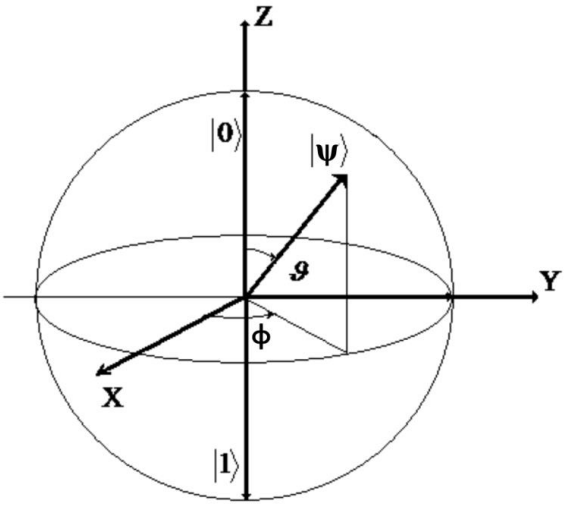
УНИВЕРСИТЕТ ИТМО

А.А. Гайдаш, Б.А. Наседкин, Э.О. Самсонов,

С.В. Савельева

КВАНТОВЫЕ ТЕХНОЛОГИИ

методические указания к лабораторным работам



Санкт-Петербург
2022

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ
РОССИЙСКОЙ ФЕДЕРАЦИИ
УНИВЕРСИТЕТ ИТМО

А.А. Гайдаш, Б.А. Наседкин, Э.О. Самсонов, С.В. Савельева

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», 12.05.01 «Электронные и оптико-электронные приборы и системы специального назначения», 16.03.01. «Техническая физика», 18.03.02 «Энерго- и ресурсосберегающие процессы в химической технологии, нефтехимии и биотехнологии» в качестве учебно-методического пособия для реализации основных профессиональных образовательных программ высшего образования бакалавриата и специалитета.

Санкт-Петербург
2022

А.А. Гайдаш, Б.А. Наседкин, Э.О. Самсонов, С.В. Савельева Квантовые технологии. – СПб: Университет ИТМО, 2022. – 73 с.

Рецензент: к.ф-м.н., Трифанов А. И., доцент факультета СУиР Университета ИТМО

В учебно-методическом пособии представлены краткие теоретические сведения, порядок выполнения лабораторных работ в рамках дисциплины «Квантовые технологи». Представленный материал может быть также полезен при выполнении курсового и дипломного проектирования.

Учебно-методическое пособие предназначено для бакалавров и специалистов, обучающихся по направлениям подготовки 12 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», 12.05.01 «Электронные и оптико-электронные приборы и системы специального назначения», 16.03.01. «Техническая физика», 18.03.02 «Энерго- и ресурсосберегающие процессы в химической технологии, нефтехимии и биотехнологии»

Оглавление

Лабораторная работа №1

ГЕНЕРАЦИЯ СЕКРЕТНОГО КЛЮЧА С ПОМОЩЬЮ КВАНТОВО–КРИПТОГРАФИЧЕСКОЙ УЧЕБНО-ИССЛЕДОВАТЕЛЬСКОЙ УСТАНОВКИ НА ОСНОВЕ НЕСИММЕТРИЧНОГО ВОЛОКОННО-ОПТИЧЕСКОГО ИНТЕРФЕРОМЕТРА МАЙКЕЛЬСОНА (ПНП)

Цель работы: Изучение основ квантовой криптографии.

Задачи, решаемые в работе

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

Краткие теоретические сведения

Основными проблемами классической криптографии являются аутентификация и распределение ключа. Первая проблема связана с распознаванием легитимных пользователей друг другом. Вторая проблема призвана обеспечить наличие у сторон идентичного секретного ключа, который в дальнейшем используется для кодирования и декодирования информации [1].

Безусловно секретным ключом (по Шеннону) является такой ключ, который представляет собой набор случайных (двоичных) символов, длина которого не меньше длины передаваемого сообщения и который используется лишь один раз. Однако снабжать каждое сообщение новым секретным ключом представляется трудоемкой и дорогостоящей задачей. На сегодняшний день известны способы частичного решения проблемы распределения ключа. Некоторые из них связаны с так называемыми двухключевыми или асимметричными протоколами. Они принадлежат к классу вычислительно стойких, т. е. когда раскрытие ключа становится экономически невыгодным или когда вычисление требует больше времени, чем время «ценности» сообщения. Примером асимметричных способов шифрования служит метод, предложенный в 1976 году У. Диффи и М. Хеллманом. Другим решением проблемы распределения ключа является использование квантовых носителей информации – квантовая криптография. На основе квантовых состояний, в принципе, можно генерировать безусловно секретные ключи и легко их менять. Однако заметим, что квантовое распределение ключа не решает проблему аутентификации [2,3].

Принцип генерации и квантовой рассылки секретного ключа

Квантовая криптография является, по всей видимости, единственной ветвью науки о квантовой информации и квантовой связи, реализованной на приборном уровне. Безусловная секретность ключа, распределенного между легитимными пользователями при помощи квантовых систем, определяется теоремой о запрете клонирования неизвестного квантового состояния. В известных на сегодняшний день квантовых криптографических системах используется кодирование информации в неортогональных состояниях двухуровневых систем, или кубитах, наиболее известными из которых являются протокол на двух (B92) и на четырех состояниях (BB84). Вместе с тем в литературе рассматривается множество других способов реализации секретных сообщений на основе квантовых состояний, например, протокол на перепутанных состояниях. Однако на практике секретность квантового распределения ключа (КРК) ограничена рядом факторов. Это ошибки и потери, возникающие в канале связи при передаче, отличие подготовленных состояний от идеальных, погрешности системы измерения (например, вызванные темновыми отсчетами фотодетекторов) и т. д. Именно перечисленные ошибки в основном ограничивают длину канала связи, в пределах которой гарантирована секретность квантового распределения ключа [4,5].

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

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

1. Алиса генерирует случайную последовательность битов. Боб генерирует свою последовательность битов независимо от Алисы.
2. Алиса сообщает фотонам необходимое квантовое состояние в соответствии с генерируемой случайной последовательностью и выбранным протоколом. Боб измеряет текущие квантовые состояния фотонов, изменяя состояние модулятора (-ов) в соответствии с генерируемой им случайной последовательностью и выбранным протоколом (п.1).
3. После окончания передачи последовательности Алиса и Боб обсуждают проведенные измерения по открытому каналу. Алисе необходимо знать последовательность базисов, которые использовал Боб при измерении состояния зарегистрированного фотона (результат измерения Боб не

сообщает), или необходимо знать номера битов зарегистрированных фотонов (состояние модулятора Боба не сообщается).

4. Алиса и Боб сравнивают свои последовательности битов и отбрасывают те случаи, когда их базисы не совпали и (или) когда фотон не был зарегистрирован. Оставшиеся значения бит и составляют «сырой» ключ. Ключ называется «сырым», поскольку он содержит ошибки. Под ошибками понимается несовпадение ключей Алисы и Боба. Алиса и Боб определяют число ошибок при передаче ключа, путём раскрытия небольшой части сырого ключа. Если число ошибок выше некоторого критического значения, то это свидетельствует о присутствии злоумышленника, обычно называемого Евой (Eve), и ключ аннулируется.
5. Алиса и Боб проводят коррекцию полученного ключа.

Квантово-криптографическая установка

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

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

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

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

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

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

Импульс (λ=1310 нм, τ=5 нс), излучаемый лазерным диодом ЛД со стороны Боба, пройдя волоконный светоделитель ВСД1, делится в отношении 50/50 светоделителем ВСД2. Один из световых импульсов попадает сразу на линию связи и именуется **Fast**. Другой пучок сначала проходит через линию задержки (задерживающее волокно ЗВ1) и фазовый модулятор ФМ1, затем отражается от фарадеевского зеркала ФЗ1 и проходит обратный путь к светоделителю ВСД2. Попадает на второе фарадеевское зеркало ФЗ2,

отражается и только после этого выходит на линию связи. Этот луч именуется **Slow**. Разделенные по времени импульсы Fast и Slow двигаются к Алисе: 90% света через светоделитель ВСД3 Алисы уходит на фотодиод Алисы. Более мощный импульс Fast используется для синхронизации срабатывания модулятора Алисы, а оставшиеся 10% проходят через ослабитель (аттенюатор) О и фазовый модулятор ФМ2 Алисы, затем отражаются от фарадеевского зеркала ФЗ3 и двигаются обратно к Бобу.

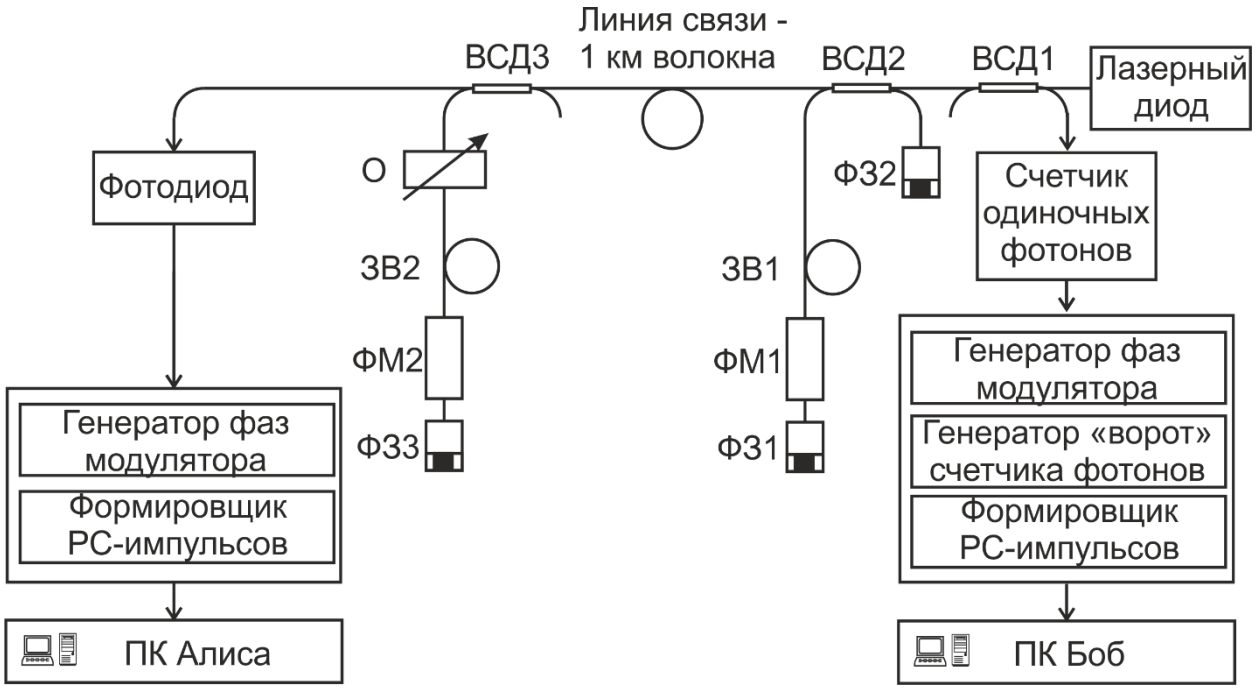


Рисунок 1 – Схема лабораторной установки

Прибывшие к Бобу импульсы проходят через делитель ВСД2 с зеркалами Фарадея в обратном порядке (ФЗ2 и ФЗ1) и попадают на светоделитель ВСД1. Необходимо отметить, что фазовый модулятор Боба активен только для импульсов, уже вернувшихся со стороны Алисы. После делителя СВД2 образуются четыре импульса: **FastFast** (не претерпевает модуляцию), **FastSlow** (претерпевает модуляцию на стороне Боба, приобретая возможный сдвиг фазы 0 или π), **SlowFast** (претерпевает модуляцию на стороне Алисы, приобретая возможный сдвиг фазы 0 или π) и **SlowSlow**, два из которых, **FastSlow** и **SlowFast**, приходят одновременно и интерферируют. Разница фаз импульсов **FastSlow и SlowFast** может быть равной **0** или **π**, что соответствует конструктивной или деструктивной интерференции на входе счётчика фотонов на стороне Боба. Результат интерференции измеряется счетчиком единичных фотонов. Для правильной работы счётчика фотонов необходим точный выбор времени задержки открывания счетчика фотонов. Счётчик должен открываться только на время, в течение которого ожидается приход интерферирующих импульсов. Время открытия счётчика (10 нс, так называемые “ворота”) выбрано немного больше длительности импульса (5 нс). Время задержки “ворот” можно менять в двоичном коде с помощью

восьми переключателей, расположенных на передней панели блока Боба. Справа расположены младшие разряды, слева - старшие. **Время задержки можно менять только с разрешения преподавателя**. Процесс передачи информации можно описать следующим образом:

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

Следует учесть, что из-за низкой квантовой эффективности детектирования единичных фотонов (порядка 10 %) и малой средней оптической мощности (меньше одного фотона на импульс в интерферирующих импульсах) средний процент зарегистрированных фотонов в единицу времени значительно меньше числа передаваемых импульсов за тот же промежуток времени. Это приводит к тому, что длина сырого ключа оказывается значительно меньше длины передаваемой последовательности импульсов в течение сеанса связи, но это не даёт ошибки в сыром ключе. Ошибки сырого ключа возникают из-за несовершенства оптической схемы (видность интерференции не равна 100%), темновых отсчетов и деятельности потенциального злоумышленника. В данной работе основной вклад в ошибку дают темновые отсчёты. Это приводит к тому, что криптографические сырые ключи Боба и Алисы будут в некоторой степени различаться.

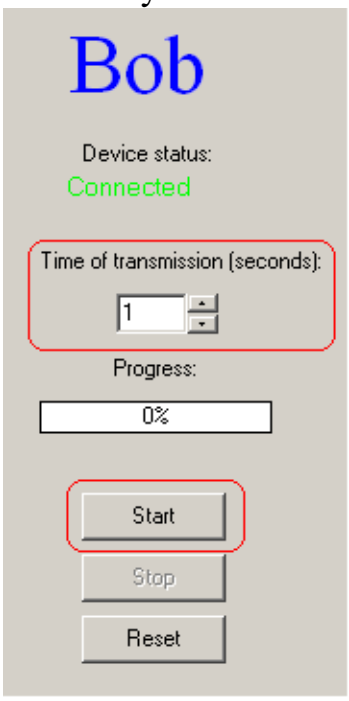
Ход лабораторной работы

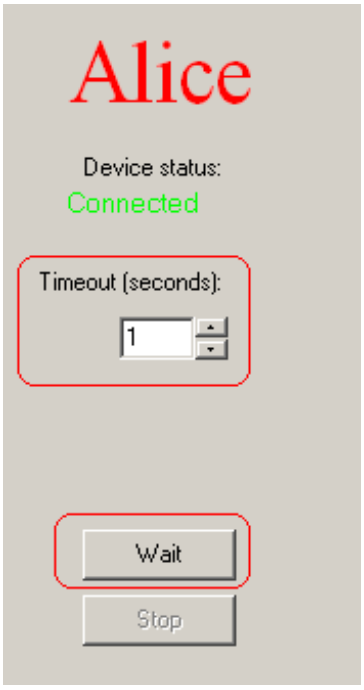
Включить блоки Алисы и Боба черным тумблером на задней панели каждого устройства. Пока не запущены программы Алисы и Боба на соответствующих компьютерах, блоки Алисы и Боба работают в автоколебательном режиме. С блока Боба передаётся непрерывная последовательность оптических импульсов. Модулятор Боба может работать

в трёх режимах: всегда фаза **0** для **FastSlow**, случайная фаза для **FastSlow** и всегда фаза **π** для **FastSlow**. Выбор режима осуществляется трёхпозиционным тумблером, расположенным внизу справа на передней панели блока Боба. Переключение производится в горизонтальном направлении. Правое положение – **фаза 0**, среднее положение – **фаза случайная**, левое положение – **фаза π**. Блок Алисы в автоматическом режиме постоянно принимает световые импульсы, и модулятор Алисы работает в режиме случайной модуляции. Счетчик фотонов включается при нажатии кнопки **Power** на передней панели устройства. При этом на дисплее счетчика высветится численное значение частоты отсчётов принимаемого сигнала в герцах. Время выхода на рабочую температуру лавинного фотодиода составляет около 10 минут.

1. Вначале включается только блок Боба. Режим модулятора – **фаза π**. В этом случае модулятор Алисы **не работает,** импульсы **Fast** и **Slow** не модулируются Алисой, и будет наблюдаться только **деструктивная** интерференция. Если **время задержки включения счётчика фотонов выбрано правильно**, то счётчик фотонов будет регистрировать только темновые отсчёты. При других значениях частоты отсчётов есть возможность установить обратное напряжение на фотодиоде в ручном режиме. При переключении режима модулятора на **фазу 0**, счётчик принимает только конструктивную интерференцию. Отношение отсчетов в конструктивном и деструктивном режимах должно быть порядка 30. При переключении режима модулятора на **фаза случайная**, счётчик принимает и конструктивную и деструктивную интерференцию. При этом частота отсчётов должна быть приблизительно в два раза меньше, чем в предыдущем случае. Если счетчик дает другие показания, то необходимо подстроить **время задержки включения счётчика фотонов** в диапазоне 1-2 младших разрядов. **Это можно делать только под руководством преподавателя!** Затем устанавливаем режим модулятора Боба в среднее положение - **фаза случайная.**
2. Включается блок Алисы. При этом будет иметь место как деструктивная, так и конструктивная интерференция (с вероятностью примерно 50% для каждой) независимо от режима модулятора Боба. Это можно проверить, переключая режимы модулятора Боба и следя за отсчётами счётчика фотонов.
3. С рабочего стола компьютера Боба запускаем программу Боба, а с компьютера Алисы — соответствующую программу Алисы. В появившемся окне программы Боба выбираем продолжительность сеанса генерации ключа (**Time of transmission**) – длительность передачи лазерных импульсов, обычно это 5 – 10 секунд. Продолжительность генерации ключа определяет длину ключа. В аналогичном окне Алисы выбираем время ожидания после окончания сеанса передачи, после которого Алиса заканчивает сеанс связи (**Timeout**). 1 секунда – достаточное время.

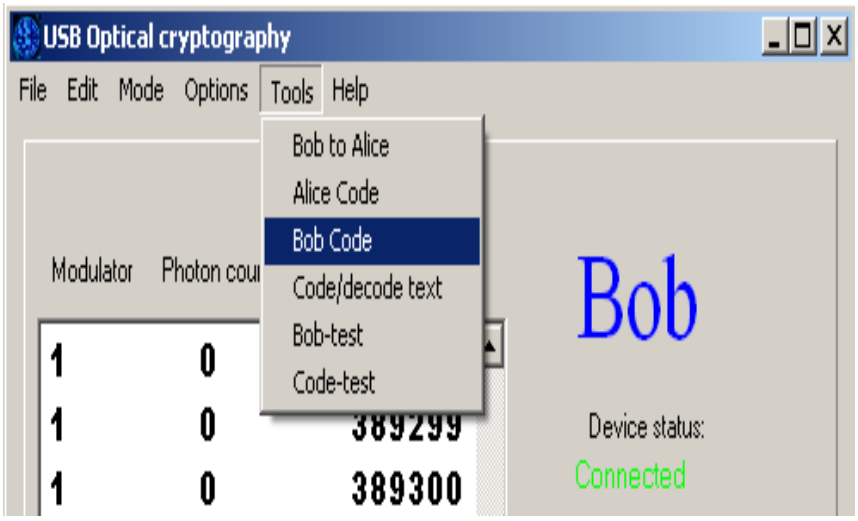
4. **Сначала** на стороне Алисы нажимаем кнопку **«wait»**, затем на стороне Боба – кнопку **«start»**.

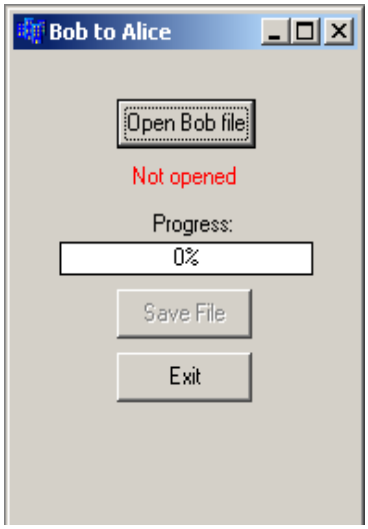




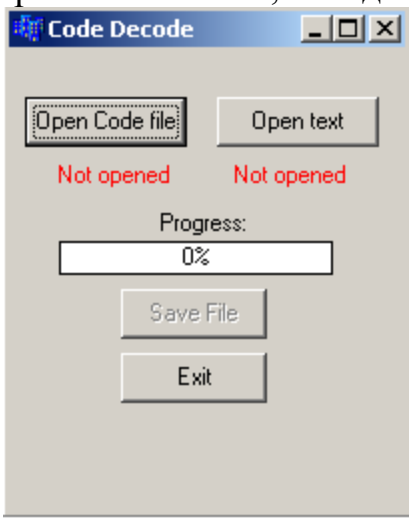
Итак, по прошествии времени сеанса мы получили последовательность состояний на модуляторе Боба (столбец Modulator), показания отсчётов счетчика (столбец **Photon counter**), а также столбец с порядковым номером каждого отсчета. У Алисы своя пронумерованная последовательность. У Алисы отсутствует столбец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

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





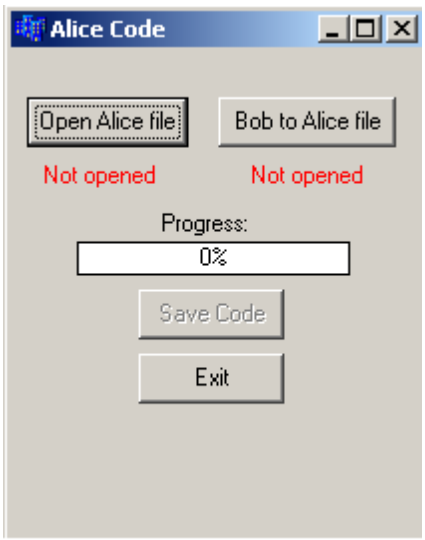
6. **Сформируем файл отсчётов счётчика фотонов**, который будет передаваться по открытому каналу Алисе. Выполняем следующую операцию: **Tools→Bob to Alice**. В появившемся окне нажимаем на кнопку «**Open Bob file**» и также выбираем файл **Bob.txt.** Заканчиваем операцию: **«Save File»** (имя нового файла **Bob_to_Alice.txt**) и **«Exit».** На этом этапе мы подготовили необходимые данные для Алисы, а именно показания счетчика фотонов и порядковые номера отсчетов.
7. Создадим текстовый файл (**.txt) (**1-2 предложения), который подлежит кодировке. Можно использовать латинские буквы, пробелы, цифры и знаки препинания. Поместим файл в папку **Bob**.
8. **Закодируем текстовый файл** полученным сырым ключом. Операция: **Tools→Code/decode text**. В появившемся окне нажимаем на кнопку **«Open Code file»**, выбираем **Bob_Code.txt.** Далее – кнопка **«Open text»,** выбираем любой текстовый файл с расширением **.txt** (содержание текста не имеет значения, но его длина не должна превышать размер секретного ключа). Новый файл сохраняем под именем **Coded_text.txt** и завершаем начатую операцию кнопками **«Save File»** и **«Exit».** На этом этапе мы закодировали текст секретным ключом, находящимся у Боба.

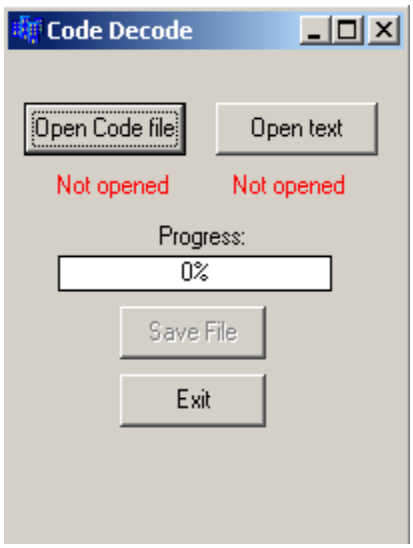


9. С помощью флэшкарты **переносим с компьютера Боба на компьютер Алисы** два файла: **Bob_to_Alice.txt и Coded_text.txt,** находящиеся в

папке **«Bob folder»** на рабочем столе (копируем их в папку **«Alice folder»**, ярлык на рабочем столе). Первый необходим для формирования ключа Алисы, а второй содержит в себе закодированный текст, который Алиса должна декодировать. Оба файла не являются секретными и могут передаваться по открытому каналу, например, по Интернету. В нашем случае используется флэшкарта.

10. **Сформируем сырой ключ Алисы.** На компьютере Алисы: **Tools→Alice_Code.** В появившемся окне: кнопка **«Open Alice file»** - выбираем **Alice.txt**, кнопка **«Bob to Alice file»** - выбираем скопированный на флэшкарту **Bob_to_Alice.txt** файл. Сохраняем этот файл под именем **Alice_Code.txt.** Завершаем операцию нажатием кнопок **«Save code»** и **«Exit».** Таким образом, у Алисы есть последовательность состояний собственного модулятора и показания счетчика фотонов, которые прислал Боб. Имея эти данные, Алиса формирует свой секретный ключ.
11. С помощью **секретного ключа Алиса декодирует** полученное сообщение от Боба **(Coded_text.txt).** Выполняется операция: **Tools→Code/decode text**. В появившемся окне нажимаем кнопку **«Open Code file»** и выбираем **Alice_Code.txt**. Следующая кнопка **«Open text»** и выбираем **Coded_text.txt**. Сохраняем новый файл как **Decoded_text.txt** и завершаем операцию. Далее можно проверить декодированный текст, в котором из-за несовершенства оборудования (конкретные причины описаны в общих положениях) будут содержаться ошибки.
12. Определить процент ошибок в сыром криптографическом ключе.





Обработка полученных результатов

1. Представить значение частоты темновых отсчётов счетчика фотонов при выключенном блоке Алисы (деструктивная интерференция).
2. Представить значение частоты отсчётов счетчика фотонов при конструктивной интерференции при выключенном блоке Алисы.

3. Представить значение частоты отсчётов счетчика фотонов при работе случайной фазовой модуляции у Боба при выключенном блоке Алисы.
4. Располагая текстом Боба и текстом, декодированным Алисой, определить процент ошибок в декодированном тексте.

Содержание отчета

1. Цель и задачи.
2. Краткое содержание теории и используемые формулы.
3. Рисунки используемых схем.
4. Текст, подлежащий кодированию, и декодированный текст.
5. Результаты, согласно требованиям раздела «Обработка полученных результатов».
6. Вывод по проделанной работе.

Контрольные вопросы

1. Что изучает квантовая криптография?
2. Какие свойства квантовых объектов используются в квантовой криптографии?
3. Почему используемая в работе установка называется «Plug&Play»? В чём состоят основные её преимущества?
4. Поясните, используя схему лабораторной установки, каким образом выполняется генерация битов абсолютно стойкого ключа (АСК).

Использованные источники литературы

1. Nielsen M.A., Chuang L.I.: Quantum computation and quantum information. Cambridge University Press, Cambridge, (2000)
2. Bennett C. H., Experimental Quantum Cryptography, Journal of Cryptology, Vol. 5, 1992, pp. 3-28.
3. Bennett C. H., Quantum Cryptography Using Any Two Nonorthogonal States, J. PHYSICAL REVIEW LETTERS, Vol. 68, № 2, 1992
4. N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, “Quantum cryptography,” Rev. Mod. Phys. **74**(1), 145–195 (2002).
5. D Stucki, N Gisin, O Guinnard, G Ribordy and H Zbinden, Quantum key distribution over 67 km with a plug&play system, New Journal of Physics, Vol. 4, January 2002

Лабораторная работа №2

ВОССТАНОВЛЕНИЕ ФАНТОМНЫХ ИЗОБРАЖЕНИЙ (ФИ)

Цель: освоить технику восстановления фантомных изображений.

Задачи, решаемые в работе

1. Провести измерения пространственного распределения интенсивности спекл-структур и интенсивностей излучения после прохождения исследуемого объекта.
2. Пользуясь полученными данными, восстановить изображение, при помощи техники восстановления фантомных изображений.

Краткие теоретические сведения

Одним из занимательных фактов в истории фантомных изображений является то, что впервые данная техника была реализована для коррелированных фотонов [1]. Техника основана на корреляционных зависимостях фотонов, генерируемых в процессе спонтанного параметрического рассеяния (СПР). Поскольку такие фотоны связаны законами сохранения энергии и импульса, можно наблюдать корреляцию по углу разлёта и частоте пар генерируемых фотонов (в данном случае мы рассматриваем характеристики, которые требуются для получения фантомных изображений). Так, рассматривая закон сохранения импульса, можно обнаружить, что для вырожденного случая волновые векторы данных фотонов имеют одинаковые значения, но противоположны по знаку. Данный факт определяет корреляцию по углу разлёта. Это означает, что при обнаружении одного из пары фотонов в точке пространства положение другого для нас становится строго определённым и рассчитывается исходя из закона сохранения импульса. Для частотного случая это будет обозначать, что, зарегистрировав фотон с определённой энергией, в другой точке пространства, соответствующей углу разлёта и времени рождения пары фотонов, мы можем обнаружить второй фотон из пары, энергия которого будет подчиняться закону сохранения энергии для СПР.

Обратимся к схеме получения фантомных изображений. В такой схеме на нелинейный кристалл направляется лазерное излучение, генерируются пары фотонов, которые направляются на поляризационный светоделитель. После светоделителя в одном из плеч устанавливается линза и исследуемый объект, при этом всё излучение собирается на один неподвижный детектор при помощи второй короткофокусной линзы. В другом плече происходит сканирование в пространстве при помощи оптического волокна, соединённого с детектором одиночных фотонов. При сканировании определяется число совпадений отсчётов на детекторах в зависимости от положения

сканирующего детектора в пространстве. При помощи полученных значений возможно получить корреляционную функцию второго порядка, которая и будет содержать в себе информацию об объекте. Важно понимать, что в данном случае изображение получается не в плече, в котором находится объект, а за счёт корреляционной функции второго порядка.

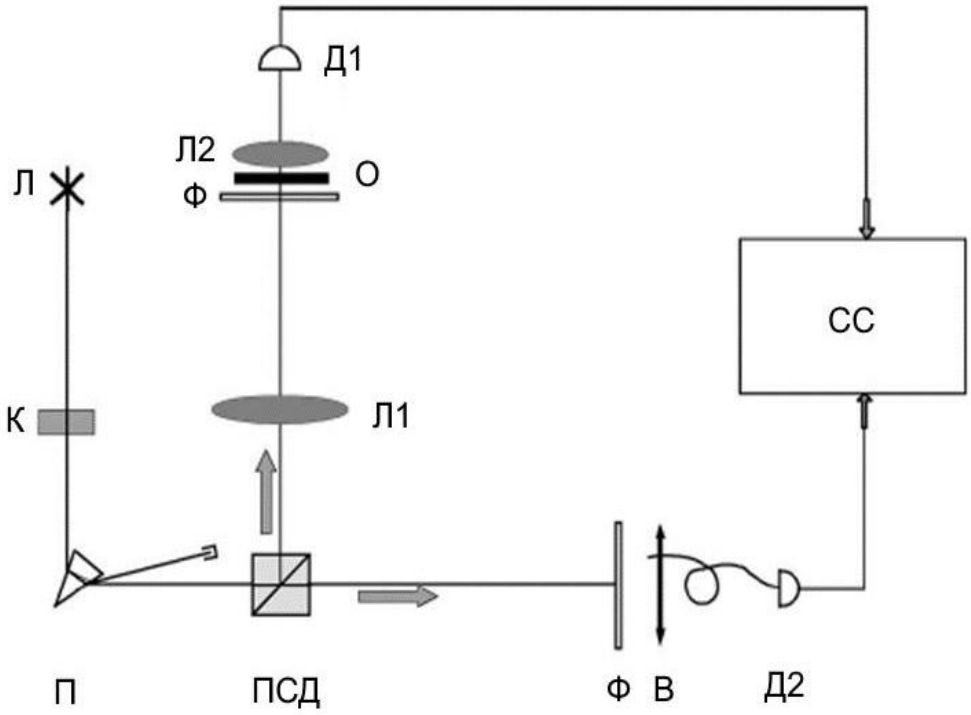


Рисунок 1 – Упрощённая схема получения фантомных изображений [1]: Л – источник лазерного излучения накачки; К – нелинейный кристалл с нелинейной восприимчивостью второго порядка; П – призма; ПСД – поляризационный светоделитель; Л1, Л2 – фокусирующие линзы; Ф – фильтр; О – исследуемый объект; В – оптическое волокно, при помощи которого производится сканирование в пространстве; Д1, Д2 – детекторы одиночных фотонов; СС – счётчик совпадений

Рассмотрев схему получения фантомных изображений на основе коррелированных фотонов (Рисунок 1), можно обнаружить, что построение изображений в такой схеме подчиняется уравнению тонкой линзы (Рисунок 2):

$$\frac{1}{S_i} + \frac{1}{S_o} = \frac{1}{f}, \qquad (1)$$

где S_o – от объекта до линзы, S_i – от линзы до изображения объекта, f' – фокусное расстояние линзы. Однако, чтобы это увидеть, придётся расположить элементы схемы как представлено на рисунке 2. В таком случае получается, что расстояние d_1 определяется как расстояние от линзы до кристалла и d_2 от кристалла до сканирующего детектора.

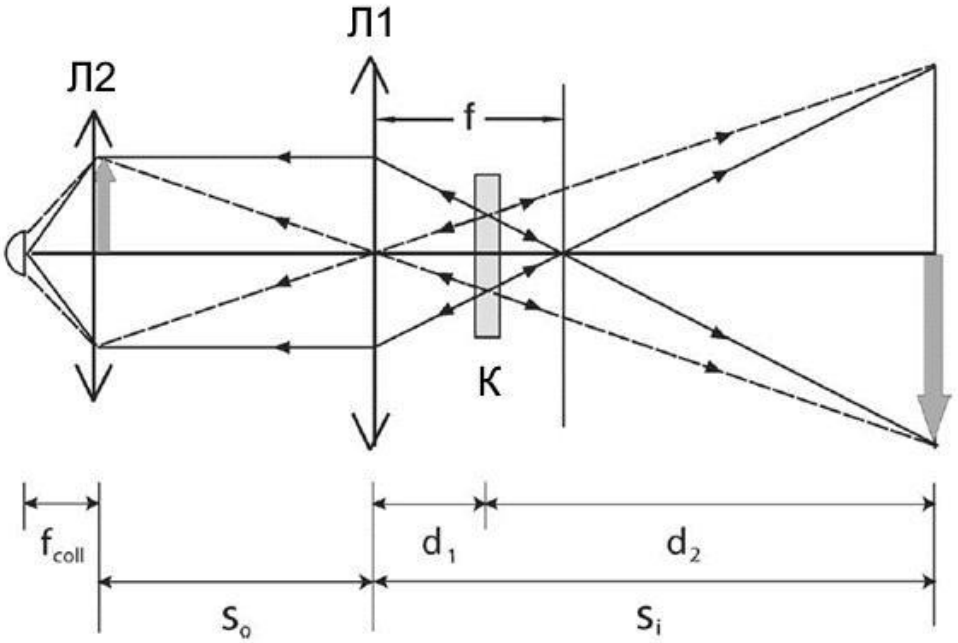


Рисунок 2 – Упрощённая схема получения фантомных изображений, демонстрирующая связь с уравнением для тонкой линзы [1]
К – нелинейный кристалл, S_o – расстояние от объекта до линзы, S_i – расстояние от линзы до изображения объекта, f' – фокусное расстояние линзы, f'_{coll} – фокусное расстояние коллективной линзы, d_1 – расстояние от линзы до кристалла, d_2 – от кристалла до сканирующего детектора

Как было сказано ранее, помимо корреляций, связанных с углом разлёта, для получения фантомных изображений можно использовать корреляции по частотам генерируемых фотонов. Это приведёт к дополнительному увеличению разрешения. В такой схеме в объектное плечо направляется длинноволновое излучение. А сканирование происходит для коротковолнового излучения [2].

Существует две точки зрения относительно того, можно ли считать технику получения фантомных изображений при помощи теплового излучения квантовой или классической. Сторонники классического подхода предполагают, что фантомные изображения получаются за счёт корреляции интенсивности спекл-структур, которые разделяются на светоделителе, что, несомненно, можно назвать классическим эффектом. Однако ряд экспериментов продемонстрировал, что данные корреляции возможно наблюдать при понижении интенсивности и работе в «однофотонном» режиме, что уже можно описать исключительно средствами квантовой оптики. При этом корреляции наблюдаются как для ближнепольного, так и для дальнепольного приближений [3].

Классическая схема получения фантомных изображений на основе псевдо-теплового излучения представлена на рисунке 3.

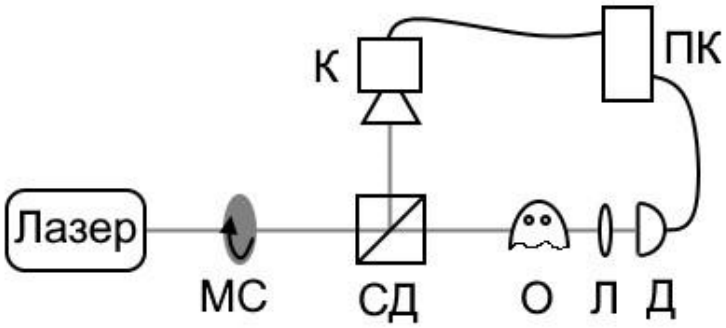


Рисунок 3 – Упрощённая схема генерации фантомных изображений на основе псевдотеплового источника [4]

Для получения псевдотеплового источника используется лазерное излучение, которое направляется на рассеивающую среду (МС). Полученное излучение направляется на светоделитель (СД). После прохождения светоделителя можно пронаблюдать, что спекл-структуры излучения идентичны, но интенсивность в каждом из каналов распределилась соответственно тому, на какое соотношение прошедших интенсивностей изготовлен светоделитель. Далее в одно из плеч устанавливается исследуемый объект (О) и неподвижный детектор (Д), на который фокусируется излучение при помощи короткофокусной линзы (Л). Во второе же плечо устанавливается камера (К), которая регистрирует распределение интенсивности в пространстве т.е. спекл-структуру.

Для восстановления изображения используется следующее выражение:

$$G(x,y) = \langle B \cdot I(x,y) \rangle - \langle B \rangle \cdot \langle I(x,y) \rangle \qquad (2),$$

где $I(x,y)$ – пространственное распределение интенсивности для спекл-структуры, B – интенсивность, регистрируемая на камерой (фотодиодом) после объекта. $\langle X \rangle$ – среднее арифметическое. Пользуясь выражением (2), возможно восстановить изображение объекта, не регистрируя данное изображение на камеру [4-6].

Описание экспериментальной установки

Лабораторная работа может быть представлена в двух вариантах.

Вариант I

В качестве источника лазерного излучения используется гелий-неоновый лазер с центральной длиной волны 632,8 нм. Излучение направляется на рассеивающую матовую среду (Р), после чего получаются спекл-структуры. Данная картина стационарна. Для получения фантомных изображений необходимо получить достаточное количество таких спекл-структур, чтобы изображение «проявилось». Для этого матовая поверхность установлена на подвижке, и её положение будет изменяться в процессе

измерений. Далее, при помощи щели (Д) выделяется небольшая часть рассеянного излучения, которое коллимируется при помощи линзы (Л). Далее излучение направляется на разбалансированный интерферометр Майкельсона, в одном из выходных каналов которого установлена камера. В отличие от «классической схемы», в данной лабораторной работе всё излучение будет направляться на камеру. Это необходимо для того, чтобы избавиться от необходимости временного согласования регистрирующего оборудования.

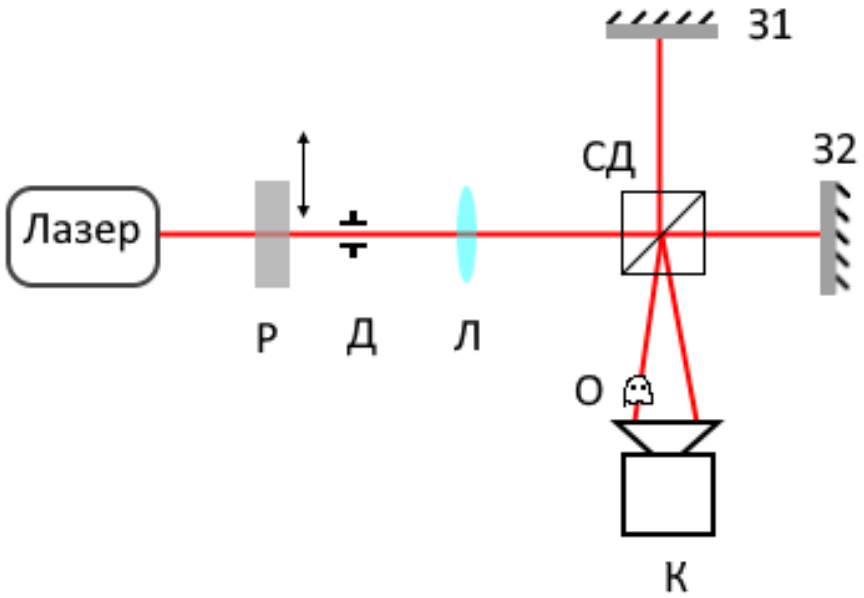


Рисунок 4 – Схема лабораторной установки вариант I
Р – рассеивающая матовая среда, Д – диафрагма, Л – плоско-выпуклая линза, СД – светоделитель, 31 и 32 – плоские зеркала, О – исследуемый объект, К – камера

Ход работы для Варианта I

1. Запустить лазер, ЭВМ, камеру.
2. Проверить, что пучки из сканирующего и объектного каналов попадают на камеру. В случае необходимости произвести юстировку.
3. Путём перемещения рассеивающей среды произвести порядка 500 измерений. Важно, чтобы спекл-структуры изменялись значительно.
4. Проверить полученные результаты, воспользовавшись приложением 1, в котором представлен код для MATLAB с комментариями. Разрешается написать свой код в любой удобной среде программирования, в данном случае необходимо поместить свой код в отчёт. Следует обратить внимание, что в зависимости от выбранного формата для сохранения распределения интенсивностей необходимо будет добавить часть кода, которая переводит формат изображения в числовую матрицу.

5. Обработать полученные результаты, воспользовавшись формулой (2). Для этого необходимо написать программу, в которой будет происходить пост-обработка полученных изображений.
6. Рассчитать соотношение сигнал-шум для восстановленного изображения. Для этого в восстановленной картине построить гистограмму распределения значений по интенсивности. В результате должно образоваться два пика. Первый будет соответствовать среднему значению шума, второй – среднему значению сигнала. Для получения соотношения сигнал-шум необходимо разделить среднее значение сигнала на среднее значение шума.
7. Подготовить отчёт.

Вариант II

В качестве источника спекл-картин будет использован проектор, который будет транслировать заранее подготовленные изображения спекл-картин. При помощи линзы (Л1) изображение спекл-картины коллимируется и направляется на исследуемый объект (О), далее прошедшее излучение собирается при помощи линзы (Л2) и регистрируется фотодиодом (ФД).

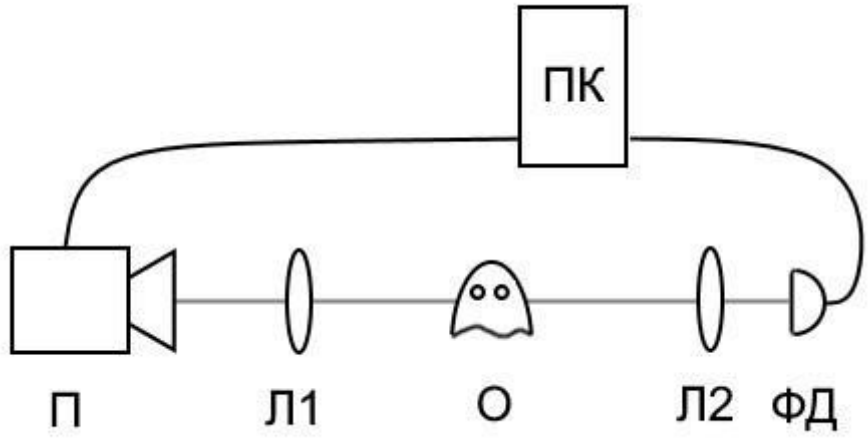


Рисунок 5 – Схема лабораторной установки вариант II
П – проектор, Л1, Л2 – фокусирующие линзы, О – исследуемый объект, ФД – фотодиод, ПК – компьютер.

Ход работы для Варианта II

1. Запустить проектор, ЭВМ.
2. Проверить, что излучение, проходящее через исследуемый объект, фокусируется на фотодиод.

3. Путём проецирования подготовленных спекл-картин произвести порядка 500 измерений интенсивности на фотодиоде.
4. Обработать полученные результаты, воспользовавшись формулой (2). Для этого необходимо написать программу, в которой будет происходить пост-обработка спекл-картин и соответствующих им измеренных интенсивностей.
5. Рассчитать соотношение сигнал-шум для восстановленного изображения. Для этого в восстановленной картине постройте гистограмму распределения значений по интенсивности. В результате должно образоваться два пика. Первый будет соответствовать среднему значению шума, второй – среднему значению сигнала. Для получения соотношения сигнал-шум необходимо разделить среднее значение сигнала на среднее значение шума.
6. Подготовить отчёт.

Содержание отчета

1. Описание процесса проведения лабораторной работы.
2. Результат проверки, вместе с использованной маской (маску можно выбрать самостоятельно).
3. Восстановленное изображение (если данное изображение не получилось восстановить, то попытаться обосновать причину).
4. Значения соотношений сигнал-шум для п. 4 и для п.5.
5. Выводы по проделанной работе.

Вопросы к защите

1. Дайте определение понятию спекл-структура.
2. За счёт вычисления какой функции происходит восстановление фантомного изображения?
3. Для каких источников существует возможность восстановления фантомных изображений? С чем это связано?
4. В «классической» схеме получения фантомных изображений используется однопиксельный детектор и камера, однако в проделанной лабораторной работе используется только фотодетектор. Поясните почему такая схема возможна.
6. Поясните на примере полученных результатов, что демонстрирует соотношение сигнал/шум.
7. Каким уравнением можно описать построение изображений для «квантовой» схемы?

8. Опишите схемы получения «классических» и «квантовых» фантомных изображений. Укажите основные различия и сходства между схемами.

Использованные источники литературы

1. Pittman T. B. et al. Optical imaging by means of two-photon quantum entanglement //Physical Review A. – 1995. – Т. 52. – №. 5. – С. R3429.
2. Karmakar S., Meyers R. E., Shih Y. Noninvasive high resolving power entangled photon quantum microscope //Journal of biomedical optics. – 2015. – Т. 20. – №. 1. – С. 016008.
3. Strekalov D. V. et al. Observation of two-photon “ghost” interference and diffraction //Physical review letters. – 1995. – Т. 74. – №. 18. – С. 3600.
4. Bromberg Y., Katz O., Silberberg Y. Ghost imaging with a single detector //Physical Review A. – 2009. – Т. 79. – №. 5. – С. 053840.
5. Ferri F. et al. High-resolution ghost image and ghost diffraction experiments with thermal light //Physical review letters. – 2005. – Т. 94. – №. 18. – С. 183602.
6. Shih Y. Quantum imaging //IEEE Journal of Selected Topics in Quantum Electronics. – 2007. – Т. 13. – №. 4. – С. 1016-1030.

Приложение 1

ПРИМЕР РЕАЛИЗАЦИИ КОДА ДЛЯ ПРОВЕРКИ ВОЗМОЖНОСТИ ИСПОЛЬЗОВАНИЯ ПОЛУЧЕННЫХ СПЕКЛОВ ДЛЯ ВОССТАНОВЛЕНИЯ ФАНТОМНОГО ИЗОБРАЖЕНИЯ

```
clc;
clear all;

Ia = zeros(x,a);
Ib= ones(x,b);
Ic = zeros(x,c);

Im = [Ia,Ib,Ic]';
```

Данные строки предназначены для формирования «виртуальной» маски

```
N = 300;
```

Число итераций должно соответствовать числу изображений, которые вы получили во время лабораторной работы.

```
IBs = zeros(x,y);
```

Создание пустого массива для суммирования произведения спекл-структур и интенсивностей в цикле

```
Bs = 0;
```

нулевое значение для суммирования полученных интенсивностей в цикле

```
Is = zeros(x,y);
```

Создание пустого массива для суммирования спекл-структур в цикле

```
for i = 1:N
```

Число итераций должно соответствовать числу изображений, которые вы получили во время лабораторной работы.

```
S = [num2str(i), 'название файла'];
```

В данной строке задаётся имя загружаемого в цикле файла. При это имя файла состоит из нескольких частей, например: 1_GI.txt. Соответственно вы составляете ваше название из двух частей. Первая – перевод числа вашего цикла в текстовый формат (num2str(i), в примере i=1). Вторая -_GI.txt, которую вы помещаете в ‘’.

```
Imag = load(s);
```

Загрузка файла, название которого было задано предыдущей строкой

```
I1 = Imag(x,y);
```

Поскольку в нашей лабораторной работе оба пучка направляются на камеру, нам необходимо вырезать ту часть, которая соответствует спекл-структуре.

Обратите внимание, что именно размерность (x,y), заданная здесь, должна влиять на остальные размерности матриц («виртуальной маски», пустых массивов).

Is = Is + I1;

Суммирование всех спекл-структур в цикле

B1 = sum(sum(I1. * Im));

Получение интенсивности путем поэлементного перемножения «виртуальной маски» и полученной спекл-структуры и суммирования всех элементов полученной матрицы.

Bs = Bs + B1;

Суммирование всех интенсивностей, полученных в цикле

IB1 = I1 * B1;

Перемножение интенсивности и соответствующей ей спекл-структуры

IBs = IB + IB1;

Суммирование произведений интенсивностей на спекл-структуры в цикле

end

IB = IBs / i;

Получение среднего значения произведений интенсивностей на спекл-структуры

B = Bs / i;

Определение среднего значения интенсивности

I = Is / i;

Определение среднего значения спекл-структуры

G = IB – B * I;

Восстановление фантомного изображения

mesh(G);

Построение фантомного изображения

Лабораторная работа №3

ИЗМЕРЕНИЕ ЗАВИСИМОСТИ ЧИСЛА ФОТОНОВ, ГЕНЕРИРУЕМЫХ В ПРОЦЕССЕ СПОНТАННОГО ПАРАМЕТРИЧЕСКОГО РАССЕЯНИЯ, ОТ ИНТЕНСИВНОСТИ ЛАЗЕРНОГО ИЗЛУЧЕНИЯ НАКАЧКИ (СПР)

Цель: формирование навыков работы с источником коррелированных фотонов.

Задачи, решаемые в работе

1. Изучить источник коррелированных фотонов на основе кристалла бета-бората бария с нелинейной восприимчивостью второго порядка, в котором реализуется I-тип синхронизма;
2. Изучить приборы регистрации одиночных фотонов на основе лавинных фотодиодов;
3. Провести юстировку схемы генерации коррелированных пар фотонов;
4. Зарегистрировать максимум излучения на счётчиках одиночных фотонов;
5. Получить зависимость числа зарегистрированных фотонов в каждом из каналов от мощности излучения.

Оборудование и материалы

Кристалл бета-бората бария, счётчики одиночных фотонов id120 (ID Quantique), время-цифровой преобразователь id800-TDC (ID Quantique), источник лазерного излучения LBX-375 (Oxxius).

Теоретические сведения

Существуют различные способы генерации коррелированных пар фотонов. Среди них наибольшее распространение получили следующие: спонтанное параметрическое рассеяние (СПР), четырёхволновое смешение (ЧВС), генерация коррелированных фотонов в полупроводниках. На данный момент наиболее распространённым методом генерации коррелированных фотонов можно назвать СПР. Впервые процесс СПР был теоретически описан Давидом Николаевичем Клышко (1966 г.). Спустя всего один год, независимо друг от друга, тремя группами были поставлены эксперименты по реализации процесса СПР в нелинейных средах с нелинейной восприимчивостью второго порядка. Основными рабочими уравнениями для СПР можно назвать условие фазового синхронизма [1]: $\vec{k}_p = \vec{k}_s + \vec{k}_i$, в котором $\vec{k}_p$, $\vec{k}_s$, $\vec{k}_i$ являются волновыми векторами для основной, сигнальной и холостой волн соответственно, и условия баланса частот излучения, участвующего во взаимодействии, которое, по сути, не что иное, как закон сохранения энергии:

$\omega_p = \omega_s + \omega_i$. Процесс СПР можно описать как аннигиляцию одного фотона накачки и рождения двух фотонов, которые называются сигнальным и холостым фотоном. Стоит отметить, что данный процесс невозможен с точки зрения нелинейной оптики в отсутствие затравочного излучения, на котором будет происходить генерации. Это противоречит экспериментальным данным, и в этом плане квантовая теория даёт более точное описание этому процессу. Условия СПР могут выполняться в нелинейных оптических средах с нелинейной восприимчивостью второго порядка. В общем случае условия фазового синхронизма выполнить невозможно, но существует несколько частных способов его реализации [2]. Так, в одноосных и двуосных кристаллах можно подобрать такое направление, при котором условия синхронизма будут выполняться для вырожденного случая (такого, при котором длина волн генерируемого излучения будет равна удвоенной длине волны накачки) для различных поляризаций излучения. Другим способом реализации условий синхронизма является компенсация разности между значениями волновых векторов (фазовой расстройки), вектором обратной решётки в нелинейных фотонных кристаллах (НФК). Выделяют три типа синхронизма: 0, I и II. При 0-типе поляризации волн, участвующих во взаимодействии, одинаковы, такой случай реализуется в НФК. В случае I-типа между собой ортогональны поляризация накачки и генерируемого (сигнального и холостого) излучения, поляризации которых лежат в одной плоскости. В случае II-типа синхронизма поляризации сигнального и холостого излучения взаимно перпендикулярны.

Фотоны могут коррелировать по времени и месту рождения, поляризации, углу разлёта и энергии [3]. Наиболее примечательным квантовым свойством коррелированных фотонов является группировка при прохождении светоделителя. В общем случае фотоны, попадая на светоделитель, проходят его независимо друг от друга. Коррелированные же фотоны при прохождении светоделителя при одновременном попадании на него начинают распространяться совместно [4].

Описание рабочей установки

В качестве источника излучения накачки будет выступать лазер LBX-375 (Л) с центральной длиной волны 375 нм, поляризация данного лазера является горизонтальной. В качестве нелинейной среды, в которой будет реализовываться СПР, будет использован отрицательный одноосный кристалл бета-бората бария (BBO). Кристалл вырезан под углом thet= 29,0°. Это гарантирует выполнение условий синхронизма для реализации вырожденного случая СПР при накачке, равной 400 нм, и генерации излучения на длине волны, равной 800 нм. В то же время, вследствие зависимости показателя преломления, а как следствие и волнового вектора, от угла поворота кристалла, кристалл можно расположить таким способом, чтобы в нём реализовывались условия синхронизма для генерации излучения на длине волны 750 нм при накачке на 375 нм. При этом предполагается, что фотоны

будут распространяться под углом относительно излучения накачки, образуя конус, при этом коррелированные фотоны будут находиться на противоположных сторонах конуса (Рисунок 1).

Излучение накачки будет регистрироваться счётчиками одиночных фотонов (Д1 и Д2), с квантовой эффективностью порядка 80% на длине волны регистрации. Мёртвое время счётчиков составляет 1 мкс. Счётчики соединены с время-цифровым преобразователем (СС), временное разрешение которого составляет 89 пкс (Рисунок 2).

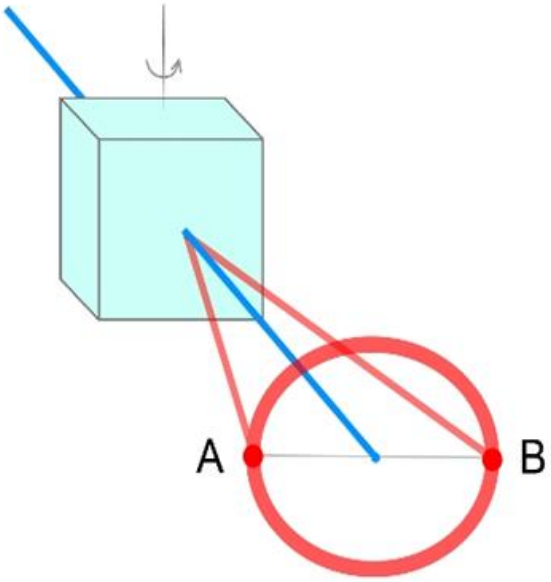


Рисунок 1 – Схема разлёта фотонов при СПР I-типа.
Точками A и B обозначены противоположные стороны конуса, в которых находятся коррелированные фотоны

Ход работы

1. Провести юстировку схемы, используя дополнительный лазер, зеркало и светоделитель. Зеркало и светоделитель выставить таким образом, чтобы лазерный луч, отражённый от передней грани светоделителя пересекался с лучом, отражённым от зеркала. Точка пересечения должна находиться на передней грани кристалла BBO и совпадать с точкой излучения накачки.
2. Вращая микрометрические винты зеркал (З4 и З5), направить излучение юстировочного лазера на счётчики одиночных фотонов.
3. Отключить юстировочный лазер.
4. Выставить мощность лазерного излучения накачки на 20мВт. Убедиться, что излучение проходит через диафрагмы и попадает на зеркала (З2 и З3), кристалл бета-бората бария (BBO).
5. Вращая микрометрические винты зеркал (З4 и З5), получить максимум регистрируемых событий.

6. Провести измерения зависимости числа отсчётов в каждом из каналов в диапазоне от 0 до 50 мВт с шагом в 5 мВт.
7. Построить зависимости.

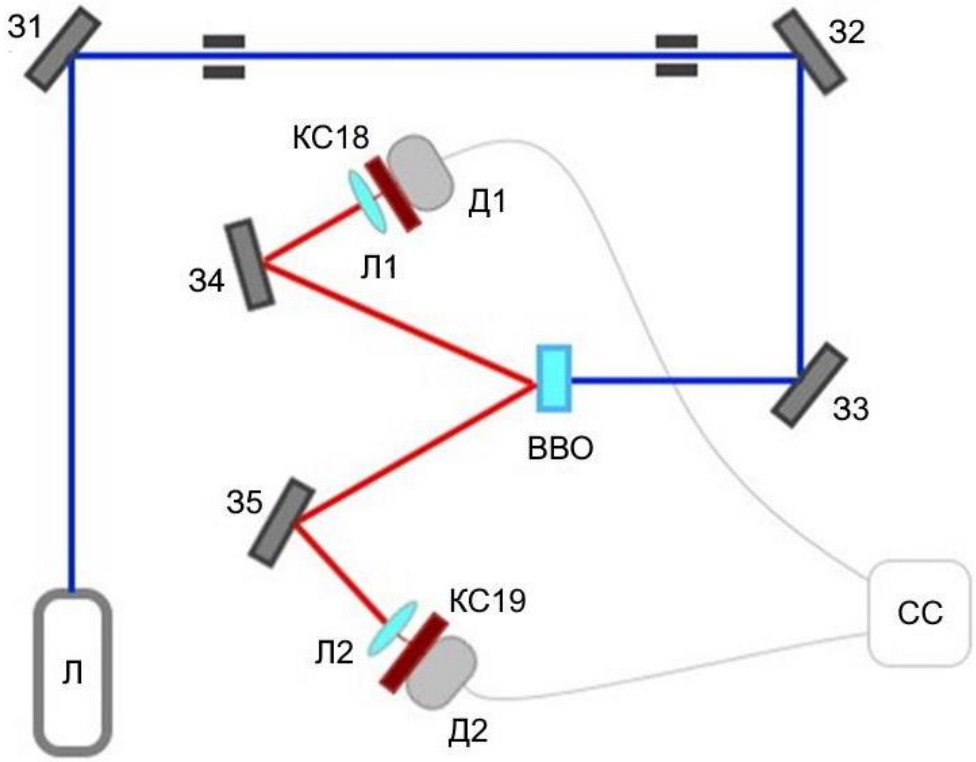


Рисунок 2 – схема экспериментальной установки
Л – источник лазерного излучения, З1, З2, З3, З4, З5 – плоское зеркало, КС18, КС19 – оптический фильтр , Л1, Л2 – линза, Д1, Д2 – детектор одиночных фотонов, ВВО – кристалл бета-бората бария (либо иодата лития)

Содержание отчета

1. Краткий пересказ теории, в котором отражены основные моменты работы схемы генерации СПР-излучения, и ответы на вопросы (не обязательно списком).
2. График зависимости числа зарегистрированных отсчётов от мощности лазерного излучения накачки.
3. На графике необходимо выделить линейный участок, для которого при помощи метода наименьших квадратов (МНК), рассчитать коэффициент корреляции (важно не путать корреляции фотонов и данный коэффициент корреляции, который демонстрирует коэффициент, насколько ваша зависимость соответствует линейной).
4. Привести вид прямой, полученной при помощи использования МНК, на графике с измеренными данными.

Вопросы к защите

1. Запишите условие фазового синхронизма и уравнение баланса частот. Как данные условия выполняются при постановке эксперимента?
2. Перечислите и сопоставьте корреляционные свойства фотонов, которые определяются данными уравнениями. Какие из перечисленных видов корреляций мы могли наблюдать в проделанном эксперименте?
3. По каким параметрам разделяют условия синхронизма? Перечислите типы синхронизма. В чём заключается различие типов синхронизма? В чём принципиальное отличие вырожденного случая синхронизма от невырожденного?
4. При решении связанных дифференциальных уравнений для случая СПР возникает необходимость условия, которое не требуется при использовании квантовой теории, что это за условие?
5. Перечислите источники оптических потерь, которые могут возникнуть в экспериментальной установке (обратите внимание, что нас интересуют только потери, связанные с генерируемым излучением). Объясните разницу между полученными значениями в каналах.
6. Выполнение какого условия позволяет нам сделать вывод, что мы работаем в режиме СПР?
7. Первоначальная юстировка установки производится при помощи дополнительного лазера. С чем это связано?
8. В каких целях могут быть использованы коррелированные фотоны? Перечислите известные схемы и их применение (подготовить схематические изображения, например, скрин из статьи, и уметь рассказать об основных элементах)

Использованные источники литературы

1. Самарцев В. В. Коррелированные фотоны и их применение. — М.: ФИЗМАТЛИТ, 2014. — 168 с. — ISBN 978-5-9221-1511-7.
2. Нелинейно-оптические кристаллы. Свойства и применение в квантовой электронике: Справочник/Г. Г. Гурзадян, В. Г. Дмитриев, Д. Н. Никогосян. — М.: Радио и связь, 1991.— 160 с: ил. ISBN 5-256-00859-5.
3. Shih Y. Entangled biphoton source-property and preparation //Reports on Progress in Physics. – 2003. – Т. 66. – №. 6. – С. 1009.
4. Couteau C. Spontaneous parametric down-conversion //Contemporary Physics. – 2018. – Т. 59. – №. 3. – С. 291-304.

Виртуальная лабораторная работа №4

МОДЕЛИРОВАНИЕ ПРОЦЕССА СПОНТАННОГО ПАРАМЕТРИЧЕСКОГО РАССЕЯНИЯ СВЕТА

Цель: моделирование процесса спонтанного параметрического рассеяния для различных условий синхронизма.

Задачи, решаемые в работе

1. Изучение зависимости угла разлета сигнального и холостого излучения при выходе из кристалла от фазовой расстройки
2. Изучение условий синхронизма генерируемого излучения для I и II типов синхронизма

Теоретические сведения

Явление спонтанного параметрического рассеяния (СПР) света представляет собой оптический параметрический процесс спонтанного распада фотонов падающего на среду монохроматического излучения (называемого «накачкой») с несущей частотой ω_p на пары фотонов — сигнальный (ω_s) и холостой (ω_i), в условиях выполнения законов сохранения энергии (1.1) и импульса (1.2) [1]. Данные условия были названы условиями фазового синхронизма, которые можно представить в следующем виде:

$$\hbar\omega_p = \hbar\omega_s + \hbar\omega_i, \quad (1)$$

$$\vec{k}_p = \vec{k}_s + \vec{k}_i, \quad (2)$$

где $\hbar$ – постоянная Планка, $\omega = \frac{c}{\lambda}$ – частота излучения, c – скорость света в вакууме, λ – длина волны излучения, $k = \frac{2\pi n}{\lambda}$ – волновой вектор, n – показатель преломления, p, s, i – фотоны накачки, сигнала и холостого соответственно.

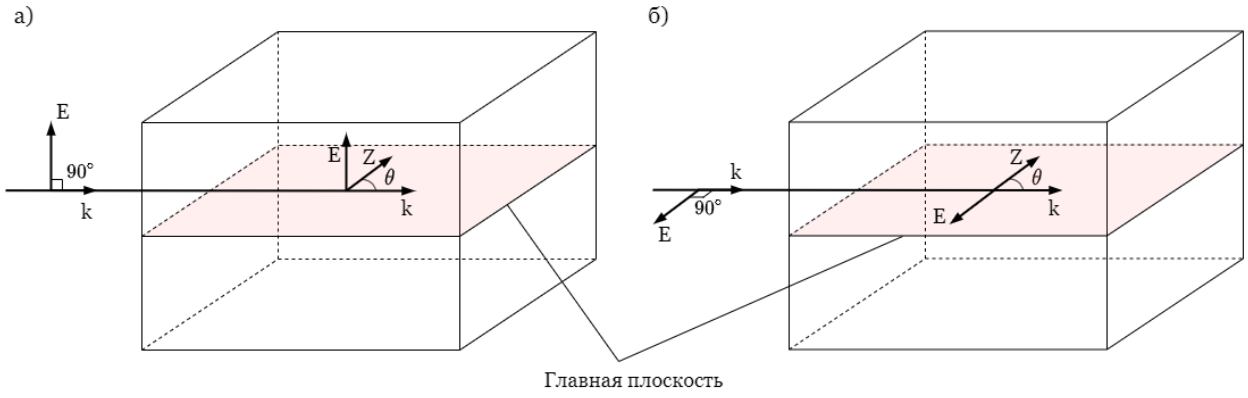


Рисунок 1 Главная плоскость кристалла и обыкновенный луч (а), необыкновенный луч (б)

Для выполнения условия фазового синхронизма необходимо использование среды с квадратичной нелинейностью (например, кристаллы $LiIO_3, LiNbO_3, BBO, KTP$). Другими словами, процесс СПР возможен только в анизотропных кристаллах для волн с различной поляризацией. Таким образом, выделяют два типа синхронизма:

1) **первый тип** синхронизма имеет место при одинаковой поляризации сигнального и холостого фотона, отличной от фотона накачки

$$\vec{k}_p^e = \vec{k}_s^o + \vec{k}_i^o \quad \left(\vec{k}_p^o = \vec{k}_s^e + \vec{k}_i^e\right), \tag{3}$$

2) **второй тип** синхронизма реализуется при различной поляризации сигнального и холостого фотонов

$$\vec{k}_p^e = \vec{k}_s^{e\,(o)} + \vec{k}_i^{o\,(e)} \quad \left(\vec{k}_p^o = \vec{k}_s^{o\,(e)} + \vec{k}_i^{e\,(o)}\right), \tag{4}$$

где o – обыкновенный луч, поляризация которого перпендикулярна главной плоскости кристалла, а e – необыкновенный луч, поляризация которого лежит в главной плоскости кристалла, как показано на Рисунке 1. Первое уравнение принадлежит к отрицательным кристаллам, а второе, в круглых скобках, к положительным. Важно учитывать, что показатель преломления обыкновенного луча не зависит от направления распространения в нелинейном кристалле, тогда как для необыкновенного луча, наоборот, зависит от угла между направлением распространения и главной оптической и рассчитывается следующим образом [2]:

$$n_e^{eff}(\lambda, \theta) = \left[\frac{cos^2(\theta)}{n_o^2(\lambda)} + \frac{sin^2(\theta)}{n_e^2(\lambda)}\right]^{-\frac{1}{2}}, \tag{5}$$

где n_e^{eff} – эффективный показатель преломления необыкновенного луча, 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 $n_e^{eff}(\lambda, 90°) = n_e$). Стоит учесть, что показатели преломления рассчитываются индивидуально для каждого кристалла (формулы для расчета приведены в источнике [2]).

Таким образом, в данной работе необходимо рассчитать условия синхронизма для каждого типа в двумерном и трехмерном пространстве для различных видов нелинейных кристаллов, используемых для генерации СПР.

I тип синхронизма на плоскости

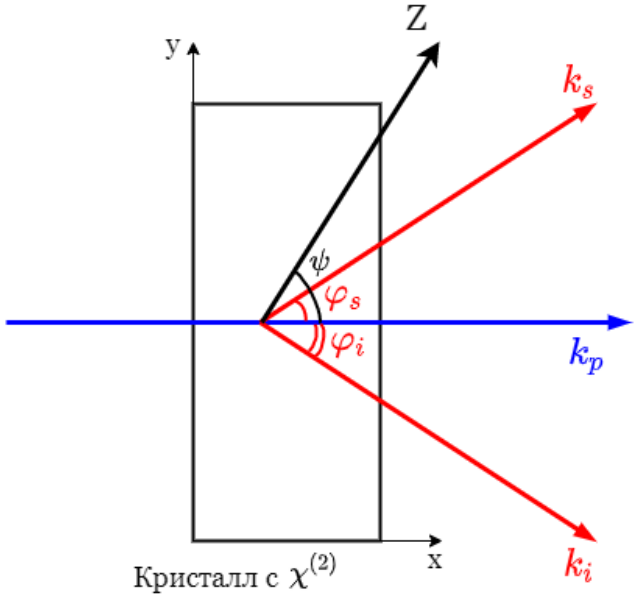


Рисунок 2 Процесс СПР I типа на плоскости (вид сверху)

Рассмотрим условия фазового синхронизма первого типа для неколлинеарного вырожденного случая (волновые вектора сигнального и холостого фотонов не параллельны лучу накачке и $\lambda = \lambda_s = \lambda_i$), считая, что луч накачки перпендикуляр плоскости кристалла (то есть $\theta = \psi$, где ψ – угол, под которым вырезан кристалл)

$$\vec{k}_p^e(\lambda_p, \psi) = \vec{k}_s^o(\lambda_s) + \vec{k}_i^o(\lambda_i). \quad (6)$$

Спроецировав данное выражение на координатные оси, получим систему уравнений следующего вида:

$$\begin{cases} k_p^e(\lambda_p, \psi) = k_s^o(\lambda_s)\, cos(\varphi_s) + k_i^o(\lambda_i)\, cos(\varphi_i) \\ k_s^o(\lambda_s)\, sin(\varphi_s) = k_i^o(\lambda_i)\, sin(\varphi_i) \end{cases}, \quad (7)$$

где φ – угол между направлением распространением сгенерированного фотона и нормали кристалла. Решая данную систему уравнений при заданных условиях, можно показать, что

$$k^o(\lambda) = k_s^o(\lambda_s) = k_i^o(\lambda_i) = \frac{2\pi n_0(\lambda)}{\lambda}. \quad (8)$$

$$\varphi = \varphi_s = \varphi_i = arccos\left(\frac{k_p^e(\lambda_p, \psi)}{2k^o(\lambda)}\right). \quad (9)$$

Однако следует помнить, что данный угол разлета фотонов рассчитан при условии их распространения в объеме нелинейного кристалла и будет отклонятся от первоначальной траектории при выходе сгенерированного излучения вследствие преломления света. Используя закон Снеллиуса, можно рассчитать угол разлета фотонов при выходе из кристалла

$$\varphi' = \varphi_s' = \varphi_i' = \arcsin\big(n_0(\lambda)\, sin(\varphi)\big), \quad (10)$$

где φ' – угол между направлением распространением сгенерированного фотона при выходе из кристалла и нормали к нему.

Для определения углов разлета сгенерированных пар фотонов при заданном угле выреза кристалла удобно использовать формулу фазовой расстройки

$$\Delta k = k_p^e(\lambda_p, \psi) - 2k^o(\lambda)\, cos(\varphi). \quad (11)$$

Таким образом, картина интенсивности сгенерированной пары фотонов в пространстве определяется следующим выражением:

$$r = sinc^2(\Delta k \cdot p), \quad (12)$$

где r – некая точка в пространстве, $sinc$ – кардинальный синус, p – безразмерный коэффициент, отвечающий за «толщину» генерируемого кольца (в данной работе принять равным порядка $5 \cdot 10^{-5}$).

I тип синхронизма в объеме

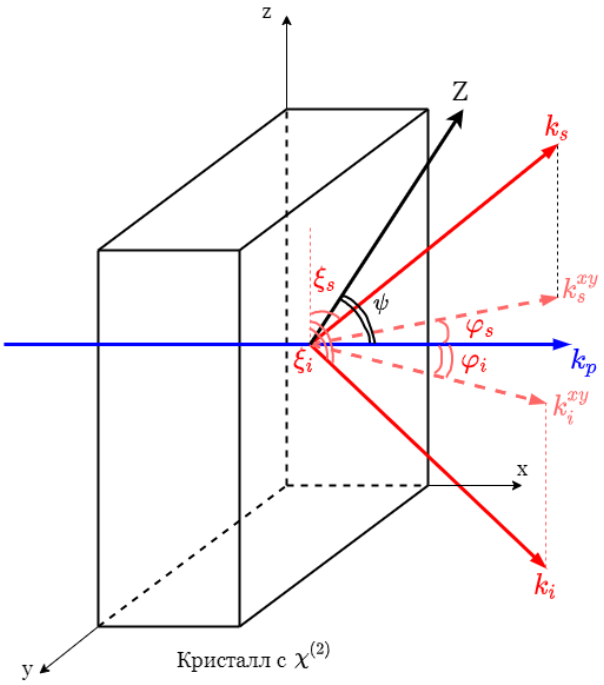


Рисунок 3 Процесс СПР I типа в объеме

При рассмотрении первого типа в объеме условия фазового синхронизма останутся неизменны, однако при его проецировании на координатные оси система будет иметь более сложный вид

$$\begin{cases} k_p^e(\lambda_p, \psi) = k_s^o(\lambda_s)\cos(\varphi_s)\, cos(\xi_s) + k_i^o(\lambda_i)\, cos(\varphi_i)\, cos(\xi_i) \\ k_s^o(\lambda_s)\, sin(\varphi_s)\, cos(\xi_s) = k_i^o(\lambda_i)\, sin(\varphi_i)\, cos(\xi_i) \\ k_s^o(\lambda_s)\, sin(\xi_s) = k_i^o(\lambda_i)\, sin(\xi_i) \end{cases}. \quad (13)$$

Решая данную систему уравнений, можно получить следующие соотношения, аналогичные синхронизму на плоскости:

$$\begin{cases} k^o(\lambda) = k_s^o(\lambda_s) = k_i^o(\lambda_i) = \frac{2\pi n_0(\lambda)}{\lambda} \\ \xi = \xi_s = \xi_i \\ \varphi = \varphi_s = \varphi_i \end{cases}. \quad (14)$$

В этом случае также не стоит забывать про закон Снеллиуса, который определяет углы разлета фотонов при выходе излучения из кристалла

$$\begin{cases} \varphi' = \arcsin\big(n_0(\lambda)\, sin(\varphi)\big) \\ \xi' = \arcsin\big(n_0(\lambda)\, sin(\xi)\big) \end{cases}, \quad (15)$$

В заключение запишем уравнение фазовой расстройки для первого типа синхронизма в объеме

$$\Delta k = k_p^e\big(\lambda_p, \psi\big) - 2k^o(\lambda)\, cos(\varphi)\, cos(\xi) \quad (16)$$

Кольцо СПР можно получить с помощью выражения (12), подставив в него «объемную» фазовую расстройку, полученную выше. Важно понимать, что полученная картина будет представлять собой два наложенных кольца – одно сигнальное, другое холостое. При более полном описании следовало рассматривать полученные выражения независимо для углов сигнального и холостого лучей, однако, вследствие их равенства, в текущей и предыдущей главе они были рассмотрены совместно.

II тип синхронизма на плоскости

Теперь рассмотрим условия фазового синхронизма второго типа на плоскости для неколлинеарного случая с равенством длин волн сигнального и холостого лучей ($\lambda_s = \lambda_i$), также считая, что луч накачки, перпендикуляр плоскости кристалла ($\theta = \psi$ для луча накачки)

$$\vec{k}_p^e\big(\lambda_p, \psi\big) = \vec{k}_s^o(\lambda_s) + \vec{k}_i^e(\lambda_i, \theta). \quad (17)$$

Важным отличием второго типа синхронизма от первого является то, что один из лучей распространяется по необыкновенной траектории (далее будем считать, что по необыкновенной траектории распространяется холостой луч). Это означает, что при втором типе синхронизма модули волновых векторов сигнального и холостого пучков окажутся не равными друг другу $\big(k_s^o(\lambda_s) \neq k_i^e(\lambda_i, \theta)\big)$, в отличие от первого типа. Таким образом, уравнения фазовой расстройки должны быть рассмотрены отдельно для сигнального и холостого излучения.

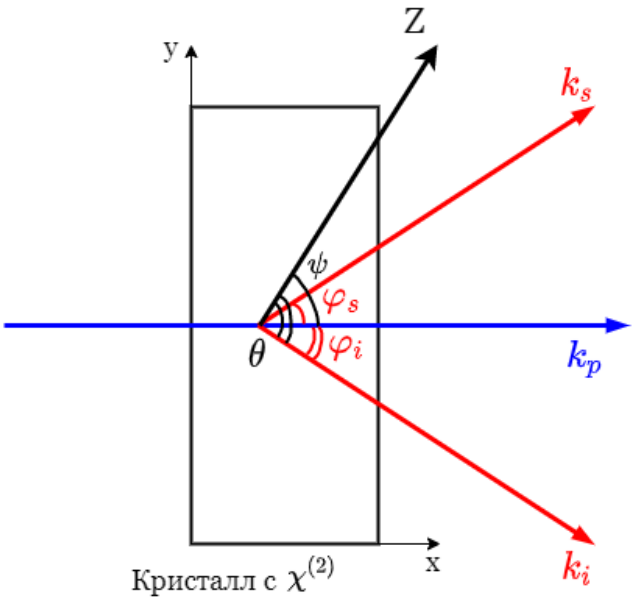


Рисунок 4 Процесс СПР II типа на плоскости (вид сверху)

Как и для первого типа синхронизма, спроецируем выражение (17) на координатные оси:

$$\begin{cases} k_p^e(\lambda_p, \psi) = k_s^o(\lambda_s)\, cos(\varphi_s) + k_i^e(\lambda_i, \theta)\, cos(\varphi_i) \\ k_s^o(\lambda_s)\, sin(\varphi_s) = k_i^e(\lambda_i, \theta)\, sin(\varphi_i) \end{cases}, \quad (18)$$

где $\theta = \psi - \varphi_i$ – угол между оптической осью кристалла и холостым пучком излучения.

Решим данную систему уравнений отдельно для сигнального и холостого пучков излучения, однако вначале необходимо определить зависимость между углами φ_s и φ_i для расчета угла θ в обоих случаях (если этого не сделать, выражение (21) решить будет нельзя, так как искомый угол будет в обоих частях выражения). Для этого необходимо выразить волновой вектор холостого пучка из первого уравнения и подставить его во второе. Таким образом, получаем

$$\varphi_i = arctg\left(\frac{k_s^o(\lambda_s)\, sin(\varphi_s)}{k_p^e(\lambda_p, \psi) - k_s^o(\lambda_s)\, cos(\varphi_s)}\right). \quad (19)$$

Следовательно, из второго уравнения получаем

$$\varphi_s = arcsin\left(\frac{k_i^e(\lambda_i, \theta)\, sin(\varphi_i)}{k_s^o(\lambda_s)}\right), \quad (20)$$

$$\varphi_i = arcsin\left(\frac{k_s^o(\lambda_s)\, sin(\varphi_s)}{k_i^e(\lambda_i, \theta)}\right), \quad (21)$$

Применив закон Снеллиуса (выражение (10)), получим углы при выходе из кристалла.

Для решения уравнения фазовой расстройки необходимо выразить косинусы углов сигнального и холостого пучков через друг друга

$$cos(\varphi_s) = \sqrt{1 - sin^2(\varphi_s)} = \sqrt{1 - \left(\frac{k_i^e(\lambda_i,\theta)\, sin(\varphi_i)}{k_s^o(\lambda_s)}\right)^2}, \qquad (22)$$

$$cos(\varphi_i) = \sqrt{1 - sin^2(\varphi_i)} = \sqrt{1 - \left(\frac{k_s^o(\lambda_s)\, sin(\varphi_s)}{k_i^e(\lambda_i,\theta)}\right)^2}. \qquad (23)$$

Далее, использовав уравнения фазовой расстройки

$$\Delta k = k_p^e(\lambda_p, \psi) - k_s^o(\lambda_s)\, cos(\varphi_s) - k_i^e(\lambda_i, \theta)\, cos(\varphi_i) \qquad (24)$$

относительно одного из углов (сигнального или холостого) и применив выражение (12), можно получить картину разлета фотонов на плоскости отдельно для сигнального и холостого кольца.

II тип синхронизма в объеме

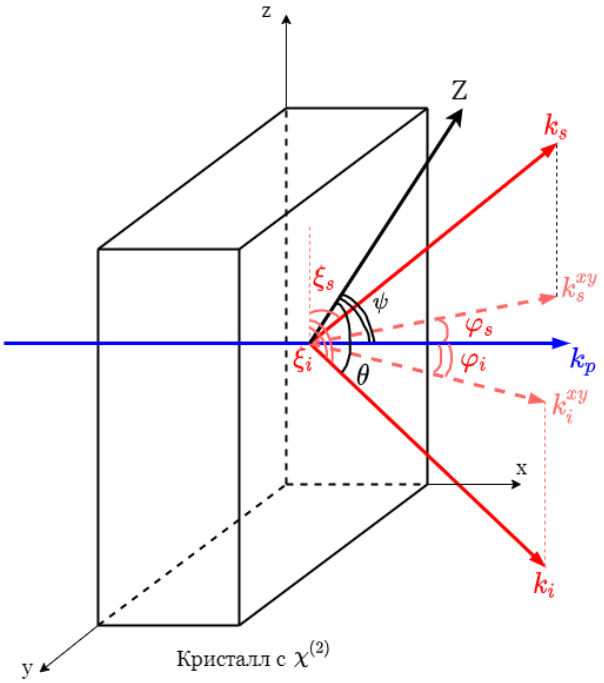


Рисунок 5 Процесс СПР II типа в объеме

Последним шагом рассмотрим фазовый синхронизм второго типа в объеме для неколлинеарного случая с равенством длин волн сигнального и холостого луча ($\lambda_s = \lambda_i$). Будем следовать привычным шагам. Помня условия синхронизма для второго типа (выражение (17)), спроецируем его на координатные оси:

$$\begin{cases} k_p^e(\lambda_p, \psi) = k_s^o(\lambda_s)\, \cos(\varphi_s)\, cos(\xi_s) + k_i^e(\lambda_i, \theta)\, cos(\varphi_i)\, cos(\xi_i) \\ k_s^o(\lambda_s)\, sin(\varphi_s)\, cos(\xi_s) = k_i^e(\lambda_i, \theta)\, sin(\varphi_i)\, cos(\xi_i) \\ k_s^o(\lambda_s)\, sin(\xi_s) = k_i^e(\lambda_i, \theta)\, sin(\xi_i) \end{cases}. \qquad (25)$$

Далее выразим соответствующие углы друг через друга, помня про выражение (19). Таким образом, для углов сигнального пучка получим

$$cos(\xi_s) = \sqrt{1 - sin^2(\xi_s)} = \sqrt{1 - \left(\frac{k_i^e(\lambda_i,\theta)\, sin(\xi_i)}{k_s^o(\lambda_s)}\right)^2}, \quad (26)$$

$$\cos(\varphi_s) = \sqrt{1 - sin^2(\varphi_s)} = \sqrt{1 - \left(\frac{k_i^e(\lambda_i,\theta)\, sin(\varphi_i)\, cos(\xi_i)}{k_s^o(\lambda_s)\, cos(\xi_s)}\right)^2}, \quad (27)$$

а для углов холостого пучка получим следующее:

$$cos(\xi_i) = \sqrt{1 - sin^2(\xi_i)} = \sqrt{1 - \left(\frac{k_s^o(\lambda_s)\, sin(\xi_s)}{k_i^e(\lambda_i,\theta)}\right)^2}, \quad (28)$$

$$\cos(\varphi_i) = \sqrt{1 - sin^2(\varphi_i)} = \sqrt{1 - \left(\frac{k_s^o(\lambda_s)\, sin(\varphi_s)\, cos(\xi_s)}{k_i^e(\lambda_i,\theta)\, cos(\xi_i)}\right)^2}. \quad (29)$$

В заключение, воспользовавшись уравнением фазовой расстройки

$$\Delta k = k_p^e(\lambda_p, \psi) - k_s^o(\lambda_s)\cos(\varphi_s)\, cos(\xi_s) - k_i^e(\lambda_i,\theta)\, cos(\varphi_i)\, cos(\xi_i) \quad (30)$$

и выражением (12), можно рассчитать кольца СПР для второго типа синхронизма.

Частотно-угловой спектр

В заключение рассмотрим частотно угловой спектр СПР. Под этим понятием будем понимать зависимость вероятности СПР от частоты и направления испускания фотонов. Он определяется следующим выражением, вывод которого выходит за рамки данного методического описания и приведен в [3]:

$$N_q(\omega) = \left(\frac{\chi^{(2)} L E_0}{4c}\right)^2 \frac{\omega}{n_i(\omega)} \frac{\omega_p - \omega}{n_s(\omega_p - \omega)}\, sinc^2\left(\Delta k \cdot \frac{L}{2}\right), \quad (31)$$

где $\chi^{(2)}$ – квадратичная восприимчивость или нелинейность (пропорциональна эффективной нелинейности кристалла), L – длина нелинейного кристалла, E_0 – амплитуда электрического поля волны накачки (в данной работе принять равной 1), n_i и n_s – показатели преломления холостого и сигнального лучей (совпадают с обыкновенными и необыкновенными показателями преломления).

Ход работы

Варианты для каждого задания выдаются в индивидуальном порядке преподавателем. Параметры используемых в расчетах кристаллов приведены в конце.

1) Построить зависимость фазовой растройки от угла разлета сигнального и холостого пучков излучения при выходе из кристалла.
2) Получить «кольцо» СПР в объеме при выходе излучения из кристалла для I-типа синхронизма.
3) Получить «кольцо» СПР в объеме внутри кристалла и при выходе излучения из него для II-типа синхронизма.
4) Построить частотно угловой спектр.

Параметры кристаллов [4]

BBO

Дисперсионные зависимости (длина волны указана в мкм):

$$n_o^2 = 2.7405 + \frac{0.0184}{\lambda^2 - 0.0179} - 0.0155 \cdot \lambda^2$$

$$n_e^2 = 2.3730 + \frac{0.0128}{\lambda^2 - 0.0156} - 0.0044 \cdot \lambda^2$$

Эффективная нелинейность:

$$d_{eoo} = 0.12 \cdot 10^{-12} \cdot sin(\theta) - 1.78 \cdot 10^{-12} \cdot cos(\theta)\, sin(3\varphi)$$

$LiIO_3$

Дисперсионные зависимости (длина волны указана в мкм):

$$n_o^2 = 3.415716 + \frac{0.047031}{\lambda^2 - 0.035306} - 0.008801 \cdot \lambda^2$$

$$n_e^2 = 2.918692 + \frac{0.035145}{\lambda^2 - 0.028224} - 0.003641 \cdot \lambda^2$$

Эффективная нелинейность:

$$d_{eoo} = 5.53 \cdot 10^{-12} \cdot sin(\theta)$$

$LiNbO_3$

Дисперсионные зависимости (длина волны указана в мкм):

$$n_o^2 = 4.9130 + \frac{0.1173 + 1.65 \cdot 10^{-8} \cdot T^2}{\lambda^2 - (0.212 + 2.7 \cdot 10^{-8} \cdot T^2)^2} - 2.78 \cdot 10^{-2} \cdot \lambda^2$$

$$n_e^2 = 4.5567 + 2.605 \cdot 10^{-7} \cdot T^2 + \frac{0.097 + 2.7 \cdot 10^{-8} \cdot T^2}{\lambda^2 - (0.201 + 5.4 \cdot 10^{-8} \cdot T^2)^2} - 2.24 \cdot 10^{-2} \cdot \lambda^2$$

Эффективная нелинейность:

$$d_{eoo} = 5.44 \cdot 10^{-12} \cdot sin(\theta) - 2.76 \cdot 10^{-12} \cdot cos(\theta)\, sin(3\varphi)$$

Содержание отчета

1. В зависимости от варианта, выданного преподавателем, поместить в отчёт:
   а) зависимость угла разлета сигнального и холостого пучков излучения при выходе из кристалла от фазовой расстройки
   б) «кольцо» СПР в объеме при выходе излучения из кристалла для I-типа синхронизма.
   в) «кольцо» СПР в объеме внутри кристалла и при выходе излучения из него для второго типа синхронизма.
   г) Построить частотно-угловой спектр
2. При подготовке отчёта, поместите код программы на отдельную страницу с подписью: «**ПРИЛОЖЕНИЕ А**».

Использованные источники литературы

1. Couteau C. Spontaneous parametric down-conversion //Contemporary Physics. – 2018. – Т. 59. – №. 3. – С. 291-304.
2. Shih Y. Entangled biphoton source-property and preparation //Reports on Progress in Physics. – 2003. – Т. 66. – №. 6. – С. 1009.
3. Самарцев В. В. Коррелированные фотоны и их применение. — М.: ФИЗМАТЛИТ, 2014. — 168 с. — ISBN 978-5-9221-1511-7.
4. Нелинейно-оптические кристаллы. Свойства и применение в квантовой электронике: Справочник/Г. Г. Гурзадян, В. Г. Дмитриев, Д. Н. Никогосян. — М.: Радио и связь, 1991.— 160 с: ил. ISBN 5-256-00859-5.

Виртуальная лабораторная работа №5

ОПРЕДЕЛЕНИЕ УГЛОВ РАЗЛЁТА КОРРЕЛИРОВАННЫХ ФОТОНОВ

Цель: определить угол разлёта генерируемых фотонов для вырожденного случая спонтанного параметрического рассеяния.

Задачи, решаемые в работе

3. Рассчитать показатель преломления для излучения накачки при фиксированном угле поворота кристалла.
4. Получить график зависимости длины холостого излучения от длины волны сигнального излучения.
5. Получить график значений фазовой расстройки в зависимости от длины волны сигнального излучения и угла разлёта.
6. Выбрать угол, при котором фазовая расстройка для вырожденного случая будет минимальной.

Теоретические сведения

Существуют различные способы генерации коррелированных пар фотонов. Среди них наибольшее распространение получили следующие: спонтанное параметрическое рассеяние (СПР), четырёхволновое смешение (ЧВС), генерация коррелированных фотонов в полупроводниках. На данный момент «рабочей лошадкой» для генерации коррелированных фотонов можно назвать СПР. Впервые процесс СПР был теоретически описан Давидом Николаевичем Клышко (1966 г.). Спустя всего год, независимо друг от друга, тремя группами были поставлены эксперименты по реализации процесса СПР в нелинейных средах с нелинейной восприимчивостью второго порядка. Основными рабочими уравнениями для СПР можно назвать условие фазового синхронизма [1]:

$$\vec{k}_p = \vec{k}_s + \vec{k}_i, \qquad (1),$$

в котором $\vec{k}_p$, $\vec{k}_s$, $\vec{k}_i$ являются волновыми векторами для волн накачки, сигнальной и холостой, соответственно.

И условия баланса частот, которое, по сути, не что иное, как закон сохранения энергии:

$$\omega_p = \omega_s + \omega_i. \qquad (2).$$

Данные условия возникают как при работе с уравнениями нелинейной оптики, так и в квантовом случае. При этом в квантовом случае, обычно, мы рассуждаем о взаимодействии единиц фотонов. Так процесс СПР можно

описать как аннигиляцию одного фотона накачки и рождение двух фотонов, которые называются сигнальным и холостым фотоном. Стоит отметить, что данный процесс невозможен с точки зрения нелинейной оптики в отсутствие затравочного излучения, на котором будет происходить генерация. Это противоречит экспериментальным данным, и в этом плане квантовая теория даёт более точное описание этому процессу. Условия СПР могут выполняться в нелинейных оптических средах с нелинейной восприимчивостью второго порядка. В общем случае условия фазового синхронизма выполнить невозможно, но существуют несколько частных способов его реализации. Так, в одноосных и двуосных кристаллах можно подобрать такое направление, при котором условия синхронизма будут выполняться для вырожденного случая (при котором длина волн генерируемого излучения будет равна удвоенной длине волны накачки) для различных поляризаций излучения. Другим способом реализации условий синхронизма является компенсация разности между значениями волновых векторов (фазовой расстройки) вектором обратной решётки в нелинейных фотонных кристаллах (НФК). Выделяют три типа синхронизма 0, I и II. При 0-типе поляризации волн, участвующих во взаимодействии, одинаковы, такой случай реализуется в НФК. В случае I-типа между собой ортогональны поляризации накачки и генерируемого (сигнального и холостого) излучения. В случае II-типа взаимно перпендикулярны поляризации сигнального и холостого излучения.

Фотоны могут коррелировать по времени и месту рождения, поляризации, углу разлёта и энергии. Наиболее примечательным квантовым свойством коррелированных фотонов является группировка при прохождении светоделителя. В общем случае фотоны, попадая на светоделитель, проходят его независимо друг от друга. Коррелированные же фотоны при прохождении светоделителя при одновременном попадании на него начинают распространяться совместно.

Прежде чем приступить к описанию интересующих нас свойств кристалла, стоит отметить, что будет использована терминология, применяемая в нелинейной оптике. В то же время условия, которые будут выведены, могут быть использованы как для нелинейного, так и для квантового случаев.

При планировании эксперимента наибольшее внимание стоит уделить кристаллу, в котором будут реализованы условия фазового синхронизма. От угла, под которым вырезан кристалл, зависят значения показателей преломления и значение нелинейной эффективности и, как следствие, углы разлёта генерируемых фотонов. На рисунке 1 представлены индикатрисы показателей преломления для отрицательных и положительных одноосных кристаллов. Видно, что показатель преломления для обыкновенной волны остаётся неизменным в зависимости от направления, в то время как для необыкновенной волны он изменяется по следующему закону [2]:

$$n_e(\lambda,\theta) = \left[\left(\frac{\cos\theta}{n_0}\right)^2 + \left(\frac{\sin\theta}{n_e}\right)^2\right]^{-\frac{1}{2}}, \qquad (3)$$

где θ – угол поворота кристалла.

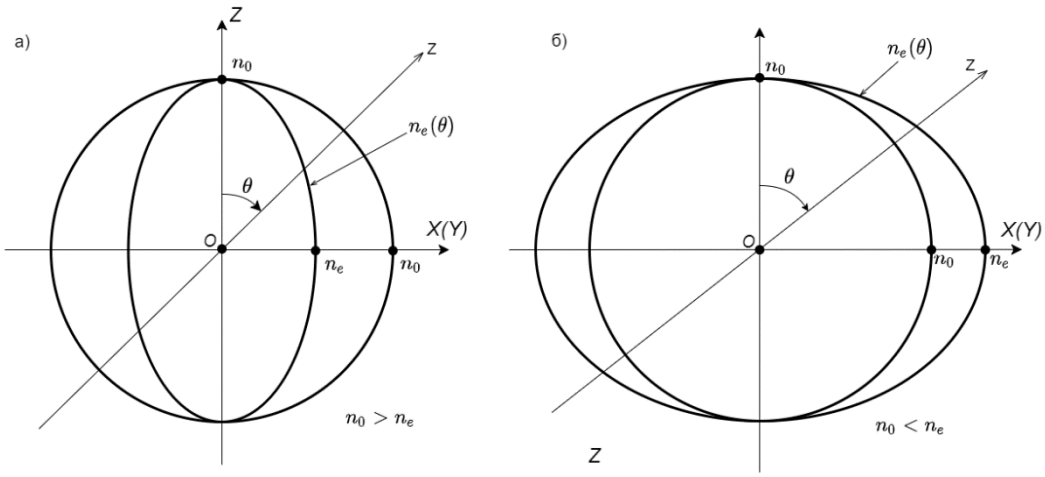


Рисунок 1 – индикатрисы показателей преломления
а) индикатрисы показателей преломления для отрицательного кристалла б) индикатрисы показателей преломления для положительного кристалла

Показатели преломления для кристалла бета-бората бария можно вычислить, пользуясь следующими уравнениями Зельмейера:

$$n_o = \sqrt{2{,}7359 + \frac{0{,}01878}{\lambda^2 - 0{,}01822} - 0{,}01354 \cdot \lambda^2}, \quad (4),$$

$$n_e = \sqrt{2{,}3753 + \frac{0{,}01224}{\lambda^2 - 0{,}01667} - 0{,}01516 \cdot \lambda^2}, \quad (5)$$

где λ – длина волны в мкм.

От значения показателя преломления зависят значения волновых векторов. Так, для I-типа синхронизма, значения волновых векторов будут определяться следующим образом:

$$k_p = \frac{2\pi n_e(\lambda,\theta)}{\lambda_p}, \quad (6)$$

$$k_s = \frac{2\pi n_o(\lambda_s)}{\lambda_s}, \quad (7)$$

$$k_i = \frac{2\pi n_o(\lambda_i)}{\lambda_i}. \quad (8)$$

Стоит обратить внимание на то, что в уравнении (6) используется показатель преломления для необыкновенной волны, который зависит от угла и вычисляется из уравнения (3).

Далее обратим своё внимание на векторное условие фазового синхронизма (1), которое можно так же рассмотреть, как систему из двух уравнений:

$$k_p = k_s cos\varphi_s' + k_i cos\varphi_i' \quad (9)$$

$$k_s \sin(\varphi_s') = k_i \sin(\varphi_i') \quad (10)$$

где φ_s' – угол между волновым вектором накачки и волновым вектором сигнального излучения, φ_i' – угол между волновым вектором накачки и волновым вектором холостого излучения.

Пользуясь уравнениями (9) и (10), можно вычислить углы разлёта сигнального и холостого фотонов на выходе из кристалла. Для этого воспользуемся законом Снеллиуса:

$$\sin(\varphi_s') = \frac{\sin(\varphi_s)}{n_o(\lambda_s)}, \quad (11)$$

$$\sin(\varphi_i') = \frac{\sin(\varphi_i)}{n_o(\lambda_i)}, \quad (12),$$

где φ_s – угол разлёта сигнального фотона, φ_i – угол разлёта холостого фотона. Подставим выражения (11) и (12) в уравнение (10):

$$k_s \frac{\sin(\varphi_s)}{n_o(\lambda_s)} = k_i \frac{\sin(\varphi_i)}{n_o(\lambda_i)}. \quad (13)$$

Воспользовавшись выражением (13), для (9) получим:

$$k_p = k_s \sqrt{1 - \left(\frac{\sin(\varphi_s)}{n_o(\lambda_s)}\right)^2} + k_i \sqrt{1 - \left[\frac{\lambda_i}{\lambda_s}\right]^2 \left(\frac{\sin(\varphi_s)}{n_o(\lambda_i)}\right)^2}. \quad (14)$$

Из выражения (14) можно получить значение угла разлёта для сигнального фотона и вычислить угол разлёта холостого фотона из выражения (13).

Важным условием при решении уравнения (14) является выполнение условия баланса частот (2), которое так же можно выразить через длины волн:

$$\frac{1}{\lambda_p} = \frac{1}{\lambda_s} + \frac{1}{\lambda_i}. \quad (15)$$

Предполагая, что длина волны накачки и сигнального излучения будет известна, длину холостой волны можно выразить следующим образом:

$$\lambda_i = \frac{\lambda_s \lambda_p}{\lambda_s - \lambda_p}. \quad (16)$$

При рассмотрении условий фазового синхронизма можно говорить о фазовой расстройке Δk. При выполнении условий синхронизма $\Delta k = 0$. В противном случае фазовую расстройку можно вычислить следующим образом:

$$\Delta k = k_p - k_s \sqrt{1 - \left(\frac{\sin(\varphi_s)}{n_o(\lambda_s)}\right)^2} - k_i \sqrt{1 - \left[\frac{\lambda_i}{\lambda_s}\right]^2 \left(\frac{\sin(\varphi_s)}{n_o(\lambda_i)}\right)^2}. \quad (17)$$

Варьируя значения углов разлёта и длин сигнальной и холостой волн, можно подобрать условия, при которых $\Delta k = 0$.

Ход работы

Рассматривается отрицательный одноосный кристалл бета-бората бария, в котором реализуется I-тип синхронизма. Для бета-бората бария поляризация излучения накачки будет необыкновенной (е), для сигнального и холостого – обыкновенной (о). Кристалл вырезан под углом θ=29,2°. Длина волны излучения накачки λ_p= 400 нм.

Задание рекомендуется выполнять в Matlab, но возможно применение иных программных средств.

1. Рассчитайте показатель преломления волны накачки для заданного угла. Для этого рассчитайте обыкновенный и необыкновенный показатели преломления, пользуясь уравнениями (4) и (5). Полученные значения подставьте в уравнение (3).
2. Пользуясь уравнением (16), получите зависимость длины холостой волны от длины сигнальной волны.
3. Пользуясь уравнением (17), запрограммируйте двойной цикл, в котором будет рассчитываться фазовая расстройка, учитывая зависимость показателя преломления и волнового вектора от длины волны, изменяя угол разлёта φ_s в пределах от -10° до 10° с шагом в 0,1° и длину волны сигнального излучения от 500 до 1200 нм с шагом в 1 нм. В результате должен получиться массив значений размерами 201x701. Примените функцию **sinc**^{2}(X*0,0005), где X – ваши значения, **sinc –** кардинальный синус.
7. Постройте трёхмерный график зависимости значения фазовой расстройки от угла разлёта и длины сигнальной волны.
8. Выберете угол, который соответствует вырожденному случаю ($\Delta k \to 0$).

Содержание отчета

3. Значение показателя преломления для волны накачки.
4. График зависимости длины холостой волны от длины сигнальной волны.
5. Трёхмерный график для зависимости фазовой расстройки от угла разлёта фотонов и длины волны сигнального излучения.
6. Угол разлёта фотонов для вырожденного случая при накачке 400нм.
7. При подготовке отчёта, поместите код программы на отдельную страницу с подписью: «**ПРИЛОЖЕНИЕ А**».

Вопросы к защите

1. Запишите условие фазового синхронизма и уравнение баланса частот. Как данные условия выполняются при постановке эксперимента?
2. Перечислите и сопоставьте корреляционные свойства фотонов, которые определяются данными уравнениями. Какие из перечисленных видов корреляций мы могли наблюдать в проделанном эксперименте?

3. По каким параметрам разделяют условия синхронизма? Перечислите типы синхронизма. В чём заключается различие типов синхронизма? В чём принципиальное отличие вырожденного случая синхронизма от невырожденного?
4. При решении связанных дифференциальных уравнений для случая СПР, возникает необходимость условия, которое не требуется при использовании квантовой теории, что это за условие?
5. Перечислите источники оптических потерь, которые могут возникнуть в экспериментальной установке (обратите внимание, что нас интересуют только потери, связанные с генерируемым излучением). Объясните разницу между полученными значениями в каналах.
6. Выполнение какого условия позволяет нам сделать вывод, что мы работаем в режиме СПР?
7. Первоначальная юстировка установки производится при помощи дополнительного лазера. С чем это связано?
8. В каких целях могут быть использованы коррелированные фотоны? Перечислите известные схемы и их применение (подготовить схематические изображения, например, скрин из статьи, и уметь рассказать об основных элементах)

Использованные источники литературы

1. Couteau C. Spontaneous parametric down-conversion
2. Shih Y. Entangled biphoton source—property and preparation // Rep. Prog. Phys. – 66 – 2003 – pp.1009–1044.

Лабораторная работа №6

ПРОВЕРКА НАРУШЕНИЯ НЕРАВЕНСТВА БЕЛЛА (ВЛР Э)

Цель работы: Изучение *неклассических* свойств квантовой механики.

Задачи, решаемые в работе

1. Изучение свойств запутанных состояний.
2. Построение квантовых логических схем для приготовления и измерения запутанных состояний.
3. Проверка нарушения неравенства Белла.

Краткие теоретические сведения

ЭПР парадокс

В *классическом* понимании физические свойства объектов не зависят от наблюдения, измерение только обнаруживает эти свойства. В соответствии с принципами квантовой механики объект, над которым не проводится наблюдение, не обладает физическими характеристиками, существующими независимо от наблюдения, физические характеристики возникают вследствие эксперимента [1].

Такой взгляд на природу был неоднозначно воспринят в научном сообществе. Наиболее ярким примером является мысленный эксперимент, предложенный А. Эйнштейном, Б. Подольским, Н. Розеном (ЭПР), направленный на то, чтобы показать неполноту квантовой механики. Авторы собирались показать, что физическая характеристика всегда является элементом действительности.

В качестве примера можно рассмотреть запутанное состояние из двух кубитов:

$$|\psi\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}} \qquad (1)$$

Первый кубит принадлежит Алисе, второй Бобу, которые находятся на достаточно большом расстоянии друг от друга. Пусть Алиса определяет величину проекции спина на ось $\vec{v}$, то есть измеряет наблюдаемую $\vec{v}\cdot\vec{\sigma} = v_1\sigma_1 + v_2\sigma_2 + v_3\sigma_3$, где $\sigma_{1,2,3}$ – матрицы Паули, а $v_{1,2,3}$ – компоненты трехмерного единичного вектора $\vec{v}$. Если при измерении Алиса получает результат $+1(-1)$, то она может утверждать, что Боб будет иметь в результате измерения $+1(-1)$. Результат $+1$ соответствует измеренному кубиту в состоянии $|0\rangle$, а -1 – кубиту в состоянии $|1\rangle$. Таким образом, Алиса всегда может предсказать результат, получаемый Бобом при измерении проекции его спина на ось $\vec{v}$, и процесс измерения Боба не будет влиять на результат. Эйнштейн, Подольский и Розен хотели тем самым показать неполноту квантовой механики, продемонстрировав, что в квантовой механике не

хватает некоторых «элементов действительности», то есть приписать системам свойства, существующие вне зависимости от выполняемых над ними измерений. Однако позже появилось экспериментальное опровержение этой теории, в основу которого лег результат, известный как неравенство Белла.

Неравенство Белла

При описании неравенства Белла, как правило, предлагается следующий мысленный эксперимент. Предполагается, что есть две системы, представленные на рисунке 1. Готовится состояние двух частиц: одна посылается Алисе, другая Бобу. Каждый имеет два прибора и может случайным образом провести любое из двух измерений: A, A' и B, B'. Измерения имеют только два возможных исхода: $+1$ или -1. Процессы измерения Алисы и Боба синхронизированы во времени, а события, соответствующие этим измерениям, являются абсолютно удаленными.

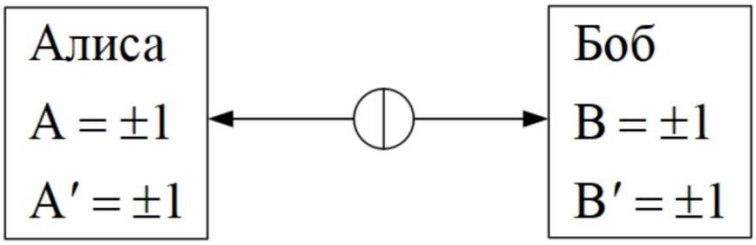


Рисунок 1. Визуализация мысленного эксперимента для описания неравенства Белла

John Clauser, Michael Horne, Abner Shimony и Richard Holt вывели следующее CHSH неравенство, основанное на *классическом* понимании физических свойств объектов:

$$E(AB) + E(A'B) + E(AB') - E(A'B') \leq 2, \qquad (2)$$

где математическое ожидание

$$E(AB) = \sum_{a,b=\pm 1} ab \cdot P(a,b), \qquad (3)$$

P – вероятность совместного события, a, b – исходы каждого отдельного события. Это неравенство является частью большого набора неравенств, называемых неравенствами Белла, так как первое из этих неравенств было предложено Беллом.

При выводе неравенства было сделано два предположения: 1 – все наблюдаемые имеют определенные значения, которые существуют вне зависимости наблюдения. 2 – измерение Алисы не влияет на результат измерения Боба и наоборот, то есть никакая информация не может передаваться быстрее скорости света. Первое называют предположением локальности, второе – предположением реализма. Это интуитивно понятные нам предположения, при которых неравенство Белла выполняется. Однако,

как дальше будет видно, это неравенство может нарушаться, следовательно, по крайней мере одно из этих предположений неверно!

Эксперимент Белла

Проведем аналогичное рассуждение, используя аппарат квантовой механики. Пусть Чарли подготовил запутанное состояние $|\psi\rangle$. После этого, он передает первый кубит Алисе, а второй Бобу, которые проводят измерения следующих наблюдаемых:

$$A = Z\,B = \frac{Z+X}{\sqrt{2}}\;A' = X\,B' = \frac{Z-X}{\sqrt{2}} \tag{4}$$

где $Z = (1\;0\;0\;-1)$, а $X = (0\;1\;1\;0)$. Средние значения представленных наблюдаемых, записанных с применением квантово-механических обозначений $\langle\cdot\rangle$:

$$\langle \mathrm{AB}\rangle = \langle\psi|\mathrm{A}\otimes\mathrm{B}|\psi\rangle = \frac{1}{\sqrt{2}} \quad \langle \mathrm{AB'}\rangle = \_\_ \qquad \langle \mathrm{A'B}\rangle = \_\_ \quad \langle \mathrm{A'B'}\rangle = \_\_ \tag{5}$$

Тогда

$$\langle AB\rangle + \langle A'B\rangle + \langle AB'\rangle - \langle A'B'\rangle = 2\sqrt{2} \tag{6}$$

Видно, что неравенство Белла в этом случае нарушается. Были поставлены эксперименты, которые демонстрируют невыполнение неравенств Белла, то есть статистика измерений не может быть объяснена какой-либо локальной теорией скрытых переменных, и должны существовать корреляции, выходящие за рамки классической теории.

Существование *неклассических* явлений открывает для нас новые возможности. Например, большинство достижений в области квантовых вычислений и квантовой информатики непосредственно связаны с запутанными состояниями. Главная задача квантовых технологий на данный момент – использование этих новых ресурсов для задач, не выполнимых или трудно выполнимых с помощью классических подходов.

Ход лабораторной работы

Описанный выше эксперимент Белла можно наглядно построить с помощью квантовых логических схем, использующих условные обозначения операторов, действующих на кубит. Аналогичный эксперимент можно поставить на реальном квантовом компьютере, доступ к которому предоставлен компанией IBM [2].

В лабораторной работе предлагается построить простую модель для проверки нарушения неравенства Белла, используя унитарные операции, в программном пакете для моделирования. Предлагается для моделирования использовать программный пакет Wolfram Mathematica, который позволяет реализовывать простые операции линейной алгебры, необходимые для выполнения работы. Лабораторная работа может быть выполнена с

использованием языка программирования python, c++ и др. Для выполнения работы также можно использовать пакет для моделирования динамики квантовых систем QuTiP (http://qutip.org), который находится в открытом доступе. С помощью данного пакета можно производить все необходимые вычисления, строить квантовые логические схемы и визуализировать результаты измерения.

Для проверки нарушения неравенства Белла необходимо построить схему, позволяющую приготовить запутанное состояние $|\psi\rangle$ (Рисунок 2).

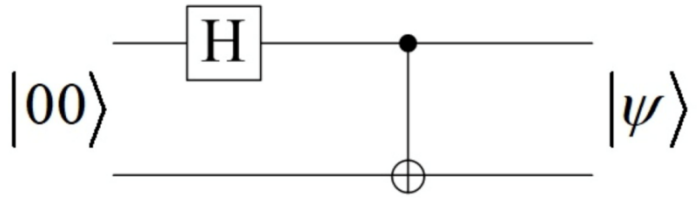


Рисунок 2. Схема для приготовления запутанного состояния

Предлагается получить состояние на выходе схемы двумя способами: 1 – последовательное применение операторов в пространстве двух кубит к исходному состоянию $|00\rangle$, 2 – представление в виде одного оператора, состоящего из композиции операторов, который действует на входное состояние.

Запишите промежуточные расчеты, получите выходные состояния и приложите код.

Далее, необходимо построить 4 схемы, реализующие проективные измерения в различных базисах, эквивалентные двум доступным Алисе и Бобу измерениям. Каждая схема должна готовить запутанное состояние (Рисунок 2) и производить измерение наблюдаемых: $AB, A'B, AB', A'B'$. Известно, что непосредственно измерение некоторым устройством эквивалентно измерению наблюдаемой A, тогда измерения других наблюдаемых реализуются путем применения к состоянию унитарных операций и последующего измерения наблюдаемой A (Рисунок 3).

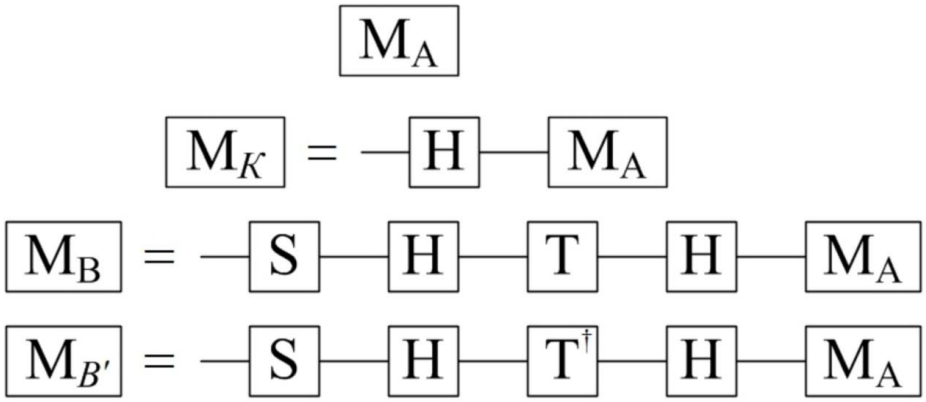


Рисунок 3. Измерение наблюдаемых A, A', B, B'. M_A – непосредственное измерение некоторым устройством, эквивалентное измерению наблюдаемой A. $M_K, M_B, M_{B'}$ - соответствуют измерениям наблюдаемых A', B, B' соответственно. S, H, T – унитарные операторы.

Постройте 4 схемы и получите состояние на выходе каждой схемы до измерения наблюдаемой A. Вычислите средние значения $\langle AA \rangle$ для каждой схемы и проверьте выполнение неравенства Белла.

Вычислите вероятности получения четырех состояний $|00\rangle, |11\rangle, |01\rangle, |10\rangle$ после измерений наблюдаемой A. Рассчитайте математическое ожидание для совместных событий и проверьте выполнение неравенства Белла.

	P (0,0)	P (1,1)	P (0,1)	P (1,0)	$E(AB)$
AB					
$A'B$					
AB'					
$A'B'$					
$\langle AB \rangle + \langle A'B \rangle + \langle AB' \rangle - \langle A'B' \rangle =$					

Содержание отчета

1. Цель и задачи.
2. Краткое содержание теории.
3. Рисунки используемых схем.
4. Написанный код/программа.
5. Таблица с результатами расчетов.

6. Вывод по проделанной работе.

Контрольные вопросы

1. Приведите другие примеры запутанных состояний.
2. Вычислите все средние значения наблюдаемых в (5).
3. Если кубит находится в состоянии $|0\rangle$ и выполняются измерения наблюдаемой X и Z, чему будут равны средние значения наблюдаемых?

Использованные источники литературы

1. Nielsen, M.A., Chuang, L.I.: Quantum computation and quantum information. Cambridge University Press, Cambridge, (2000)
2. https://quantum-computing.ibm.com

Лабораторная работа №7

МОДЕЛИРОВАНИЕ УНИТАРНОЙ ДИНАМИКИ КУБИТА, ИЗУЧЕНИЕ ПРИНЦИПОВ РАБОТЫ БАЗОВЫХ КВАНТОВЫХ АЛГОРИТМОВ (ДК)

Цель работы: Изучение принципов работы квантовых схем и алгоритмов.

Задачи, решаемые в работе

1. Реализация унитарных операций и их представление на сфере Блоха
2. Моделирование работы квантового алгоритма Дойча
3. Моделирование работы квантового алгоритма Гровера

Краткие теоретические сведения

Кубит

Кубит представляет собой квантовую систему, состояние которой задается вектором состояния $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$, параметризованным двумя комплексными числами, удовлетворяющими условию $|a|^2 + |b|^2 = 1$ [1]. В общем случае комплексных коэффициентов α и β они могут быть представлены в виде

$$\alpha = e^{i\gamma}\cos\frac{\theta}{2}, \beta = e^{i\lambda}\sin\frac{\theta}{2}. \quad (1)$$

Тогда кубит принимает вид

$$|\psi\rangle = e^{i\gamma}\cos\frac{\theta}{2}|0\rangle + e^{i\lambda}\sin|1\rangle, \quad (2)$$

или

$$|\psi\rangle = e^{i\gamma}(\cos\frac{\theta}{2}|0\rangle + e^{i(\lambda-\gamma)}\sin|1\rangle). \quad (3)$$

Опуская фазовый множитель $e^{i\gamma}$, который для многих задач является несущественным, получаем:

$$|\psi\rangle = \cos\frac{\theta}{2}|0\rangle + e^{i\varphi}\sin|1\rangle), \quad (4)$$

где $\varphi = \lambda - \gamma$. Таким образом, полученное представление кубита имеет два параметра – θ и φ, которые можно интерпретировать как углы сферической системы координат. Кубит представляется вектором единичной длины в трехмерном пространстве. Такое геометрическое изображение кубита называется его представлением на сфере Блоха (Рисунок 1).

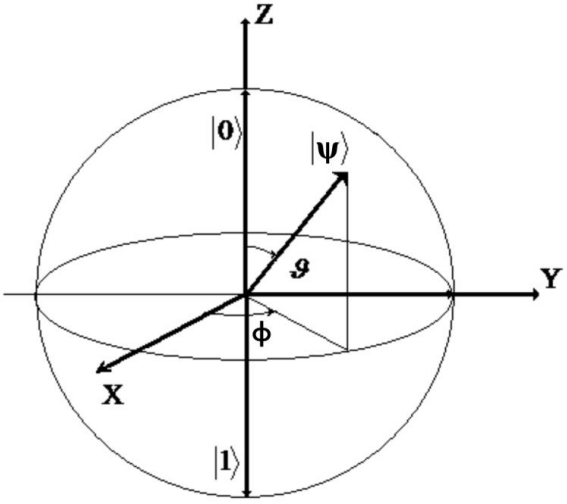


Рисунок 1. Геометрическое изображение кубита – сфера Блоха

Квантовые операторы

Эволюция состояния замкнутой квантовой системы во времени описывается уравнением Шредингера

$$i\hbar\frac{d|\psi\rangle}{dt} = \mathrm{H}|\psi\rangle, \tag{5}$$

где H – гамильтониан системы. Решение уравнения Шредингера, с гамильтонианом, не зависящим от времени, может быть записано в виде

$$|\psi'\rangle = e^{\frac{-i\mathrm{H}t}{\hbar}}|\psi\rangle. \tag{6}$$

Физическое воздействие на систему переводит ее в другое состояние $|\psi'\rangle$.

Операции над кубитами описываются унитарными операторами $\mathrm{U} = e^{\frac{-i\mathrm{H}t}{\hbar}}$, которые сохраняют нормализацию вектора состояния.

$$|\psi'\rangle = \mathrm{U}|\psi\rangle \tag{7}$$

Вектор $|\psi\rangle$ играет роль входного сигнала, оператор U определяет вычислительный процесс, а вектор $|\psi'\rangle$ представляет собой результат вычисления [2].

Наиболее часто используемыми являются следующие однокубитовые операторы:

$$\begin{gathered}\mathrm{X} = \begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix} \quad \mathrm{Z} = \begin{pmatrix}1 & 0\\ 0 & -1\end{pmatrix} \quad \mathrm{Y} = \begin{pmatrix}0 & -i\\ i & 0\end{pmatrix}\\ \mathrm{H} = \frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix} \quad \mathrm{S} = \begin{pmatrix}1 & 0\\ 0 & i\end{pmatrix} \quad \mathrm{T} = \begin{pmatrix}1 & 0\\ 0 & e^{\frac{i\pi}{4}}\end{pmatrix}\end{gathered} \tag{8}$$

Двухкубитовые операции

Два отдельных кубита относятся к разным векторным пространствам $|\psi_1\rangle \in H_1$, $|\psi_2\rangle \in H_2$. Векторное пространство, элементами которого являются пары векторов, первый из которых принадлежит пространству H_1, а второй – пространству H_2 задается тензорным произведением пространств $H_1 \otimes H_2$. Элементы его обозначаются как $|\psi\rangle = |\psi_1\rangle \otimes |\psi_2\rangle$. Для того, чтобы представить векторы состояния и операторы тензорного произведения пространств $H_1 \otimes H_2$ в вычислительном базисе, введем понятие тензорного (Кронекерова) произведения матриц. Пусть A – матрица $m \times n$, B – матрица $r \times s$. Произведение Кронекера матриц A и B определяется как матрица $(m \cdot r) \times (n \cdot s)$

$$A \otimes B = \begin{pmatrix} A_{11}B & A_{12}B & \cdots & A_{1n}B \\ A_{21}B & A_{22}B & \cdots & A_{2n}B \\ \cdots & \cdots & \cdots & \cdots \\ A_{m1}B & A_{m2}B & \cdots & A_{mn}B \end{pmatrix} \quad (9)$$

В пространстве нескольких кубит могут использоваться условные операции, при которых состояние управляемого кубита зависит от состояния управляющих. Одним из примеров таких операций является наиболее часто используемый оператор CNOT (Рисунок 2). Если верхний (управляющий) кубит находится в состоянии $|1\rangle$, к нижнему (управляемому) применяется операция смены бита (оператор X).

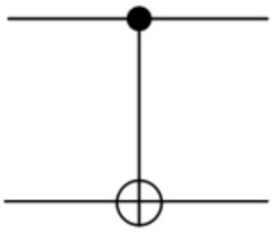


Рисунок 2. Схематичное изображение и матрица оператора CNOT

Матричное представление оператора CNOT имеет вид

$$NOT = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \quad (10)$$

Более общим случаем является произвольная управляемая операция CU. Если управляющий кубит находится в состоянии $|1\rangle$, к управляемому применяется операция U.

Все представленные однокубитовые и двухкубитовые операторы будут необходимы для выполнения лабораторных работ. Однако существуют операторы, работающие в пространстве трех кубит и более. Например, аналог оператора CNOT для трех кубит – оператор Тоффоли (CCNOT), но основе которого может быть реализована управляемая операция для большого числа кубит. Также существуют тождественные схемы, использующие универсальный набор операторов, которые позволяют реализовать любую унитарную операцию. Более подробно о квантовых операторах будет рассказано в рамках курса.

Алгоритм распознавания функций (алгоридм 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:

$$f_1|0\rangle = |0\rangle,\ f_1|1\rangle = |0\rangle, \text{ или } f_1|x\rangle = |0\rangle, x = 0, 1, \quad (11)$$

$$f_2|0\rangle = |1\rangle,\ f_2|1\rangle = |1\rangle, \text{ или } f_2|x\rangle = |1\rangle, x = 0, 1. \quad (12)$$

Две другие функции f_3 и f_4 – сбалансированные:

$$f_3|x\rangle = |x\rangle,\ f_4|x\rangle = \mathrm{NOT}|x\rangle, x = 0, 1. \quad (13)$$

Требуется узнать, к какому из двух классов принадлежит неизвестная функция f? Классический алгоритм требует две операции, для квантового алгоритма Дойча требуется одна операция.

Для реализации этого алгоритма построим двухкубитовый унитарный оператор U_f, действующий по правилу:

$$U_f\,(|x\rangle \otimes |y\rangle) = |x\rangle \otimes (|y\rangle \oplus f|x\rangle). \quad (14)$$

Для каждой из четырех функций f, U_f принимает следующий вид:

$$U_1 = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \quad U_2 = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$
$$U_3 = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \quad U_4 = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix}. \quad (15)$$

Распознавание функции f заменяется на распознавание оператора U_f. На вход схемы всегда подается двухкубитовое состояние $|01\rangle$. Схема квантового алгоритма Дойча изображена на рисунке 3. С помощью представленного алгоритма можно за одну итерацию (одно обращение к U_f) определить класс функции f.

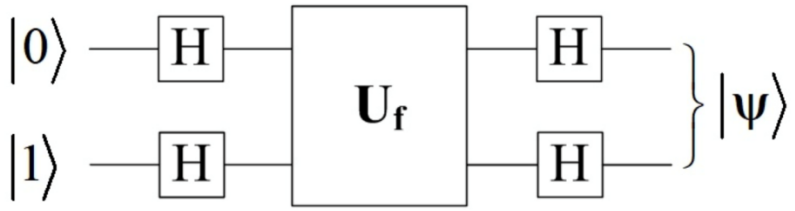


Рисунок 3. Квантовая схема, реализующая алгоритм Дойча

Квантовый алгоритм поиска (алгоритм Гровера)

Классический алгоритм поиска в неотсортированной базе данных из N элементов способен найти требуемый за O(N) операций. Квантовый алгоритм поиска (алгоритм Гровера) способен ускорить поиск до O($\sqrt{N}$) операций. Здесь рассмотрена общая процедура работы алгоритма Гровера и представлена одна из возможных схем.

Перед итерацией алгоритма система находится в состоянии $\left|0^{\otimes n}\right\rangle$. Далее готовится равновероятная суперпозиция состояний:

$$|\Psi\rangle = \frac{1}{N^{1/2}} \sum_{x=0}^{N-1} |x\rangle. \qquad (16)$$

После этого происходит непосредственно итерация алгоритма Гровера, которая состоит из применения оракула, который распознает решение задачи поиска, и применения операции инверсии относительно среднего, которая увеличивает амплитуду вероятности отмеченного состояния и уменьшает амплитуды других состояний.

На рисунке 4 приведен пример реализации двухкубитового алгоритма Гровера. Алгоритм позволяет за одну итерацию найти отмеченное состояние среди четырех: $|00\rangle$, $|01\rangle$, $|10\rangle$, $|11\rangle$. Переключение состояния, удовлетворяющего условиям поиска, реализовано в блоке оракула. Операция $(X \otimes X)CZ$ в блоке оракула соответствует отмеченному состоянию $|00\rangle$, $(X \otimes I)CZ$ – $|01\rangle$, $(I \otimes X)CZ$ – $|10\rangle$, $(I \otimes I)CZ$ – $|11\rangle$. Состояние на выходе алгоритма является решение задачи поиска, т.е. отмеченным оракулом состоянием.

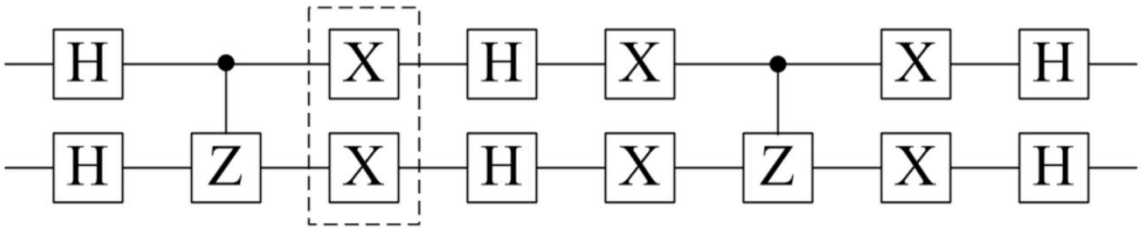


Рисунок 4. Квантовая схема, реализующая алгоритм Гровера

Ход лабораторной работы

1. Применить к каждому из входных состояний $|0\rangle$ и $\frac{|0\rangle+|1\rangle}{\sqrt{2}}$ три любых унитарных оператора на выбор. Получить итоговое состояния и изобразить их расположение на сфере Блоха.
2. Построить модель алгоритма Дойча и получить состояния на выходе алгоритма для каждой из четырех функций f.
3. Построить модель алгоритма Гровера и получить на выходе алгоритма каждое из четырех отмеченных состояний.

Для выполнения лабораторной работы предлагается использовать программный пакет для моделирования Wolfram Mathematica, который позволяет реализовывать простые операции линейной алгебры, необходимые для выполнения работы. Лабораторная работа может быть выполнена с использованием языка программирования python, c++ и др. Для выполнения работы также можно использовать пакет для моделирования динамики квантовых систем QuTiP (http://qutip.org), который находится в открытом доступе. С помощью данного пакета можно производить все необходимые вычисления, строить квантовые логические схемы и визуализировать результаты измерения.

Содержание отчета

1. Цель и задачи.
2. Краткое содержание теории.
3. Рисунки используемых схем.
4. Написанный код/программа.
5. Результаты расчетов.
6. Вывод по проделанной работе.

Контрольные вопросы

1. Приведите пример составного оператора, тождественного оператору X,
2. Приведите схему и матрицу трехкубитового оператора CCZ,
3. Опишите один квантовый алгоритм на выбор из тех, что не были описаны в лабораторной работе.

Литература

1. Nielsen M.A., Chuang L.I.: Quantum computation and quantum information. Cambridge University Press, Cambridge, (2000)
2. С.А.Чивилихин: КВАНТОВАЯ ИНФОРМАТИКА, Учебное пособие, Санкт-Петербург, (2009)

Лабораторная работа №8

КВАНТОВОЕ РАСПРЕДЕЛЕНИЕ КЛЮЧА НА БОКОВЫХ ЧАСТОТАХ ФАЗОМОДУЛИРОВАННОГО ИЗЛУЧЕНИЯ (ВЛР А)

Цель работы: теоретическое изучение основных принципов квантового распределения ключа на боковых частотах (КРКБЧ) фазомодулированного излучения.

Задачи, решаемые в работе

1. Изучение основных принципов фазовой модуляции монохроматического излучения.
2. Исследование влияния основных характеристик системы квантового распределения ключа на боковых частотах на ее производительность.

Краткие теоретические сведения

Введение

До недавнего времени применение одиночных фотонов ограничивало скорость генерации ключей по технологическим причинам (эксплуатация только в лабораторных условиях, низкая скорость генерации одиночных фотонов и т.п. причины, приведенные, например, в обзоре по источникам однофотонного излучения [1]), следовательно, применение ослабленного (содержащего в среднем менее одного фотона в импульсе или за время посылки в случае непрерывного излучения) лазерного излучения (когерентных состояний) являлось разумной альтернативой. В частности, различные протоколы КРК с фазовым кодированием, использующие ослабленные когерентные состояния, широко распространены, например [2 – 4]. Одним из них является протокол КРК, реализованный на принципе боковых частот, который впервые показан в 1998 году в [5] и далее развивался в [6 – 9]. В данной лабораторной работе мы будем изучать именно этот протокол. Легко показать, что конечный набор когерентных состояний будет линейно независимым, в отличие от однофотонных состояний с поляризационным кодированием, как в протоколе BB84, приводит к принципиально других свойствам и, следовательно, методам исследования информационных характеристик. Впрочем, последнее явно выходит за рамки данной лабораторной работы.

Далее рассмотрим оптическую схему установки и описание простейшего протокола. Для моделирования процесса формирования секретного ключа далее будут представлены физическая и информационная модели, которые будут впоследствии объединены.

Оптическая схема

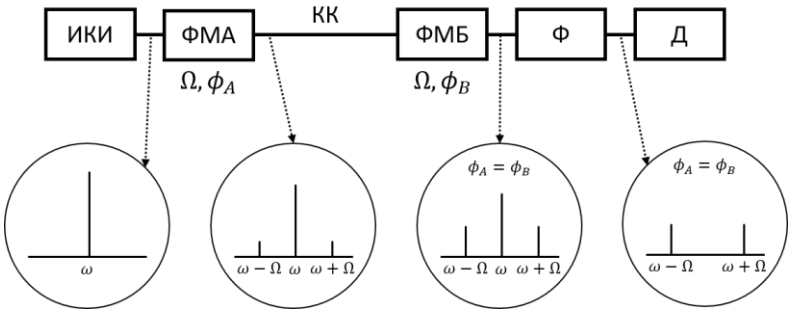


Рисунок – 1 Оптическая схема (упрощенная) исследуемой системы КРКБЧ (обозначения приведены в тексте)

Оптическая схема представлена на Рис. 1. Источник когерентного излучения ИКИ испускает слабый монохроматический свет (сигнал), в спектре которого после фазовой модуляции в электрооптическом модуляторе ФМА, к которому приложен осциллирующий электрический сигнал с частотой Ω порядка нескольких ГГц и фазой ϕ_A, появляются боковые частоты (на схеме показаны только первые боковые частоты). Далее модулированный сигнал проходит через квантовый канал КК (оптическое волокно), где претерпевает затухание. После сигнал проходит второй электрооптический модулятор, к которому также приложен осциллирующий электрический сигнал с частотой Ω и фазой ϕ_B. В зависимости от разности фаз ϕ_A и ϕ_B амплитуды боковых частот увеличиваются (забирая часть энергии с центральной частоты в случае $\phi_A = \phi_B$) или уменьшаются (энергия перетекает на центральную частоту). Узкополосный фильтр Ф пропускает только боковые частоты (и малую часть центральной частоты), далее происходит регистрация сигнала с помощью детектора одиночных фотонов Д.

Простейший протокол

Рассмотрим подробнее наиболее простой протокол квантового распределения ключа, т. е. последовательность шагов, которая позволяет передавать последовательность коррелированных бит только между отправителем и получателем, использующим представленную выше схему

1. **Распределение квантовых состояний**
   a. Отправитель, управляя фазовым модулятором ФМА, выбирает случайным образом фазу модулирующего сигнала из набора $\{0, \pi\}$, соответствующую значению бита 0 или 1. Отправитель производит случайную смену фазы модулирующею сигнала с некоторой периодичностью (в один период происходит посылка одного бита).
   b. Получатель, управляя фазовым модулятором ФМБ, аналогичным образом выбирает значение фазы модулирующего сигнала из того же набора значений фаз. Получатель производит случайную смену фазы модулирующего сигнала с некоторой периодичностью, в такт смене фазы у отправителя.

c. Получатель записывает, при каких выбранных значениях фазы происходит срабатывание детектора одиночных фотонов. В идеальном случае срабатывание детектора происходит только при совпадении фаз модулирующих сигналов ($\phi_A = \phi_B$).
d. Перечисленные выше пункты повторяются до тех пор, пока не произойдет определенного числа срабатываний детектора (в общем случае определяется условиями криптографической стойкости протокола, рассмотрение которой не входит в данную лабораторную работу).

2. Определение параметров

a. Отправитель выбирает случайным образом некоторое количество посылок (в асимптотическом случае, когда число посылок стремится к бесконечности, число посылок для определения ошибок пренебрежимо мало) и оглашает для них выбранное значение бита.
b. Получатель сравнивает полученные значения со своими и вычисляет долю ошибок Q, т.е. тех случаев, когда значение бит разное.
c. Оба отбрасывают посылки, использованные для определения доли ошибок.
d. Возможно определение дополнительных параметров, например числа (или скорости) срабатывания детектора. Выполнение определенных условий для значений дополнительных параметров скорее всего сигнализирует о попытке перехвата, и, следовательно, протокол должен быть остановлен.

3. Исправление ошибок

a. На основе оцененного уровня ошибок отправитель объявляет соответствующую избыточность (например, синдром алгоритма исправления ошибок). В асимптотическом пределе отношение наименьшей избыточности к длине последовательности бит составляет $h(Q)$ (согласно теореме Шеннона), определяемое согласно выражению 9.
b. Получатель исправляет ошибки, используя избыточность. У обоих получаются идентичные последовательности бит.

4. Усиление секретности

a. Отправитель и получатель случайным образом (согласовано) выбирают число бит для обеспечения полного незнания третьих лиц (перехватчика) об оставшихся битах (в том числе избыточность для исправления ошибок, так как она коррелированна с битами отправителя и получателя), и отбрасывают их.

Физическая модель системы

Первая модуляция

В данном разделе рассмотрим подробнее процесс фазовой модуляции. Для этого рассмотрим сперва 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:

$$A(t)e^{im\sin(\Omega t+\phi_A)} = A(t)\sum_{n=-\infty}^{\infty} J_n(m)e^{i(\Omega t+\phi_A)n}$$
$$= A(t)\sum_{n=-\infty}^{\infty}[A_0 J_n(m)e^{i(\omega+\Omega t)t+i\phi_A n}], \qquad (1)$$

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 $\mu_0 = |A_0|^2 \Delta T/(\hbar\omega)$, где$\Delta T$ – 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.

Распространение в квантовом канале

После формирования фазомодулированного излучения его необходимо передать от отправителя к получателю через квантовый канал. В общем виде это может быть как атмосферный канал, так и оптоволоконный. Наиболее распространены последние, поэтому в данной работе будем рассматривать именно их. При распространении в оптическом волокне наиболее важным является затухание излучения (остальными эффектами, такими как, например, дисперсия или двулучепреломление, пренебрежем в рамках данной работы), которое описывается законом Бера-Бугера-Ламберта (в терминах волоконной оптики), т.е. домножением мощности (или среднего числа фотонов) на множитель вида $10^{\frac{\alpha L}{10}}$, где α – удельное пропускание на единицу длины канала (типичное значение –0,2 дБ/км для телекоммуникационной длины волны излучения 1,55 мкм), L – длина квантового канала. Аналогичным образом вводятся фиксированные потери β (типичные значения от –5 до –10 дБ) в блоке получателя, получая общее значение затухания $\gamma(L) = 10^{\frac{\alpha L+\beta}{10}}$.

Повторная модуляция

Рассмотрим также случай повторной модуляции с фазой модулирующего сигнала ϕ_B:

$$A(t)e^{im\sin(\Omega t+\phi_A)}e^{im\sin(\Omega t+\phi_B)} = A(t)e^{i2m\cos\left(\frac{\phi_A-\phi_B}{2}\right)\sin\left(\Omega t+\frac{\phi_A+\phi_B}{2}\right)} =$$

$$A(t)\sum_{n=-\infty}^{\infty} J_n\left(2m\cos\left(\frac{\phi_A-\phi_B}{2}\right)\right)e^{i\left(\Omega t+\frac{\phi_A+\phi_B}{2}\right)n} =$$

$$\sum_{n=-\infty}^{\infty}\left[A_0 J_n\left(2m\cos\left(\frac{\phi_A-\phi_B}{2}\right)\right)\right]e^{i(\omega+\Omega t)t+\frac{\phi_A+\phi_B}{2}n}. \qquad (2)$$

Таким образом, получаем излучение на боковых частотах $\omega + \Omega n$ с амплитудой $A_0 J_n(\widetilde{m})$, где $\widetilde{m} = 2m\cos\left(\frac{\phi_A-\phi_B}{2}\right)$. 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 $\mu_0(1 - J_0^2(\widetilde{m}))$ и $\mu_0 J_0^2(\widetilde{m})$ соответственно.

Спектральная фильтрация

Предполагая, что спектральный фильтр Ф пропускает ϑ часть мощности центральной частоты, среднее число фотонов, оставшееся на центральной частоте после фильтрации равно $\vartheta\mu_0 J_0^2(\widetilde{m})$.

Детектирование

Среднее число фотонов, попадающее на детектор одиночных фотонов за время ΔT, определяется суммой средних чисел фотонов всех спектральных компонентов:

$$n_{ph}(\phi_A,\phi_B) = \mu_0\left(1 - J_0^2(\widetilde{m})\right)\gamma(L) + \vartheta\mu_0 J_0^2(\widetilde{m})\gamma(L) =$$

$$\mu_0\gamma(L)\left(1-(1-\vartheta)J_0^2(\widetilde{m})\right). \qquad (3)$$

Поскольку $n_{ph} \ll 1$, принимая во внимание типично большие оптические потери в квантовом канале, воспользуемся теорией Л. Манделя [10], описывающей вероятность срабатывания детектора одиночных фотонов за временное окно ΔT в линейном приближении:

$$P_{det}(\phi_A,\phi_B) = \eta_D n_{ph}(\phi_A,\phi_B) + \gamma_{dark}\Delta T, \qquad (4)$$

где η – квантовая эффективность детектора, γ_{dark} – частота темновых срабатываний детектора (ложных срабатываний). Обозначим вероятность темнового отсчета в виде $p_{dark} = \gamma_{dark}\Delta T$.

Информационная модель системы

Пропускная способность канала

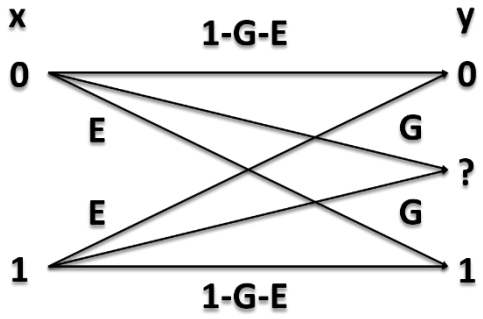


Рисунок 2 – Схема симметричного марковского двоичного канала со стиранием и ошибкой

Обозначения на Рисунке 2: x – событие посылки отправителем бита в канал («0» или «1»), y – события, соответствующие результату измерения получателя («0», «1» и «?», где последний символ обозначает неопределенный результат измерения, вызванный отсутствием срабатывания детектора), $G = P(?|0) = P(?|1)$ – вероятность получения неопределенного результата (стирания), $E = P(0|1) = P(1|0)$ – вероятность инверсии бита (ошибки).

Информационная пропускная способность (или емкость) квантового канала может быть описана в терминах классическо-квантового симметричного марковского двоичного канала со стиранием и ошибкой [11]. Структура канала полностью определяется матрицей условных вероятностей $P(y|x)$, где x – событие посылки отправителем бита в канал («0» или «1») с соответствующей вероятностью $P(x)$ (равной 1/2), y – события, соответствующие результату измерения получателя («0», «1» и «?», где последний символ обозначает неопределенный результат измерения, например, отсутствие срабатывания детектора) с соответствующими вероятностями $P(y)$. Обозначим условную вероятность получения неопределенного результата измерения получателем – G, а условную вероятность неверного измерения бита (результат измерения – бит «1» вместо посланного бита «0», и наоборот) – E, схема квантового канала указана на Рисунке 2. Пропускная способность канала описывается взаимной информацией $I(x;y)$, которая в свою очередь выражается из энтропии вероятности результатов измерений $H(y)$ и условной энтропии $H(y|x)$:

$$I(x;y) = H(y) - H(y|x) \qquad (5)$$

Зная $P(y|x)$ и $P(x)$, легко найти $P(y)$ и далее энтропию:

$$H(y) = -\sum_y P(y)\log_2 P(y) = -(1-G)\log_2\left(\frac{1-G}{2}\right) - G\log_2 G, \qquad (6)$$

и условную энтропию:

$$H(y|x) = -\sum_x P(x) \sum_y P(y|x) \log_2 P(y|x) =$$

$$-(1-G-E)\log_2(1-G-E) - G\log_2 G - E\log_2 E \qquad (7)$$

Таким образом, представим вывод выражения, описывающего пропускную способность квантового канала:

$$I(x;y) = -(1-G)\,log_2\left(\frac{1-G}{2}\right) + (1-G-E)\,log_2(1-G-E) + E\,log_2(E)$$

$$= (1-G) - (1-G)\,log_2(1-G) + (1-G-E)\,log_2(1-G-E) + E\,log_2(E)$$

$$= (1-G)\left(1 - log_2(1-G) + \frac{1-G-E}{1-G} log_2(1-G-E) + \frac{E}{1-G} log_2(E)\right)$$

$$= (1-G)\left(1 + \frac{1-G-E}{1-G} log_2\left(\frac{1-G-E}{1-G}\right) + \frac{E}{1-G} log_2\left(\frac{E}{1-G}\right)\right)$$

$$= (1-G)\left(1 - h\left(\tfrac{E}{1-G}\right)\right) = (1-G)\big(1-h(Q)\big) \qquad (8)$$

где

$$h(Q) = -Q\log_2 Q - (1-Q)\log_1(1-Q) \qquad (9)$$

– функция бинарной энтропии, Q – коэффициент квантовых ошибок, являющийся основополагающим параметром, характеризующим работу системы. Стоит отметить то обстоятельство, что Q появляется в выражении (8) естественным образом. Таким образом, пропускная способность квантового канала состоит из двух множителей: $1-G$ определяет вероятность срабатывания детектора (и в конечном счете скорость генерации сырого ключа[1]), $1-h(Q)$ определяет уменьшение длины ключа за счет публичного оглашения части бит (избыточности) $h(Q)$ (в асимптотическом пределе) для исправления Q ошибок в ключе.

[1] От англ. raw key, т. е. последовательность бит после первого этапа протокола (распределение квантовых состояний).

Оценка перехваченной информации

Как было уже сказано ранее, подробное описание оценки потенциально перехваченной информации о формируемом ключе не входит в рассмотрение данной лабораторной работы. Однако для полной картины работы протокола КРКБЧ введем понятие границы Холево. Это граница сверху на классическую информацию, содержащуюся в некоторой квантовой системе. Для фазомодулированных состояний она определяется следующим образом:

$$\chi = h\left(\tfrac{1-e^{-2\mu}}{2}\right) \qquad (10)$$

где μ – среднее число фотонов на боковых частотах.

Объединенная модель

Выразим условную вероятность получения неопределенного результата измерения получателем G и условную вероятность неверного измерения бита E через вероятность срабатывания детектора одиночных фотонов $P_{det}(\phi_A, \phi_B)$:

$$E = P_{det}(0, \pi \pm \Delta\phi), \quad (11)$$

$$1 - G - E = P_{det}(0, \pm\Delta\phi), \quad (12)$$

где $\Delta\phi$ – среднее отклонение фазы модулирующего сигнала ввиду неидеальности системы синхронизации. Справедливость выражений (11) и (12) может быть подтверждена рассмотрением простого примера. Допустим, отправитель выбрал $\phi_A = 0$. У получателя обнаружится ошибка, если он выберет противоположную фазу $\phi_B = \pi$, но его детектор сработает.

Аналогично, получатель верно декодирует бит, если, выбрав $\phi_B = 0$, его детектор сработает.

Таким образом, коэффициент квантовых ошибок Q выражается в следующей форме:

$$Q = \frac{E}{1-G} = \frac{P_{det}(0,\pi \pm \Delta\phi)}{P_{det}(0\pi \pm \Delta\phi)+P_{det}(0,\pi \pm \Delta\phi)} = \frac{1-V}{2}, \quad (13)$$

где V – видность, еще одна важная характеристика, по которой можно оценить ожидаемый средний уровень коэффициента квантовых ошибок еще на моменте отладки системы, определяемая в виде:

$$V\frac{P_{det}(0 \pm \Delta\phi)-P_{det}(0,\pi \pm \Delta\phi)}{P_{det}(0 \pm \Delta\phi)+P_{det}(0,\pi \pm \Delta\phi)}. \quad (14)$$

Таким образом, скорость генерации секретного[2] ключа будет определяться следующим выражением:

$$K = F\,(1 - G)\,(1 - h(Q) - \chi), \quad (15)$$

где $F = \frac{1}{\Delta T}$ – частота посылок.

[2] В действительности это не совсем так, однако в рамках данной лабораторной работы будем предполагать наиболее простой случай – граница Холево учитывает всю перехваченную информацию.

Приближения

Учитывая все представленные в разделах выше преобразования, получаем:

$$P_{det}(0, \pm\Delta\phi) = \eta_D\mu_0\gamma(L)(1 - (1 - \vartheta)J_0^2(2m\,cos(\Delta\phi/2))) + p_{dark}, \quad (16)$$

$$P_{det}(0, \pi \pm \Delta\phi) = \eta_D\mu_0\gamma(L)(1 - (1 - \vartheta)J_0^2(2m\,sin(\Delta\phi/2))) + p_{dark} \quad (17)$$

Предположим, значение индекса модуляции малым ($m \ll 1$ и $\mu_0 \gg \mu$), тогда применимы следующие приблизительные значения:

$$J_0^2(m) \approx 1 - \frac{m^2}{2}, \quad (18)$$

следовательно,

$$\mu = \mu_0\left(1 - J_0^2(m)\right) \approx \mu_0 \frac{m^2}{2} \quad (19)$$

$$\mu_0 J_0^2(m) \approx \mu_0 \left(1 - \frac{m^2}{2}\right) \approx \mu_0 - \mu \approx \mu_0 \quad (20)$$

Тогда

$$P_{det}(0, \pm \Delta\phi) = \eta_D \gamma(L)(4\mu \cos^2(\Delta\phi/2) + \vartheta\mu_0) + p_{dark}, \quad (21)$$

$$P_{det}(0, \pi \pm \Delta\phi) = \eta_D \gamma(L)(4\mu \sin^2(\Delta\phi/2) + \vartheta\mu_0) + p_{dark}, \quad (22)$$

Типичные значения параметров

1. η_D: от 10 до 25 %;
2. α: от -0.22 до -0.18 дБ/км;
3. β: от -10 до -5 Дб;
4. ϑ: от 10^{-3} до 10^{-2};
5. μ: от 0.1 до 0.2;
6. μ_0: от 4 до 20;
7. $\Delta\phi$: от 1° до 10°;
8. γ_{dark}: от 1 до 1000 Гц;
9. F: от 100 до 500 МГц.

Ход работы, первая часть

1. Получите график спектра монохроматического сигнала. Подберите значение частоты сигнала ω таким образом, чтобы линия спектра находилась посередине графика.
2. Получите график спектра фазомодулированного сигнала. Подберите значения индекса модуляции m и частоты модулирующего сигнала Ω таким образом, чтобы боковые пики были отчетливо видны и не были расположены слишком далеко от центрального.
3. Далее по полученному графику найдите значение первой боковой частоты $\omega + \Omega$.
4. Получите график зависимости мощности бокового сигнала $|A_0 J_n(m)|^2$ от индекса модуляции m. Убедитесь, что второй график пропорционален первому (с точностью до множителя, определяемого параметрами дискретного преобразования Фурье), что свидетельствует о том, что представленные в методическом указании выражения верно описывают процесс модуляции.
5. Получите график спектра фазомодулированного сигнала для разных значений фазы повторной модуляции ϕ_B, например $0, \pi/2, \pi$.
6. Получите график зависимости мощности бокового сигнала от

разности фаз модулирующих сигналов. Убедитесь, что второй график пропорционален первому (с точностью до множителя, определяемого параметрами дискретного преобразования Фурье), это свидетельствует о том, что представленные в методическом указании выражения верно описывают процесс модуляции.

Ход работы, вторая часть

1. Выведите выражения для Q и V, подставив в выражения (13) и (14) выражения (21), (22) и упростив, представьте их в отчете.
2. Выберете по одному типичному значению параметров и постройте графики зависимости V, Q и K от длины квантового канала L, для последней зависимости рекомендуется использовать логарифмический масштаб по оси ординат. Построенные зависимости и выбранные значения параметров представьте в отчете, также представьте значения максимальной скорости генерации ключа при $L = 0$, а также максимальной дальности, при которой $K = 0$.
3. Постройте графики V, Q и K в зависимости от любого другого параметра, полагая $L = 0$, для последней зависимости также рекомендуется использовать логарифмический масштаб по оси ординат. Сделайте вывод о характере полученной вами зависимости, о том, как варьирование выбранного параметра может сказаться на производительности системы КРКБЧ. Построенные зависимости и вывод о характере полученной вами зависимости представьте в отчете.

Методические указания

Для математического моделирования рассматриваемых процессов и построения графиков зависимостей при выполнении данной лабораторной работы необходимо использовать программные пакеты Wolfram Mathematica, версии не ниже 11.3.

Содержание отчета:

1. Цель и задачи.
2. Краткое содержание теории.
3. Ход работы, первая часть (включая необходимые графики и расчеты).
4. Ход работы, вторая часть (включая необходимые графики и расчеты).
5. Выводы по проделанной работе.

Список литературы

1. MD Eisaman, J Fan, A Migdall, and SV Polyakov. Invited review article: Single-photon sources and detectors. *Review of scientific instruments*, 82(7):071101, 2011.
2. M Lucamarini, KA Patel, JF Dynes, B Frohlich, AW Sharpe, AR Dixon, ZL Yuan, RV Penty, and AJ Shields. Efficient decoy-state quantum key distribution with quantified security. *Optics express*, 21(21):24550–24565, 2013.
3. M Lucamarini, ZL Yuan, JF Dynes, and AJ Shields. Overcoming the rate–distance limit of quantum key distribution without quantum repeaters. *Nature*, 557(7705):400, 2018.
4. B Frohlich, M Lucamarini, JF Dynes, LC Comandar, WWS Tam, A Plews, AW Sharpe, Z Yuan, and AJ Shields. Long-distance quantum key distribution secure against coherent attacks. *Optica*, 4(1):163–167, 2017.
5. J-M Merolla, YT Mazurenko, and J-P Goedgebuer. Quantum gryptography using frequency modulation of weak ligh pulses. In *Technical Digest. 1998 EQEC. European Quantum Electronics Conference (Cat. No. 98TH8326)*, pages 101–101. IEEE, 1998.
6. J-M Merolla, YT Mazurenko, J-P Goedgebuer, and WT Rhodes. Single-photon interference in sidebands of phase-modulated light for quantum cryptography. *Physical review letters*, 82(8):1656, 1999.
7. J-M Merolla, YT Mazurenko, J-P Goedgebuer, L Duraffourg, H Porte, and WT Rhodes. Quantum cryptographic device using single-photon phase modulation. *Physical review A*, 60(3):1899, 1999.
8. J-M Merolla, YT Mazurenko, J-P Goedgebuer, H Porte, and WT Rhodes. Phase-modulation transmission system for quantum cryptography. *Optics letters*, 24(2):104–106, 1999.
9. AV Gleim, VI Egorov, Yu V Nazarov, SV Smirnov, VV Chistyakov, OI Bannik, AA Anisimov, SM Kynev, AE Ivanova, RJ Collins, SA Kozlov, and GS Buller. Secure polarization-independent subcarrier quantum key distribution in optical fiber channel using bb84 protocol with a strong reference. *Optics express*, 24(3):2619–2633, 2016.
10. L Mandel and E Wolf. *Optical coherence and quantum optics*. Cambridge university press, 1995.
11. TM Cover and JA Thomas. *Elements of information theory*. John Wiley & Sons, 2012.

Лабораторная работа №9

КВАНТОВЫЙ ГЕНЕРАТОР СЛУЧАЙНЫХ ЧИСЕЛ

Цель работы: Изучение свойств квантового генератора случайных чисел (КГСЧ).

Задачи, решаемые в работе

1. Изучение генерации случайных последовательностей основанной на квантовых эффектах
2. Изучение влияния паразитных шумов на энтропию квантового генератора случайных чисел

Сведения из теории

Физические генераторы недетерминированных случайных чисел используют в качестве источника энтропии хаотическое поведение сложных физических систем. Такие генераторы нашли широкое применение в ряде приложений, в которых детерминированные источники случайных последовательностей, например, генераторы псевдослучайных последовательностей, не могут быть использованы. К таким приложениям относятся криптографические системы, системы аутентификации и др.

Применение источников энтропии, построенных на основе эффектов квантовой оптики, является одним из наиболее перспективных подходов к построению генераторов последовательностей недетерминированных случайных чисел [1-3], что обеспечивается фундаментальной вероятностной природой квантовых процессов.

В лабораторной работе предлагается изучить работу квантового генератора случайных чисел, основанного на флуктуациях вакуума [1]. Принципом работы данного типа генераторов 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) данные 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. Полученный при этом итоговый сигнал является квантовым шумом, который можно при помощи последующей обработки (ПО) преобразовать в случайную последовательность (СЧ). Основным преимуществом данной схемы является измерение квантовых состояний при помощи классических детекторов, что достигается за счет использования гомодинного детектирования.

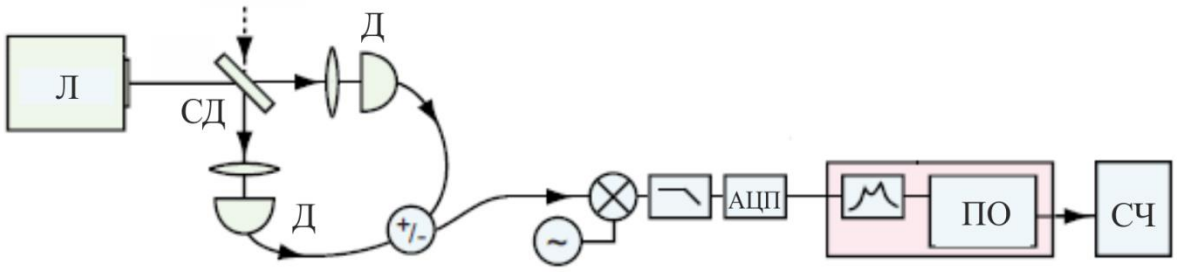


Рисунок 1 — Схема КГСЧ, основанного на флуктуациях вакуума [1].

Квантовый шум имеет нормальное распределение. Распределение наблюдаемого шума является суммой электронного и квантового шумов, оно характеризуется дисперсией и, вследствие независимости электронного и квантового шумов, она может быть представлена в виде

$$\sigma_M^2 = \sigma_E^2 + \sigma_Q^2, \quad (1)$$

где σ_Q^2 – дисперсия квантового сигнала; σ_E^2 – дисперсия электронного шума.

Одной из важнейших характеристик системы является характеристика детектора, определяющая отношение электронного и квантового шумов. Это отношение выражено в виде

$$QCNR = 10 \cdot \log_{10}(\sigma_M^2/\sigma_E^2). \quad (2)$$

Аналогично измеряемому шуму, битовая последовательность, полученная путем измерения лазерного излучения с помощью балансного детектора и оцифровки на аналогово-цифровой преобразователь (АЦП), тоже распределена по нормальному закону.

Максимальная случайность, которая может быть извлечена из последовательности, характеризуется минимальной энтропией (Энтропия Реньи). Учитывая, что классическая составляющая шума может быть скомпрометирована, величина квантовой случайности характеризуется условной энтропией, она учитывает возможность нарушителя использовать классический шум для управления генератором. Было показано, что условная энтропия может быть рассчитана по следующей формуле:

$$H_\infty(M|E) = -\log_2\left(max\left(\frac{1}{2}\left(\mathrm{erf}\left(\frac{e_{max}-R+3\delta/2}{\sqrt{2}}\right)+1\right)\right),\left(\mathrm{erf}\left(\frac{\delta}{2\sqrt{2}}\right)\right)\right), \quad (3)$$

где e_{max} – максимальное значение электронного шума, R – диапазон АЦП, $\delta = R/2^{n-1}$– разрешение АЦП; n – число бит АЦП.

Ход работы

Работа выполняется с использованием экспериментального стенда. Установка аналогична представленной на Рис. 1. В работе предлагается исследовать шумы КГСЧ и оценить влияние классического шума на результат

работы генератора. Для этого необходимо вычислить значения *QCNR* и *H*, используя экспериментально полученные данные.

Для определения характеристик классического шума необходимо подключить к генератору осциллограф и зафиксировать значения уровня шума за произвольный промежуток времени при выключенном лазере. Наблюдаемый шум является классическим электронным шумом. Предлагается зафиксировать величину дисперсии классического шума σ_E^2. После этого на вход светоделителя подается мощность и фиксируются значения уровня шума за произвольный промежуток времени для пяти произвольных значений мощности лазера. По полученным данным нужно вычислить дисперсию квантового шума σ_Q^2 и значения *QCNR*. Для вычисления энтропии необходимо определить среднее и максимальное значение электронного шума, *R* принять равным единице, $n = 8$. Необходимо вычислить условную энтропию КГСЧ для двух значений классического шума.

Содержание отчета:

1. Цель и задачи.
2. Краткое содержание теории.
3. Рисунки используемых схем.
4. Величина дисперсии классического шума, дисперсия квантового шума для пяти значений мощности лазера, дисперсия квантового шума, значение отношения электронного и квантового шумов, значение условной энтропии
5. Вывод по проделанной работе.

Контрольные вопросы

1. Что используют в качестве источника энтропии физические КГСЧ?
2. Каков принцип работы КГСЧ, основанного на флуктуациях вакуума? Что является основным её преимуществом?
3. Что характеризует минимальная энтропия?

Список литературы

1. Symul, T. Real time demonstration of high bitrate quantum random number generation with coherent laser light / T. Symul, S. M. Assad, P. K. Lam. // Appl. Phys. — 2011. — V 98. — P. 3.
2. An ultrafast quantum random number generator with provably bounded output bias based on photon arrival time measurements / Wahl M. [et al.] // Applied Physics Letters. —2011. — 98. — P. 171105.
3. A fast and compact quantum random number generator /T. Jennewein, U. Achleitner [et.al.]. // Sci. Instrum. — 1999. — V 8. — P. 23. 71(4), 1675–1680 (2000)

А.А. Гайдаш, Б.А. Наседкин, Э.О. Самсонов, С.В. Савельева

Квантовые технологии

Учебно-методическое пособие

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

Редакционно-издательский отдел
Университета ИТМО
197101, Санкт-Петербург, Кронверский пр., 49