (1.1) слагаемое I(x, y) будет рассчитано на компьютере, а не зарегистрировано многопиксельной камерой. Важность данной модификации заключается в миниатюризации и упрощении оптической схемы, а также в том, что процесс формирования спекл-структур становится более контролируемым, что позволяет оптимизировать параметры системы и увеличить ее быстродействие.

На сегодняшний день одной из главных проблем ФИ остается большое число итераций, необходимых для восстановления изображения. Другими словами, данная технология не обладает необходимым быстродействием. Современные подходы к ее решению основаны на комбинации вычислительных ФИ и методов машинного обучения [89]. Отдельно стоит упомянуть, что данный подход позволяет существенно сократить чис-

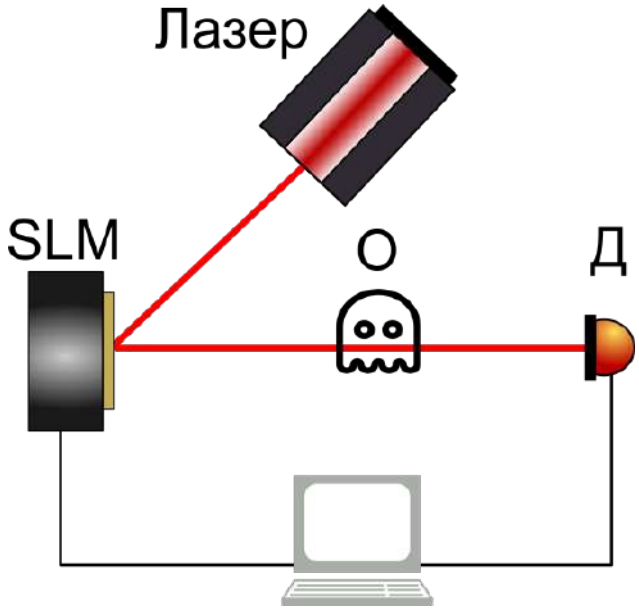


Рис. 64: Принципиальная схема вычислительных ФИ, где SLM – пространственный модулятор света, О – объект, Д – однопиксельный (собирающий) детектор

ло итераций и, как следствие, время на восстановление изображения, что открывает путь данной технологии к ее практическому использованию.

Далее будет рассмотрено, в чем заключается преимущество и практическая значимость технологии ФИ. Стоит сразу сказать, что данная технология не претендует на замену существующим классическим методам получения изображения, а направлена на использование в ранее недоступных сценариях. В частности, основным достоинством ФИ является их сильная помехоустойчивость, что позволяет использовать данную технологию в сложных погодных условиях и других сценариях с высоким содержанием посторонних шумов в канале. Данное преимущество обеспечивается запутанностью при квантовом случае и случайным распределением спеклов в псевдотепловом случае (при этом важно, чтобы спекл структуры, падающие на объект, и зарегистрированные камерой/рассчитанные на компьютере совпадали, что накладывает дополнительные ограничения). Преодоление существующего дифракционного предела – другое потенциальное применение данной технологии. Вследствие того, что дифракционный предел определяется половиной длиной волны, а существующие регистрирующие системы ограничены определёнными спектральными диапазонами, актуальной является задача поиска методов, позволяющих обойти ограничения, связанные с дифрак-

ционным пределом. Данная задача может быть решена с помощью квантового метода ФИ. При помощи процесса спонтанного параметрического рассеяния (СПР) можно создать пару запутанных фотонов на разных длинах волн: на малой длине волны для облучения объекта и на большой для регистрации на существующие камеры (важно отметить, что фотон на малой длине волны тоже должен быть зарегистрирован, но вследствие необходимости получения только общей интенсивности эта задача является более простой и экономически выгодной). Также данный принцип позволяет изучать светочувствительные объекты, которые не выдерживают высокоэнергетического коротковолнового излучения [90].

8.5 Вывод

Таким образом, в главе 8 были рассмотрены теоретические основы технологии ФИ, разобраны основные методики, изучены математические принципы и показано современное состояние представленной научной области. Технология ФИ находятся на достаточно ранней стадии своего развития, однако научными группами со всего мира уже были сделаны важные и перспективные открытия, которые открывают данной технологии дорогу к практическому применению. Также дополним, что технология ФИ является одной из точек соприкосновения квантовой и классической теорий, что может привести к новым научным открытиям.

8.6 Контрольные вопросы

1. Принцип работы оптической схемы формирования квантовых фантомных изображений.

2. Принцип работы оптической схемы формирования псевдотепловых фантомных изображений.

3. Что является основной идеей псевдотепловых ФИ?

4. Какие соотношения расстояний в плечах необходимо соблюдать для предотвращения искажения изображения объекта, полученного с помощью псевдотеплового метода?

5. В чем заключается различие квантового и псевдотеплового фантомного изображения?

6. Какие параметры являются основными при восстановлении фантомного изображения?

7. Как определяется соотношение “вход-выход” для квантового случая для спонтанного параметрического рассеяния на кристалле?

8. Как определяется соотношение “вход-выход” на светоделителе для псевдотеплового случая?

9. В чем заключается главная проблема при восстановлении фантомных изображений?

10. В чем заключается основное достоинство фантомных изображений?

Список литературы

[1] Matthew D Eisaman, Jingyun Fan, Alan Migdall, and Sergey V Polyakov. Invited review article: Single-photon sources and detectors. *Review of scientific instruments*, 82(7):071101, 2011.

[2] Gilbert N Lewis. The conservation of photons. *Nature*, 118(2981):874–875, 1926.

[3] Paul Adrien Maurice Dirac. The quantum theory of the emission and absorption of radiation. *Proceedings of the Royal Society of London. Series A, Containing Papers of a Mathematical and Physical Character*, 114(767):243–265, 1927.

[4] George P. Miroshnichenko, Alexei D. Kiselev, Alexander I. Trifanov, and Artur V. Gleim. Algebraic approach to electro-optic modulation of light: exactly solvable multimode quantum model. *J. Opt. Soc. Am. B*, 34(6):1177–1190, 2017.

[5] Karl Kraus, Arno Böhm, John D Dollard, and WH Wootters. States, effects, and operations: fundamental notions of quantum theory. lectures in mathematical physics at the university of texas at austin. *Lecture notes in physics*, 190, 1983.

[6] W Forrest Stinespring. Positive functions on c*-algebras. *Proceedings of the American Mathematical Society*, 6(2):211–216, 1955.

[7] Man-Duen Choi. Completely positive linear maps on complex matrices. *Linear algebra and its applications*, 10(3):285–290, 1975.

[8] Alexander Semenovich Holevo. Bounds for the quantity of information transmitted by a quantum communication channel. *Problemy Peredachi Informatsii*, 9(3):3–11, 1973.

[9] Benjamin Schumacher, Michael Westmoreland, and William K Wootters. Limitation on the amount of accessible information in a quantum channel. *Physical review letters*, 76(18):3452, 1996.

[10] Benjamin Schumacher. Quantum coding. *Physical Review A*, 51(4):2738, 1995.

[11] Michael A Nielsen and Isaac L Chuang. Quantum computation and quantum information, 2000.

[12] Christopher A Fuchs. Distinguishability and accessible information in quantum theory. *arXiv preprint quant-ph/9601020*, 1996.

[13] Igor Devetak. The private classical capacity and quantum capacity of a quantum channel. *IEEE Transactions on Information Theory*, 51(1):44–55, 2005.

[14] G. Brassard C. H. Bennett. The dawn of a new era for quantum cryptography: The experimental prototype is working! *ACM SIGACT News*, 20(4):78–80, 1989.

[15] Y. S. Kim, Y. C. Jeong, and Y. H. Kim. Implementation of polarization-coded free-space bb84 quantum key distribution. *Laser Physics*, 18(6):810, Jun 2008.

[16] V. L. Kurochkin, A. V. Zverev, Yu. V. Kurochkin, I. I. Ryabtsev, and I. G. Neizvestny. Experimental studies in quantum cryptography. *Russian Microelectronics*, 40(4):245–253, Jul 2011.

[17] V. L. Kurochkin and A. V. Kolyako. Investigating the bit rate of a quantum key over free space, depending on the conditions of transmission. *Bulletin of the Russian Academy of Sciences: Physics*, 80(1):1–4, Jan 2016.

[18] V. L. Kurochkin, I. I. Ryabtsev, and I. G. Neizvestny. Experimental setup for quantum cryptography by means of single polarized photons. *Technical Physics*, 50(6):727–731, Jun 2005.

[19] M. Bohmann, R. Kruse, J. Sperling, C. Silberhorn, and W. Vogel. Probing free-space quantum channels with laboratory-based experiments. *Phys. Rev. A*, 95:063801, Jun 2017.

[20] M. J. García-Martínez, N. Denisenko, D. Soto, D. Arroyo, A. B. Orue, and V. Fernandez. High-speed free-space quantum key distribution system for urban daylight applications. *Appl. Opt.*, 52(14):3311–3317, May 2013.

[21] Tobias Schmitt-Manderbach, Henning Weier, Martin Fürst, Rupert Ursin, Felix Tiefenbacher, Thomas Scheidl, Josep Perdigues, Zoran Sodnik, Christian Kurtsiefer, John G. Rarity, Anton Zeilinger, and Harald Weinfurter. Experimental demonstration of free-space decoy-state quantum key distribution over 144 km. *Phys. Rev. Lett.*, 98:010504, Jan 2007.

[22] Ursin R. et al. Entanglement-based quantum communication over 144 km. *Nature physics.*, 3:010504, Jan 2007.

[23] Nauerth S. et al. Air-to-ground quantum communication. *Nature Photonics.*, 7:382–386, Jan 2013.

[24] Christopher J Pugh, Sarah Kaiser, Jean-Philippe Bourgoin, Jeongwan Jin, Nigar Sultana, Sascha Agne, Elena Anisimova, Vadim Makarov, Eric Choi, Brendon L Higgins, and Thomas Jennewein. Airborne demonstration of a quantum key distribution receiver payload. *Quantum Science and Technology*, 2(2):024009, 2017.

[25] P Villoresi, T Jennewein, F Tamburini, M Aspelmeyer, C Bonato, R Ursin, C Pernechele, V Luceri, G Bianco, A Zeilinger, and C Barbieri. Experimental verification of the feasibility of a quantum channel between space and earth. *New Journal of Physics*, 10(3):033038, 2008.

[26] C Bonato, A Tomaello, V Da Deppo, G Naletto, and P Villoresi. Feasibility of satellite quantum key distribution. *New Journal of Physics*, 11(4):045017, 2009.

[27] Jian-Yu Wang, Bin Yang, Sheng-Kai Liao, Liang Zhang, Qi Shen, Xiao-Fang Hu, Jin-Cai Wu, Shi-Ji Yang, Hao Jiang, Yan-Lin Tang, et al. Direct and full-scale experimental verifications towards ground–satellite quantum key distribution. *Nature Photonics*, 7(5):387, 2013.

[28] Juan Yin, Yuan Cao, Yu-Huai Li, Sheng-Kai Liao, Liang Zhang, Ji-Gang Ren, Wen-Qi Cai, Wei-Yue Liu, Bo Li, Hui Dai, et al. Satellite-based entanglement distribution over 1200 kilometers. *Science*, 356(6343):1140–1144, 2017.

[29] Sheng-Kai Liao, Hai-Lin Yong, Chang Liu, Guo-Liang Shentu, Dong-Dong Li, Jin Lin, Hui Dai, Shuang-Qiang Zhao, Bo Li, Jian-Yu Guan, et al. Long-distance free-space quantum key distribution in daylight towards inter-satellite communication. *Nature Photonics*, 11(8):509, 2017.

[30] Bruno Piccirillo, Vincenzo D'Ambrosio, Sergei Slussarenko, Lorenzo Marrucci, and Enrico Santamato. Photon spin-to-orbital angular momentum conversion via an electrically tunable q-plate. *Applied Physics Letters*, 97(24):241104, 2010.

[31] Vincenzo D'ambrosio, Eleonora Nagali, Stephen P Walborn, Leandro Aolita, Sergei Slussarenko, Lorenzo Marrucci, and Fabio

Sciarrino. Complete experimental toolbox for alignment-free quantum communication. *Nature communications*, 3:961, 2012.

[32] Giuseppe Vallone, Vincenzo D'Ambrosio, Anna Sponselli, Sergei Slussarenko, Lorenzo Marrucci, Fabio Sciarrino, and Paolo Villoresi. Free-space quantum key distribution by rotation-invariant twisted photons. *Physical review letters*, 113(6):060503, 2014.

[33] Alicia Sit, Frédéric Bouchard, Robert Fickler, Jérémie Gagnon-Bischoff, Hugo Larocque, Khabat Heshami, Dominique Elser, Christian Peuntinger, Kevin Günthner, Bettina Heim, et al. High-dimensional intracity quantum cryptography with structured photons. *Optica*, 4(9):1006–1010, 2017.

[34] Hugo Larocque, Jérémie Gagnon-Bischoff, Dominic Mortimer, Yingwen Zhang, Frédéric Bouchard, Jeremy Upham, Vincenzo Grillo, Robert W Boyd, and Ebrahim Karimi. Generalized optical angular momentum sorter and its application to high-dimensional quantum cryptography. *Optics Express*, 25(17):19832–19843, 2017.

[35] Thomas Jennewein, Ulrich Achleitner, Gregor Weihs, Harald Weinfurter, and Anton Zeilinger. A fast and compact quantum random number generator. *Review of Scientific Instruments*, 71(4):1675–1680, 2000.

[36] André Stefanov, Nicolas Gisin, Olivier Guinnard, Laurent Guinnard, and Hugo Zbinden. Optical quantum random number generator. *Journal of Modern Optics*, 47(4):595–598, 2000.

[37] Qiurong Yan, Baosheng Zhao, Qinghong Liao, and Nanrun Zhou. Multi-bit quantum random number generation by measuring positions of arrival photons. *Review of Scientific Instruments*, 85(10):103116, 2014.

[38] Witjaksono Gunawan. A quantum random number generator. *Patent*, WO 2009064167 A2:15, 05 2009.

[39] Gregoire Ribordy, Jean-Daniel Gautier, Hugo Zbinden, and Nicolas Gisin. Performance of ingaas/inp avalanche photodiodes as gated-mode photon counters. *Applied optics*, 37(12):2272–2277, 1998.

[40] Mario Stipčević and B Medved Rogina. Quantum random number generator based on photonic emission in semiconductors. *Review of scientific instruments*, 78(4):045104, 2007.

[41] Marco Fiorentino, C M. Santori, S M. Spillane, William Munro, and R G. Beausoleil. Secure self-calibrating quantum random bit generator. *Physical Review A*, 75, 01 2007.

[42] Osung Kwon, Young-Wook Cho, and Yoon-Ho Kim. Quantum random number generator using photon-number path entanglement. *Applied Optics*, 48(9):1774–1778, 2009.

[43] MJ Applegate, O Thomas, JF Dynes, ZL Yuan, DA Ritchie, and AJ Shields. Efficient and robust quantum random number generation by photon number detection. *Applied Physics Letters*, 107(7):071106, 2015.

[44] Min Ren, E Wu, Yan Liang, Yi Jian, Guang Wu, and Heping Zeng. Quantum random-number generator based on a photon-number-resolving detector. *Physical Review A*, 83(2):023820, 2011.

[45] Xiongfeng Ma, Xiao Yuan, Zhu Cao, Bing Qi, and Zhen Zhang. Quantum random number generation. *npj Quantum Information*, 2(1):1–9, 2016.

[46] Harald Fürst, Henning Weier, Sebastian Nauerth, Davide G Marangon, Christian Kurtsiefer, and Harald Weinfurter. High speed optical quantum random number generation. *Optics express*, 18(12):13029–13037, 2010.

[47] ZL Yuan, BE Kardynal, AW Sharpe, and AJ Shields. High speed single photon detection in the near infrared. *Applied Physics Letters*, 91(4):041114, 2007.

[48] Thomas Symul, SM Assad, and Ping K Lam. Real time demonstration of high bitrate quantum random number generation with coherent laser light. *Applied Physics Letters*, 98(23):231103, 2011.

[49] Клышко Д.Н. Когерентный распад фотонов в нелинейной среде. *Письма в Журнал экспериментальной и теоретической физики*, 6(1):490–492, 1967.

[50] Хохлов Р.В. Чунаев О.Н. Ахманов С.А., Фадеев В.В. Квантовые шумы в параметрических уселителителях света. *Письма в Журнал экспериментальной и теоретической физики*, 6:575–578, 1967.

[51] Byer R. L. Harris S. E., Oshman M. K. Observation of tunable optical parametric fluorescence. *Physical Review Letters*, 18(18):732, 1967.

[52] Byer R. L. Harris S. E., Oshman M. K. *Physical Review Letters*, 18:905, 1967.

[53] Ярив А. *Квантовая электроника и нелинейная оптика.* Сов. радио, 1973.

[54] Nikogosyan D. N. Dmitriev V. G., Gurzadyan G. G. *Handbook of nonlinear optical crystals.* Физматлит, 2009.

[55] Shih Y. Entangled biphoton source-property and preparation. *Reports on Progress in Physics*, 66(6):1009, 2003.

[56] Fejer M. M. et al. Quasi-phase-matched second harmonic generation: tuning and tolerances. *IEEE Journal of quantum electronics*, 28(11):2631–2654, 1992.

[57] Magnitskiy S. et al. A spdc-based source of entangled photons and its characterization. *Journal of Russian Laser Research*, 36(6):618–629, 2015.

[58] Bennett C. H. et al. Teleporting an unknown quantum state via dual classical and einstein-podolsky-rosen channels. *Physical Review Letters*, 7(13):1895, 1993.

[59] Chun-Yan L. et al. Secure quantum key distribution network with bell states and local unitary operations. *Chinese Physics Letters*, 22(5):1049, 2005.

[60] Lim C. C. W. et al. Device-independent quantum key distribution with local bell test. *Physical Review Letters*, 3(3):031006, 2013.

[61] Clauser J. F. et al. Proposed experiment to test local hidden-variable theories. *Physical Review Letters*, 23(5):880, 1969.

[62] Kwiat P. G. Altepeter J. B., Jeffrey E. R. Phase-compensated ultra-bright source of entangled photons. *Optics Express*, 13(22):8951–8959, 2005.

[63] Kuklewicz C. E. et al. High-flux source of polarization-entangled photons from a periodically poled ktiopo 4 parametric down-converter. *Physical Review A.*, 69(1):013807, 2004.

[64] Wong F.N.C. Kim T., Fiorentino M. Phase-stable source of polarization-entangled photons using a polarization sagnac interferometer. *Physical Review A.*, 73(1):012316, 2006.

[65] Tabakaev D. et al. On the role of entanglement in entangled two-photon absorption molecular spectroscopy. *arXiv preprint arXiv*, page 1910.07346, 2019.

[66] Strekalov D. V. et al. Observation of two-photon "ghost" interference and diffraction. *Physical Review Letters*, 74(18):3600, 1995.

[67] Shih Y. Karmakar S., Meyers R. E. Noninvasive high resolving power entangled photon quantum microscope. *Journal of Biomedical Optics*, 20(1):016008, 2015.

[68] Chen H. et al. Experimental demonstration on the deterministic quantum key distribution based on entangled photons. *Scientific reports*, 6(1):1–8, 2016.

[69] Ekert A. K. Quantum cryptography and bell's theorem. *Quantum Measurements in Optics*, pages 413–418, 1992.

[70] Bocquillon E. et al. Coherence measures for heralded single-photon sources. *Physical Review A.*, 79(3):035801, 2009.

[71] Fiorentino M. et al. Secure self-calibrating quantum random-bit generator. *Physical Review A.*, 75(3):032334, 2007.

[72] Fink M. et al. Entanglement-enhanced optical gyroscope. *New Journal of Physics*, 21(5):053010, 2019.

[73] Mandel L. Hong C. K., Ou Z. Y. Measurement of subpicosecond time intervals between two photons by interference. *Physical Review Letters*, 59(18):2044, 1987.

[74] O'Brien J. L. et al. Demonstration of an all-optical quantum controlled-not gate. *Nature*, 426(6964):264–267, 2003.

[75] Strekalov D. V. et al. Observation of two-photon "ghost" interference and diffraction. *Physical review letters*, 74(18):3600, 1995.

[76] Pittman T. B. et al. Optical imaging by means of two-photon quantum entanglement. *Physical Review A*, 52(5):R3429, 1995.

[77] Valencia A. et al. Two-photon imaging with thermal light. *Physical review letters*, 94(6):063601, 2005.

[78] Chen X. H. et al. Lensless ghost imaging with true thermal light. *Physical Review A*, 34(5):695–697, 2009.

[79] Han S. Gong W. Lens ghost imaging with thermal light: From the far field to the near field. *Physical Review A*, 374(36):3723–3725, 2010.

[80] Sasian J. M. Abd El-Maksoud R. H. Paraxial ghost image analysis. In *Current Developments in Lens Design and Optical Engineering X*, volume 7428, pages 84–95. SPIE, 2009.

[81] Shih Y. Meyers R., Deacon K. S. Ghost-imaging experiment by measuring reflected photons. *Physical Review A*, 77(4):041801, 2008.

[82] Shapiro J. H. Hardy N. D. Ghost imaging in reflection: resolution, contrast, and signal-to-noise ratio. In *Quantum Communications and Quantum Imaging VIII*, volume 7815, pages 112–124. SPIE, 2010.

[83] Huang J. et al. Spectral encoded computational ghost imaging. *Optics Communications*, 474:126105, 2020.

[84] Qian Y. et al. Adaptive compressed 3d ghost imaging based on the variation of surface normals. *Optics Express*, 27(20):27862–27872, 2019.

[85] Колобов М. И. *Квантовое изображение*. Физматлит, 2009.

[86] Boyd R. W. Shapiro J. H. The physics of ghost imaging. *Quantum Information Processing*, 11(4):949–993, 2012.

[87] Shih Y. Quantum imaging. *Journal of Selected Topics in Quantum Electronics*, 13(4):1016–1030, 2007.

[88] Silberberg Y. Bromberg Y., Katz O. Ghost imaging with a single detector. *Physical Review A*, 79(5):053840, 2009.

[89] Lyu M. et al. Deep-learning-based ghost imaging. *Scientific reports*, 7(1):1–6, 2017.

[90] Shih Y. Karmakar S., Meyers R. E. Noninvasive high resolving power entangled photon quantum microscope. *Journal of Biomedical Optics*, 20(1):016008, 2015.

Кынев Сергей Михайлович
Гайдаш Андрей Алексеевич
Егоров Владимир Ильич
Козубов Антон Владимирович
Самсонов Эдуард Олегович
Наседкин Борис Александрович
Иванова Алена Евгеньевна

Квантовые технологии

Учебно-методическое пособие

В авторской редакции
Редакционно-издательский отдел Университета ИТМО
Зав. РИО Н.Ф. Гусарова
Подписано к печати
Заказ №
Тираж
Отпечатано на ризографе

Редакционно-издательский отдел
Университета ИТМО
197101, Санкт-Петербург, Кронверкский пр., 49, литер А