ОПТИКА И СПЕКТРОСКОПИЯ. ЛАЗЕРНАЯ ФИЗИКА

Оптический симулятор квантового распределения ключей

Л. В. Бигуаа,[1,*] С. П. Кулик[1]

[1] *Московский государственный университет имени М. В. Ломоносова, физический факультет, кафедра квантовой электроники, Центр квантовых технологий*
Россия, 119991, Москва, Ленинские горы, д. 1, стр. 2

(Поступила в редакцию 15.02.2026; после доработки 16.03.2026; подписана в печать 23.03.2026)

В статье предложена методология построения и работы оптической системы для численного и экспериментального исследования систем квантового распределения ключей (КРК). Система позволяет моделировать и экспериментально реализовывать различные атаки на известные протоколы КРК в режиме plug-and-play. Отличительной особенностью системы является то, что в ней используются лишь стандартные лабораторные инструменты, такие как диодные лазеры и фотодиодные детекторы общего назначения. Это позволяет демонстрировать работу системы КРК без необходимости развертывания дорогостоящей и технически сложной полноценной системы КРК в истинно квантовом режиме. Такая парадигма представляется полезной для различных исследований систем КРК в контексте их интенсивного развития. Во-первых, это связано с нарастающей потребностью в численном моделировании систем КРК в исследовательских целях. Во-вторых, экспериментальная реализация предлагаемого подхода необходима для практической демонстрации функционирования систем КРК, в частности при подготовке специалистов в области квантового шифрования. При этом существующие в настоящее время аналоги позволяют исследователям экспериментально воспроизводить только простейшие атаки злоумышленника (Евы) на протоколы КРК, такие как приём–перепосылка. С их помощью также возможно численно моделировать широкий спектр атак, но с использованием достаточно сложных систем проектирования. В отличие от этого предлагаемая система позволяет как численно, так и экспериментально воспроизводить атаки, начиная с простейших и заканчивая технически сложными атаками, такими как атака с отщеплением фотонов, для использования в режиме plug-and-play.

PACS: 03.67 Dd, 03.67 -a, 03.67 Hk. УДК: 53.06, 53.072, 535.8
Ключевые слова: квантовое распределение ключей, численная симуляция, атака, протокол КРК.

DOI: 10.55959/MSU0579-9392.81.2620402

ВВЕДЕНИЕ

Квантовая криптография — наиболее развитая отрасль квантовых технологий. Имеется большое число обзоров, в которых излагаются физические основы и примеры реализаций соответствующих схем [1], из которых выделим не теряющий актуальность обзор 2002 г. сотрудников группы Николя Жизана и др. [2]. В настоящее время существует множество проектов по разработке и исследованию квантовых систем распределения ключей [3], которые являются важным компонентом технологий квантового интернета (КИ) [4]. Более того, появилось множество коммерчески доступных систем квантового распределения ключей (КРК), например в Японии [5], России [6, 7], США [8], Великобритании [9], Китае [10], Швейцарии [11]. Одним из ключевых элементов в разработке таких технологий является необходимость численного моделирования систем КРК для анализа их свойств. В целом этот процесс заключается в оценке количества получаемой Евой информации для различных типов атак на исследуемый протокол, а также влияние различных инструментальных несовершенств на секретность получаемого ключа. Для этих целей было создано несколько типов численных симуляторов. Во-первых, можно выделить универсальный коммерческий пакет, такой как Ansys Interconnect platform [12]. Такая система позволяет исследователю виртуально собрать практически любую оптическую установку из реалистичных компонентов. Основная проблема в использовании такого программного обеспечения (ПО) лишь для узкоспециализированных задач, связанных только с КРК, например, заключается в сложности. Для использования такого ПО от исследователя требуется прохождение специальных курсов. Концептуально это сильно отличается от plug-and-play подхода. Под последним подразумевается, что пользователь может начать работу с системой непосредственно, без подготовки, сразу после её включения и простейшей базовой настройки. Также нужно отметить, что система Ansys не позволяет использовать еще неразработанные оптические компоненты, такие как полноценные схемы невозмущающих измерений для изучения атак с отщеплением фотонов (PNS).

В качестве шага на пути к реализации plug-and-play идеи был предложен второй тип симуляторов. Они позволяют исследователю смодели-

* E-mail: leon.006w@yandex.ru

ровать сложную систему КРК [13, 14], но при этом здесь практически не рассматривается влияние Евы. В результате были также созданы узкоспециализированные системы, способные имитировать как протоколы КРК, так и некоторые атаки [15–24]. Слабым местом здесь является достаточно ограниченное количество доступных протоколов, инструментальных несовершенств и атак для исследования. Как правило, рассматривается только простейшие атаки Евы на подобии приёма–перепосылки. Альтернативный способ исследования протоколов КРК и атак заключается в написании исследователем собственного ПО с использованием специализированных библиотек для компьютерного моделирования [25–27]. Это решение значительно сложнее из-за необходимости написания программного кода компонентов всей системы, таких как источник света, детекторы и модель влияния Евы. Таким образом, актуальной на сегодня задачей является создание универсальной системы работающей на основе принципов plug-and-play, которая могла бы моделировать как основные протоколы КРК, так и разнообразные и нетривиальные атаки для анализа распределенного секретного ключа в реалистичных условиях (например, при различных несовершенствах оборудования).

Другим ключевым компонентом в разработке систем КРК является необходимость экспериментальной реализации протоколов КРК в сочетании с различными атаками на них. Помимо существующего многообразия реализуемых сегодня коммерческих систем КРК, проводится также и множество исследований посвященных реализации различных атак. Например, это атаки типа fake-state [28] [29]; повреждение детекторов Боба лазерным импульсом Евы высокой интенсивности [30] [31]; увеличение количества фотонов в импульсе Алисы для обхода метода состояний-ловушек [32]; исследования влияния атмосферной турбулентности на эффективность проведения атаки «приём–перепосылка» [33]. Таким образом, по мере того, как различные типы атак и систем КРК становятся реальностью, важно иметь возможность продемонстрировать их специалистам в области квантовой криптографии. В частности, это необходимо при обучении специалистов для развития их понимания реального эксперимента со всеми его особенностями. Использование полноценной системы КРК для решения этой задачи, как правило, является очень дорогостоящим способом, а также технически сложной задачей. Более того, существующая теоретико-экспериментальная база не позволяет реализовать некоторые системы. Например, сегодня не существует способа [34] экспериментально воспроизвести PNS-атаку [35]. Для решения в какой-то степени этих проблем были предложены различные решения [36] [24] [37]. Такие системы позволяют исследователю воспроизвести основные протоколы КРК и некоторые атаки на них, используя стандартные лабораторные инструменты, такие как диодные лазеры и фотодиодные детекторы общего назначения. Основная идея, лежащая в основе этих систем, заключается в использовании изоморфизма между оптическими преобразованиями классических электрических полей света, проходящего через систему, и гейзенберговской эволюцией соответствующих операторов уничтожения.Таким образом, можно однозначно сопоставить результаты измерений, полученные с помощью фотодиодных детекторов и диодных лазеров, с результатами, которые были бы получены с помощью однофотонных детекторов и источников света, использующих ту же оптическую установку. Тем не менее существующие демонстрационные системы позволяют исследователю воспроизвести лишь достаточно небольшой класс атак на основные протоколы КРК, такие как приём–перепосылка или атака с двойным отсчетом на детекторах Боба [38]. Кроме того, они не подходят для кодирования кубитов по времени.

Чтобы решить все упомянутые проблемы в рамках единой платформы, основанной на принципе plug-and-play, был разработан оптический симулятор КРК, который представлен в этой статье. Этот симулятор позволяет исследователю численно и экспериментально воспроизвести большое число протоколов КРК, а также широкий спектр атак, начиная от атаки «приём–перепосылка» до технически сложных PNS-атак. Система главным образом ориентирована для применения распространенного поляризационного кодирования кубитов. Но она также может быть использована в пространственной двухмодовой кодировке или во временной кодировке кубитов.

1. ПРИНЦИПЫ РАБОТЫ СИМУЛЯТОРА

Концептуальная схема предлагаемого симулятора представлена на рис. 1.

Центральным элементом управления всей установкой является персональный компьютер (ПК), на котором установлено специальное программное обеспечение (ПО). ПК подключен к цифроаналоговому преобразователю (ЦАП). Отправляя сигнал на ЦАП, ПО может включать или выключать диодный лазер в начале схемы для работы в непрерывном или импульсном режиме. В предлагаемой схеме лазер работает в диапазоне длин волн, видимом невооруженным глазом. Это позволяет исследователю проследить путь лазерного луча через всю систему, что делает происходящее в ней процессы особенно наглядными. Далее, на оптическом пути лазерного луча имеются три слота, предназначенные для поляризатора (1) и пары поляризаторов того же типа (2). Первый поляризатор необходим для фильтрации линейной вертикальной (или горизонтальной) поляризации лазерного излучения. Вторую пару поляризаторов можно использовать как для задания регулируемых оптических потерь в схеме, поворачивая один поляризаторов на разные углы. Следующие два слота предназначены для полуволновой (3) и четвертьволновой (4) оптических фазовых

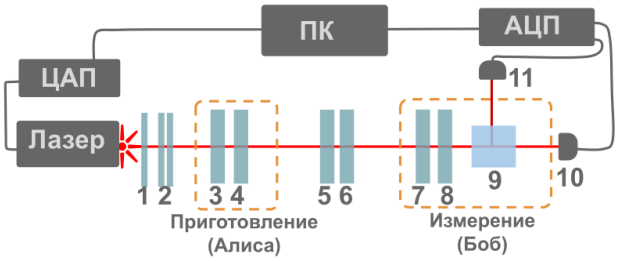

Рис. 1. Базовая схема рассматриваемого оптического симулятора: ПК — персональный компьютер, который через ЦАП посылает сигнал на включение/выключение лазерного излучения; 1, 2 — пара поляризаторов, расположенных на оптическом пути лазерного луча; 3, 4 — полуволновая (ПВП) и четвертьволновая (ЧВП) фазовые пластинки для приготовления произвольного состояния поляризации света; 5, 6 — те же фазовые пластинки для воспроизведения фазового шума в канале связи; 7, 8 — фазовые пластинки для выбора произвольного базиса измерения состояний поляризации. Вместе с поляризационным светоделителем 9 они перекодируют поляризационные моды света в пространственные. Состояние света в пространственных модах легко измеряется с помощью фотодиодных детекторов 10, 11, сигналы с которых передаются на ПК через АЦП. Каждый оптический элемент может быть извлечен/заменен в слоте, в котором он установлен

пластинок, которые можно повернуть для получения любого состояния поляризации лазерного излучения. Описанная часть установки служит в качестве станции Алисы. За ней следуют слоты для полуволновой (5) и четвертьволновой (6) фазовых пластинок. Эта область соответствует квантовому каналу связи. Вращая эти пластинки, можно создать произвольное поляризационное преобразование состояния света, проходящего по каналу, воспроизводя таким образом эффект фазового шума. Оставшаяся часть оптической схемы соответствует измерительной части Боба. Она начинается со слотов для установки четвертьволновой (7) и полуволновой (8) фазовых пластинок, которые позволяют измерять поляризацию входного светового состояния в произвольном базисе. Затем установлен поляризационный светоделитель (9), отражающий вертикально поляризованный свет в фотодиодный детектор (11) и пропускающий горизонтально поляризованные состояния в направлении фотодиодного детектора (10). Во время измерений фотодиодные детекторы Боба генерируют аналоговый сигнал, который оцифровывается на аналого-цифровом преобразователе АЦП и передается на ПК. Затем ПО математически обрабатывает эти сигналы так, чтобы воспроизвести различные квантовые режимы работы установки, как описано в оставшейся части этого раздела. ПО также можно переключить в режим численного моделирования, как описано в конце раздела. В этом случае работа проводится лишь численно и ПО заменяет реальные лазерные импульсы Алисы на симулированные, рассчитывая измеряемую мощность излучения на детекторах. В последующих разделах в систему также вводится Ева.

Рассмотрим теперь, как можно связать предлагаемую первоначально классическую установку с такой же установкой, но оснащенной однофотонными источниками и однофотонными детекторами. Начнем с классической картины эволюции электромагнитного поля света. Допустим, Алиса испускает световой импульс. Для простоты и без потери общности можно ограничиться рассмотрением лишь электрического поля. Вектор электрического поля $\mathbf{E}^A$ импульса в некоторой точке вблизи оптической оси системы, непосредственно после прохождения поляризатора (1), описывается вектором комплексных амплитуд:

$$\mathbf{E}^A = \begin{pmatrix} E_V^{\mathrm{A}} \\ E_H^{\mathrm{A}} \\ E_{Env}^{\mathrm{A}} \end{pmatrix}, \tag{1}$$

где E_H/E_V представляет собой комплексную амплитуду поля в горизонтальной/вертикальной поляризации и лишь одна из них отлична от нуля из-за действия поляризатора (предположим, $E_V^A \neq 0$); E_{Env} соответствует воображаемой вспомогательной моде, которая описывает потери энергии электрического поля при распространении импульса. Эта мода введена для рассмотрения эволюции поля унитарным образом. Когда свет достигает поляризационного светоделителя 9 (рис. 1) с результирующим вектором электрического поля $\mathbf{E}' = V_0\mathbf{E}^A$, светоделитель отображает поляризационные моды света в пространственные $\mathbf{E}^B = V_1\mathbf{E}'$, где $\mathbf{E}^B$:

$$\mathbf{E}^B = \begin{pmatrix} E_1^{\mathrm{B}} \\ E_2^{\mathrm{B}} \\ E_{Env}^{\mathrm{B}} \end{pmatrix}, \tag{2}$$

здесь E_1/E_2 представляет собой 1-ю/2-ю пространственную моду в которой расположены фотодиоды 10 и 11 на рис. 1. Теперь воспользуемся этим же формализмом для описания соответствующей гейзенберговской эволюции вектора операторов уничтожения $\hat{\mathbf{a}}^A$:

$$\hat{\mathbf{a}}^A = \begin{pmatrix} \hat{a}_V^A \\ \hat{a}_H^A \\ \hat{a}_{Env}^A \end{pmatrix}. \tag{3}$$

Этот вектор связан с соответствующим вектором $\hat{\mathbf{a}}'$ непосредственно перед светоделителем, как известно, через ту же унитарную матрицу V_0, что и ранее. Тем же образом получается вектор $\hat{\mathbf{a}}^B$ в пространственной кодировке на стороне Боба посредством соотношения:

$$\hat{\mathbf{a}}^B = V_1\hat{\mathbf{a}}' = V\hat{\mathbf{a}}^A, \tag{4}$$

где $V = V_1V_0$, а $\hat{\mathbf{a}}^B$:

$$\hat{\mathbf{a}}^B = \begin{pmatrix} \hat{a}_0^B \\ \hat{a}_1^B \\ \hat{a}_{Env}^B \end{pmatrix}. \tag{5}$$

Теперь предположим, что каждый лазерный импульс Алисы состоит только из одного V-поляризованного фотона. Требуется найти результирующую вероятностную статистику количества фотонов света вблизи детекторов Боба. Исходя из этого, используя генератор случайных чисел, ПО экспериментатора сможет воспроизвести фотоотсчёты на стороне Боба. Это позволяет экспериментатору воссоздать измерения количества фотонов света с помощью идеальных многофотонных детекторов Боба (которые регистрируют фотонную статистику без искажений) и таким образом однозначно сопоставить классическую систему её квантовому аналогу. Для этого необходимо заметить, что состояние света на выходе из источника Алисы описывается вектором состояния $\hat{a}_V^{\dagger\,A}|vac\rangle$, где $|vac\rangle$ — кет-вектор вакуумного состояния. Чтобы связать это состояние с измеряемой Бобом статистикой, нужно разложить $\hat{a}^{\dagger\,A}$ по операторам рождения на стороне Боба (5):

$$\hat{a}_V^{\dagger\,A} = v_{00}\hat{a}_0^{\dagger\,B} + v_{01}\hat{a}_1^{\dagger\,B} + v_{02}\hat{a}_{Env}^{\dagger\,B}, \qquad (6)$$

где v_{ij} — матричные элементы V. Теперь, чтобы найти статистику фотоотсчетов на детекторах Боба, нужно определить амплитуды вероятностей $|v_{00}|^2, |v_{01}|^2$ обнаружения фотона на каждом детекторе Боба. Вероятность поглощения фотона в квантовом канале при этом будет $|v_{02}|^2 = 1 - |v_{00}|^2 - |v_{01}|^2$. С этой целью нужно заметить, что классическая эволюция электрического поля описывается с помощью той же зависимости, что и в (4), и можно написать:

$$|v_{00}|^2 = \frac{W_0}{W_{in}}; |v_{01}|^2 = \frac{W_1}{W_{in}}, \qquad (7)$$

где W_k — измеренная мощность света в k-м фотодиоде Боба; W_{in} — измеренная мощность света после первого поляризатора Алисы. Проведенный анализ может быть непосредственно применен к фотонным кубитам в двухканальной пространственной кодировке [39] ввиду эквивалентности обоих кодировок [40]. Для этого экспериментатор должен заменить фазовые пластинки на приготовительной (измерительной) станции Алисы (Боба) интерферометрами Маха–Цендера 2×2. В качестве пространственных мод здесь используются соответствующие плечи интерферометра. Что касается экспериментальной реализации, то исследователь может собрать такую установку в виде простой системы в открытом пространстве из зеркал и неполяризационных светоделителей 50:50 общего назначения. Ввиду упомянутой эквивалентности кубиты с временным кодированием также могут быть реализованы [39]. Но в этом случае нужно расширить вектор выходных операторов Алисы (3) до

$$\hat{\mathbf{a}}^A = \begin{pmatrix} \hat{a}_{0E}^A \\ \hat{a}_{0L}^A \\ \hat{a}_{1E}^A \\ \hat{a}_{1L}^A \\ \hat{a}_{Env}^A \end{pmatrix}. \qquad (8)$$

Здесь $\hat{a}_{0E}^A$ ($\hat{a}_{0L}^A$) является оператором уничтожения фотона, который находится в 1-й пространственной моде и в более раннем (позднем) временном окне E (L). Соответственно $\hat{a}_{1E}^A$ и $\hat{a}_{1L}^A$ — то же самое для 2-й пространственной моды. В этом случае снова предполагается, что Алиса подает свет только в одну моду, скажем, $0E$. Подобно (6), получаем:

$$\hat{a}_{0E}^{\dagger\,A} = v_{00}\hat{a}_{0E}^{\dagger\,B} + v_{01}\hat{a}_{0L}^{\dagger\,B} + \\ + v_{02}\hat{a}_{0E}^{\dagger\,B} + v_{03}\hat{a}_{0E}^{\dagger\,B} + v_{0Env}\hat{a}_{Env}^{\dagger\,B}. \qquad (9)$$

Здесь $\hat{a}_{Env}^{\dagger\,B}$ соответствует оператору рождения фотона вне обозначенных временных окон, в частности поглощению фотонов. Чтобы найти статистику фотоотсчетов во временных окнах Боба, необходимо вычислить амплитуды вероятности $|v_{0k}|^2$ исходя из измеренных Бобом мощностей света с помощью формул (сравните с (7)):

$$|v_{0S}|^2 = \frac{W_{0S}}{W_{in}}; |v_{0L}|^2 = \frac{W_{0L}}{W_{in}} \\ |v_{1S}|^2 = \frac{W_{1S}}{W_{in}}; |v_{1L}|^2 = \frac{W_{1L}}{W_{in}}; \qquad (10)$$

где W_{kS}, W_{kL} — измеренная мощность света в k-й пространственной моде для соответствующих временных окон Боба.

При реализации схемы во временной кодировке также необходимо модифицировать установку оптического симулятора тем же образом, как и для двухканального пространственного кодирования. В частности, самый простой способ сделать это — снова реализовать систему в свободном пространстве. В этом случае исследователь также должен соединить какую-то область канала связи с оптическим волокном, используя оптоволоконный коллиматор, чтобы ввести временную задержку. Чтобы реализовать реалистичные линии задержки с длинной 20–200 см, что эквивалентно временной задержке в 1–10 нс, экспериментатор должен использовать детекторы света способные регистрировать данные в пределах временного окна в 1–10 нс. Соответственно лазер Алисы должен генерировать импульсы короче 1–10 нс, чтобы предотвратить световую интерференцию в системе. Таким образом, временное кодирование требует использования более дорогих компонентов. При этом здесь всё еще отсутствует необходимость использовать дорогие и более сложные в эксплуатации однофотонные устройства.

В свете реализации метода состояний-ловушек и соответствующих атак на него, что рассматривается в разделе ниже, также понадобится источник n-фотонных импульсов. Допустим, что Алиса испускает импульс, состоящий из n-фотонов. Остановимся на поляризационной кодировке кубитов для иллюстрации. Чтобы описать такой импульс, требуется возвести формулу (6) в n-ю степень:

$$[\hat{a}_V^{\dagger\,A}]^n = [v_{00}\hat{a}_0^{\dagger\,B} + v_{01}\hat{a}_1^{\dagger\,B} + v_{02}\hat{a}_{Env}^{\dagger\,B}]^n. \qquad (11)$$

Используя мультиномиальную теорему [41], можно представить (11) в форме:

$$[\hat{a}_V^{\dagger A}]^n = \sum_{n_0+n_1+n_2=n} \binom{n}{n_0, n_1, n_2} v_{00}^{n_0} v_{01}^{n_1} v_{02}^{n_2} \times \\ \times [\hat{a}_0^{\dagger B}]^{n_0} [\hat{a}_1^{\dagger B}]^{n_1} [\hat{a}_2^{\dagger B}]^{n_2}, \quad (12)$$

где $\binom{n}{n_0, n_1, n_2} = \frac{!n}{!n_0!n_1!n_2}$ — мультиномиальный коэффициент [41]. Теперь, чтобы рассчитать образующуюся в результате статистику бозонного сэмплинга на стороне Боба, ПО экспериментатора должно вычислить 3^n амплитуд вероятности:

$$p(n_0, n_1) = \binom{n}{n_0, n_1, n_2} |v_{00}|^{2n_0} |v_{01}|^{2n_1} |v_{02}|^{2n_2}. \quad (13)$$

Заметим, что в (13) были уже учтены нормировочные коэффициенты для операторов рождения

$$\hat{a}^\dagger |n\rangle \longrightarrow \frac{1}{\sqrt{n+1}} |n+1\rangle. \quad (14)$$

Можно видеть, что количество вероятностей (13), которое должно вычислять ПО экспериментатора, растет очень быстро по мере увеличения количества фотонов в импульсе. Чтобы уменьшить вычислительную сложность, можно ограничить количество фотонов в импульсе значением n_{max} без потери общности, если вероятность $p(n)$ появления импульса с $n > n_{max}$ пренебрежимо мала. Для этого нужно отметить, что такие n-фотонные импульсы могут появляться при сегодняшнем состоянии теории КРК только в результате реализации протоколов КРК на основе метода состояний-ловушек [35, 38]. Это означает, что импульс, содержащий в себе n фотонов, возникает лишь в результате редукции волнового вектора ослабленного когерентного импульса Алисы по энергетическому подпространству вследствие вмешательства Евы. Поскольку ослабленные когерентные импульсы имеют пуассоновскую статистику распределения числа фотонов, то можно непосредственно вычислить вероятность $p(n > n_{max}, \mu)$ обнаружения более чем n_{max} фотонов в импульсе со средним количеством фотонов $|\mu|^2$. Максимальное значение вероятности при этом окажется у импульсов с максимальным средним количеством фотонов $|\mu_{max}|^2$. Окончательно, взяв реалистичное значение $\mu_{max} \approx 1$ и зафиксировав $n_{max} = 9$, получим:

$$p(n \geq n_{max}, \mu_{max}) = 1 - \sum_{0 \leq k \leq n_{max}} \frac{\mu^k e^{-\mu}}{!k} \approx 10^{-6}. \quad (15)$$

При этом было проверено, что $3^{n_{max}}$ вероятностей в (15) могут быть вычислены менее чем за 0.1 с на центральном процессоре средней мощности при $n_{max} = 9$.

Отметим, что для обоих типов источников фотонов, 1-фотонного или n-фотонного, можно учесть ограниченную квантовую эффективность η_k каждого k-го идеального многофотонного детектора Боба. Чтобы достичь этого, нужно заменить оптическую мощность W_k, измеренную в k-м детекторе, на $\eta_k W_k$ в формуле (7) [(10)]. Это эквивалентно перекачке некоторой порции световой энергии во вспомогательную моду Env, как описано выше. Теперь предположим, что лазерные импульсы Алисы являются ослабленными когерентными и V-поляризованными, содержащие несколько фотонов $|\mu_V^A|^2$ в среднем. Такое состояние описывается как вектор:

$$\boldsymbol{\alpha}^A = \begin{pmatrix} \alpha_V^A \\ \alpha_H^A \\ \alpha_{Env}^A \end{pmatrix}, \quad (16)$$

где буква «α» описывает собственное значение когерентного состояния в соответствующей моде. Чтобы найти статистику распределения количества фотонов на стороне Боба, необходимо заметить, что соответствующие собственные значения α^B на его стороне связаны с собственными значениями $\boldsymbol{\alpha}^A$ тем же образом, что и комплексные амплитуды электрических полей:

$$\boldsymbol{\alpha}^B = V \boldsymbol{\alpha}^A. \quad (17)$$

Следовательно

$$\mu_0^B = |v_{00}|^2 \mu_V^A; \mu_1^B = |v_{01}|^2 \mu_V^A. \quad (18)$$

Точно так же, как и в предыдущем случае, тут можно учесть ограниченную квантовую эффективность η_k в k-м детекторе Боба.

Как уже упоминалось, ПО можно переключить в режим численного моделирования. В этом случае ПО непосредственно вычисляет матрицу эволюции V (например, см. формулу (4)). С этой целью в нем используются хорошо известные матрицы для каждой фазовой пластинки и поляризационного светоделителя. Используя их, ПО рассчитывает результаты на основе выбранных режимов работы источника света и детекторов.

2. ОПИСАНИЕ РЕЖИМОВ РАБОТЫ ИСТОЧНИКА И ДЕТЕТКТОРОВ

Теперь более подробно обсудим режимы работы источника Алисы и детекторов Боба, предлагаемые для ПО экспериментатора. Здесь частично заимствованы формулы из патента [37]. Для детекторов Боба предлагаются следующие режимы работы:

1. Классический режим, при котором постобработка сигналов с фотодиодов не выполняется. Детекторы показывают бегущие средние значения измеренных в данный момент мощностей света W_0, W_1. Детекторы также могут быть переключены в режим измерения коэффициентов передачи $T_0 = \frac{W_0}{W_{in}}$, $T_1 = \frac{W_1}{W_{in}}$. Они показывают суммарные потери в оптической

мощности, которую испытывает каждая мода светового поля при прохождении через оптическую схему симулятора. При временном кодировании кубитов детекторы показывают, соответственно, четыре значения для каждого временного окна.

2. Многофотонный режим имеет 5 параметров: квантовую эффективность η_k; вероятность темнового отсчета p_k^{dark} каждого детектора; временные задержки $\Delta t_{sync.}$ и Δt_{Eve}; время гейта T. Этот режим доступен только в импульсном режиме источника света. Следовательно, детекторы работают в гейтовом режиме. Теперь предположим, что Алиса испускает световой импульс в момент времени t_{sent}. Для простоты считается, что световые импульсы поступают на детекторы Боба одновременно в момент времени $t_{receive}$. При этом рассматриваются идентичные детекторы, поэтому процесс работы каждого из них описан на рис. 2 единой кривой. В случае разных детекторов и неодновременности прихода импульсов на них достаточно рассмотреть пару таких кривых. Поскольку фактическая квантовая эффективность каждого фотодиода Боба η_{act} зависит от времени, прошедшего с момента открытия гейта, ПО начинает считывать результаты измерений после временной задержки $\Delta t_{sync.}$, как показано на рис. 2. Это предотвращает воздействие обозначенной зависимости на результат измерения. Аналогично результаты измерений не считываются по прошествии времени T, меньшего фактического времени гейта T_{act}. Следовательно, T играет роль длительности гейта.

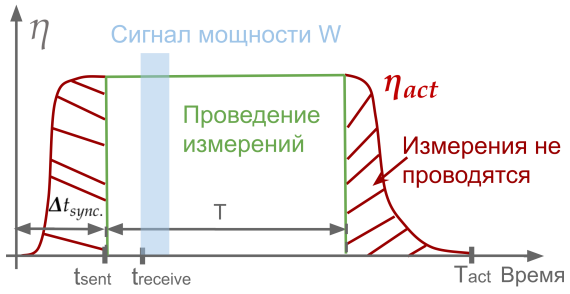

Рис. 2. Схема принципа работы многофотонного детектора

Затем, используя измеренную оптическую мощность на фотодиодах Боба, ПО вычисляет статистическое распределение $p(n_0, n_1)$ вероятности наблюдения n_0 и n_1 фотонов, соответственно, в 1-м и 2-м детекторах Боба. Для этого используется информация о выбранном режиме источника света Алисы. Для простоты рассматриваются поляризационные кубиты. В случае временного кодирования ПО удваивает количество значений для учета разных временных окон измерения. Далее, используя распределение $p(n_0, n_1)$, ПО генерирует фотоотсчёты на каждом многофотонном детекторе Боба с помощью генератора случайных чисел. Для этой цели можно пользоваться геометрической аналогией, в соответствии с которой эти вероятности располагаются вдоль числовой оси в любом удобном порядке: $x_0 = p(0,0)$, $x_1 = p_0 + p(0,1)$, $x_2 = x_1 + p(1,1)$, $x_3 = x_2 + p(1,0)$, ..., $x_N = p(n,0) + x_{N-1}$. За этим следует генерация случайной величины x из равномерного вероятностного распределения в диапазоне от 0 до x_N. Если, для примера, сгенерированное x оказывается в интервале $[x_1, x_2)$, то каждый детектор показывает единичный отсчет. Как объясняется после формулы (15), экспериментатор также может задать произвольную квантовую эффективность $\eta \leq \eta_{act}$ каждого детектора, как показано на рис. 3, *а* зеленой линией.

Можно также реалистично ввести временную задержку Δt_{Eve} во времени прибытия фотона, как это происходит в случае, когда Ева реализует time-shift атаку [38] (см. рис. 3, *б*). Это простой эквивалент более сложного использования физической линии задержки. Конечно, последнее тоже возможно в предложенной схеме, как было указано при обсуждении кодирования фотонов по времени. Кроме того, количество сгенерированных фотоотсчетов на k-м детекторе может быть увеличено за счет темновых шумов в детекторе: с вероятностью p_k^{dark} генерируется 1, также используя геометрическую аналогию, и добавляется 1 к полученным фотоотсчетам.

3. Однофотонный режим имеет тот же набор параметров, что и предыдущий. Он работает таким же образом, но ПО округляет до 1 количество фотоотсчетов, превышающее 1.

4. Режим лавинного однофотонного детектора (APD). Он содержит прежний набор параметров, дополненный несколькими новыми: пороговыми значениями числа фотонов n_{th} и оптической мощности P_{th} падающего на детектор света; также исследователь может напрямую указать зависимость квантовой эффективности детектора от времени $\eta(t)$ (по умолчанию форма прямоугольная (см. рис. 3). Принцип работы такого детектора схематично показан на рис. 4 и основан на реалистичной физической модели таких устройств [42]. Первоначально детектор работает в так называемом режиме Гейгера. В этом случае, при падении фотона на поверхность фотоприёмника, происходит быстрое увеличение тока фотодиода и происходит «отсчёт». Если количество фотонов в этом световом импульсе превышает пороговое значение n_{th}, APD переключается в линейный режим. В этом режиме ток фотодиода линейно возрастает с увеличением оптической мощности падающего на детектор света. Если эта оптическая мощность превыша-

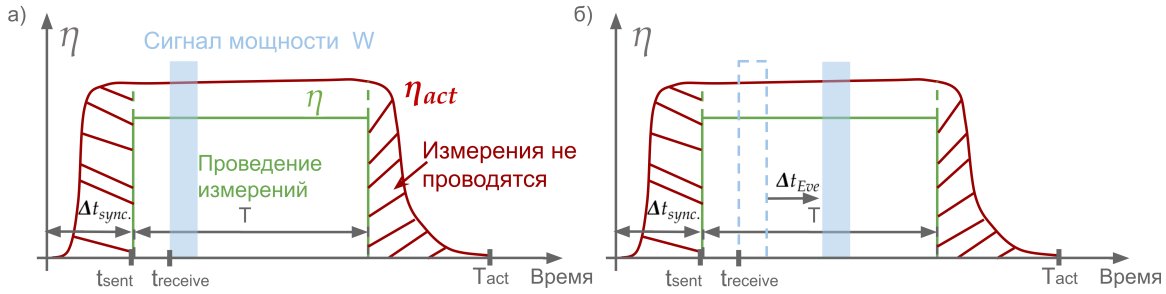

Рис. 3. Схема принципа работы многофотонного детектора из рис. 2, дополненная учетом квантовой эффективности детектора η ($а$) и временной задержкой Δt_{Eve} во времени прибытия фотона на детектор ($б$)

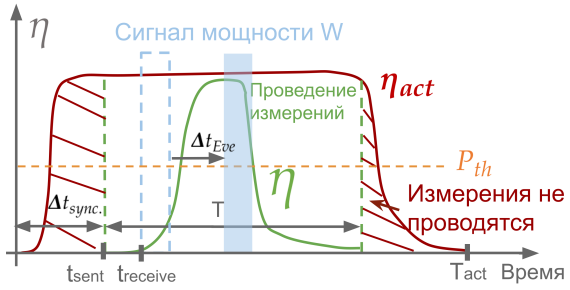

Рис. 4. Схема принципа работы лавинного однофотонного детектора

ет пороговое значение P_{th}, происходит отсчет. В противном случае отсчета не происходит.

Теперь рассмотрим различные режимы работы источника.

1. Классический режим, при котором лазер Алисы может излучать свет непрерывно с постоянной оптической мощностью W_{in} или световые импульсы той же мощности с регулируемой частотой f.

2. Однофотонный импульсный режим, который имеет в качестве параметров: вероятность успешного испускания фотона $p_{emission}$; частота испускания импульсов f; флажок включения постселекции. Параметр $p_{emission}$ введен для реалистичного учета поведения однофотонных источников, которые в настоящее время испускают фотоны с вероятностью, меньшей единицы. Теперь предположим, что постселекция отключена. Если ПО посылает источнику сигнал для создания импульса, фотон испускается с вероятностью $p_{emission}$. При успешном излучении фотона результирующие амплитуды вероятности появления одиночных фотонов $p(n_0, n_1)$ на детекторах Боба вычисляются способом, описанным в предыдущем разделе. В противном случае ПО обнуляет эти амплитуды и регистрируются лишь темновые отсчеты в детекторах Боба. Если параметр постселекции включен, то детекторы регистрируют излучение лишь для событий, при которых излучение имело место. Таким образом, если параметр постселекции включен, то для $p_{emission}$ формально устанавливается значение 1.

3. Многофотонный импульсный режим с частотой f и максимальным числом фотонов n_{max} в качестве параметров. Этот режим работает так же, как и предыдущий, но с тем исключением, что количество фотонов в каждом импульсе может быть больше 1.

Описанные режимы работы источника света могут быть дополнены регулированием оптической фазы импульса. С этой целью исследователю необходимо дополнительно встроить в схему (рис. 1) фазовый модулятор и модулятор интенсивности после лазера, переведенного в режим непрерывного излучения. В качестве фазового модулятора может быть использован простейший оптомеханический модулятор. Самый простой способ реализовать модулятор интенсивности — поворачивать поляризатор.

Если исследователь хочет ввести только фазовый сдвиг между отдельными модами излучения, то в модуляторе интенсивности нет необходимости. Для двухканальной и временной кодировки это достигается установкой оптикомеханического фазового модулятора в нужном плече интерферометра. Что касается поляризационных кубитов, то здесь можно использовать более дорогой электрооптический модулятор.

Рассмотренные режимы работы детекторов и источников всесторонне охватывают широкий набор практических сценариев применения протоколов КРК и возможных атак [38], что детально описывается в следующем разделе. Также следует отметить, что, следуя предложенной методологии, исследователи могут дополнить описанные в этом разделе режимы работы, добавив к ним новые типы детекторов и источников.

3. РЕАЛИЗАЦИЯ ПРОТОКОЛОВ КРК И АТАК

Из схемы предложенного симулятора, приведенной на рис. 1, видно, что все основные протоколы КРК, такие как BB84 [43], B92 [43] [44], SARG04 [45], протокол на 6 состояниях [46] и другие могут

быть реализованы с использованием поляризационных кубитов. Как было описано в предыдущем разделе, при необходимости легко можно использовать кубиты в пространственнной двухканальной и временной кодировках. Теперь добавим в предлагаемую схему Еву. Для большого многообразия атак, основанных на приёме–перепосылке, Ева помещается посередине, как показано на рис. 6.

Такая схема позволяет исследователю воспроизвести все основные атаки на детекторы Боба в рамках каждого протокола, используя предложенные режимы работы лазера и детекторов. В частности, это хорошо известные атаки вида double-click, fake-state и detector blinding [38]. В качестве иллюстрации в случае fake-state атаки Еве необходимо измерить однофотонный импульс Алисы и повторно отправить его как классический высокоинтенсивный импульс с правильно выбранной поляризацией и корректно установленной временной задержкой для детекторов Боба (см. рис. 3). Предложенные режимы работы детекторов также могут быть использованы для атак без Евы посередине, как в случае с time-shift атакой [38]. Здесь Еве просто нужно случайным образом манипулировать задержкой прибытия фотона на детекторы Боба.

Что касается более сложных атак, таких как PNS [35] [38] или laser seeding [32], то здесь делается правдоподобное предположение о том, что исследователя в первую очередь интересует, как произвольная атака повлияет на Боба и как он может быть защищен. Следуя этой идее, Ева рассматривается как черный ящик, внутренняя структура которого полностью игнорируется. Такой черный ящик предлагается использовать для выполнения произвольной однокубитовой атаки, используя схему, показанную на рис. 5.

Теперь предположим, что Алиса испускает импульс, который далее попадает в зону влияния Евы в квантовом канале. Воздействие Евы на проходящий импульс начинается с регистрации его оптической мощности. Основываясь на этом измерении и знаниях исследователя об углах, под которыми повернуты все предшествующие оптические пластинки, Ева неформально знает, какое состояние $|\psi\rangle$ она получила (см. рис. 5). Далее Ева может испустить световой импульс в любом желаемом состоянии света $|\tilde{\psi}\rangle$, используя свой источник. Таким образом, результирующее световое состояние связывается с входным состоянием посредством неунитарного преобразования $|\tilde{\psi}\rangle = V_{Eve}\,|\psi\rangle$. Последнее означает, что Ева на практике может выполнить любое неунитарное преобразование V_{Eve} входного состояния. Стоит отметить, что знание Евы о всей системе в целом является сугубо неформальным приёмом и не должно восприниматься буквально. Такой приём лишь позволяет Еве воспроизвести произвольный оператор V_{Eve} без необходимости в сложном лабораторном оборудовании, которого для некоторых случаев сегодня и вовсе не существует. Например, сегодня нет инструментов для выполнения атаки, подобной PNS [34].

В качестве иллюстрации рассмотрим PNS атаку, в которой Алиса использует ослабленные когерентные импульсы в качестве носителей поляризационных кубитов. Предположим, Алиса испустила такой импульс и он прибыл на станцию Евы в состоянии описываемом кет-вектором $|\psi\rangle = |e^{i\phi}\alpha\rangle$. Чтобы выполнить простейшую PNS атаку, Ева должна выполнить невозмущающее измерение, чтобы определить количество фотонов в импульсе. Такое измерение приводит к коллапсу волнового вектора до состояния с определенным количеством фотонов N. Затем Ева отщепляет K фотонов из импульса (K = 0, 1, ...). Чтобы выполнить эти действия в предложенной установке (см. рис. 5), Ева сначала измеряет оптическую мощность входящего импульса. Основываясь на этом и известном среднем количестве фотонов в начальном импульсе Алисы $|\mu|^2$, она вычисляет среднее количество фотонов $|\mu'|^2$ в полученном импульсе. Далее, используя $|\mu'|^2$, она случайным образом генерирует число фотонов N, воспроизводя таким образом процесс коллапса волнового вектора. Если N больше, чем $n_{max} = 9$ (см. формулу (15)), то Ева повторяет генерацию N до тех пор, пока не будет удовлетворено условие $N \leq n_{max}$. Наконец, Ева моделирует процесс отщепления K фотонов и воспроизводит результирующий световой импульс на своем источнике света в состоянии $|\tilde{\psi}\rangle = e^{i\tilde{\phi}}\,|N-K\rangle$. После этого на своей станции Боб измеряет статистику бозонного сэмплинга, как это предписано формулой (13). Более того, как объяснялось в предыдущем разделе о режимах источников света, исследователь может также управлять оптической фазой каждого светового импульса. Таким образом, возможно учитывать возмущения фазы светового импульса после действия Евы, если его интересует этот аспект. Также могут быть реализованы более специфические атаки, как, например, с использованием невозмущающих POVM измерений (см. о USD атаке в [38]). Ключевым элементом здесь является невозмущающее POVM измерение. Последнее может быть реализовано таким же образом, как описано выше. При этом Еве необходимо выполнить более сложную постобработку результатов подобных измерений [38].

Для большей практичности схемы на рис. 6 и 5 могут быть значительно сокращены. Результат выражается как в экономии экспериментальных инструментов, так и в снижении сложности ПО. Чтобы сделать это, нужно заметить, что любую итерацию протокола KPK можно разделить на две части. Во-первых, осуществляется обмен данными между Алисой и Евой. Это можно сделать, используя упрощенную схему из рис. 1. После этого ту же установку можно использовать для заключительной части коммуникации между Евой и Бобом. Таким образом, можно реализовать все идеи, разработанные в этом разделе, без прямого включения Евы между Алисой и Бобом.

Предложенные методы могут быть также применены к схемам типа MDI [38] путём расширения

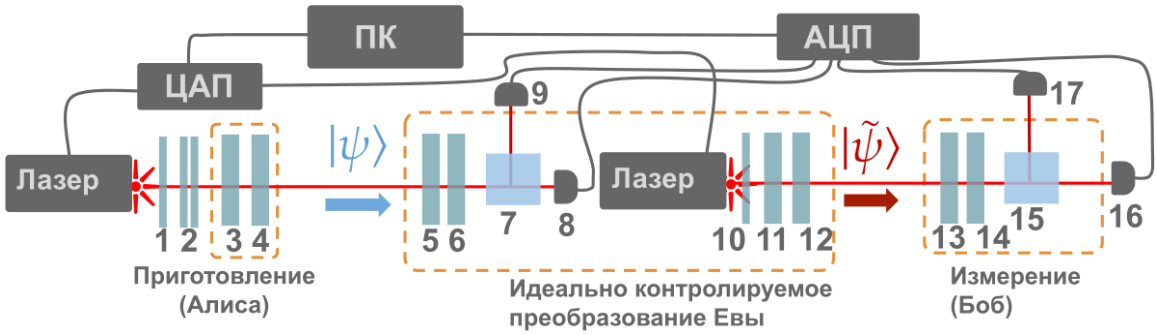

Рис. 5. Интеграция Евы в оптическую схему, показанную на рис. 1, позволяющая выполнить произвольную атаку на один кубит

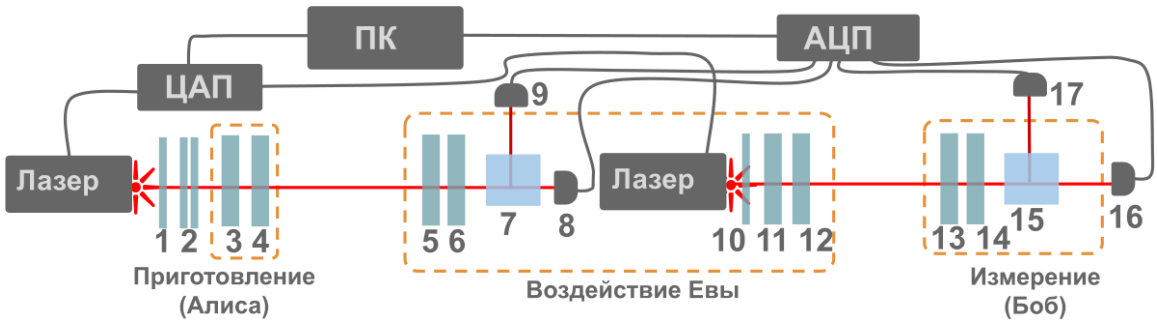

Рис. 6. Интеграция Евы в оптическую схему из рис. 1 для атак, основанных на приёме–перепосылке

предыдущей схемы (см. рис. 1) до схемы, показанной на рис. 7.

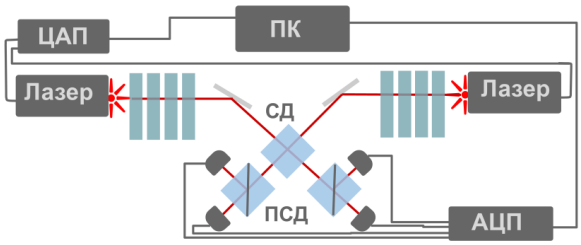

Рис. 7. Расширение схемы показанной на рис. 1 до MDI подобной схемы. Обозначения те же, что и на рис. 1. При этом СД — это неполяризационный светоделитель с коэффициентом отражения 50%; ПСД — поляризационный светоделитель. Оптические пластинки напротив каждого источника предназначены для приготовления необходимого состояния кубита, как было показано на рис. 1

Переключение ПО экспериментатора в режим численного моделирования здесь может быть реализовано тем же образом, как описано выше для введенных типов источников света и детекторов. Что касается экспериментальной реализации, то здесь можно использовать лишь когерентные состояния, поскольку среднее количество фотонов на стороне Боба линейно связано с зарегистрированной им оптической мощностью только в данном случае. Также необходимо использовать только те атаки, в которых Ева в результате порождает лишь когерентные состояния. Это связано с тем, что при использовании, например, однофотонных состояний, возникают сложные интерференционные картины операторов рождения. Это выражается в проявлении, к примеру, эффекта Хонга–Оу–Манделя.

4. СТРУКТУРА ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

Чтобы реализовать описанные выше принципы работы предложенного симулятора, было разработано ПО, основные элементы которого представлены в свидетельстве на программу для ЭВМ [47]. Программное обеспечение написано на языке C++ для применения поляризационной кодировки кубитов в качестве примера. Это ПО рассматривается как иллюстрация предложенных идей, которое может быть модифицировано под конкретные нужды исследователя. Кроме того, данное ПО может служить хорошим универсальным прототипом, который можно легко масштабировать для выполнения гораздо более широкого круга задач.

Интерфейс ПО показан на рис. 8 и разделен на две области: верхнюю и нижнюю.

Первая область изображает оптическую схему стенда как таковую, в то время как вторая предлагает различные полезные инструменты — рабочую таблицу и блок построения графиков для записи, отображения и сохранения данных. Начнем с верхней части. Слева расположен блок источника света.

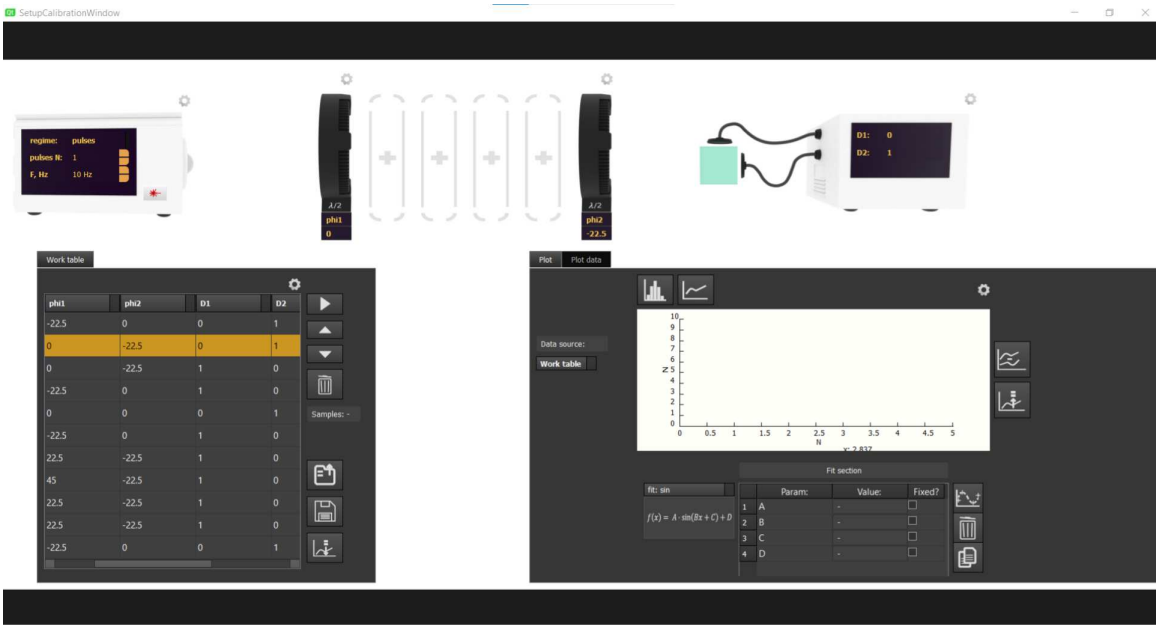

Рис. 8. Интерфейс разработанного программного обеспечения

Рис. 9. Интерфейс программного обеспечения, в котором раскрыты параметры источника света и детекторов

В нем есть необходимые элементы (кнопки и др.) для настройки всех конфигураций источников света, описанных в работе. В качестве иллюстрации на рис. 9 показаны различные параметры источника (QE — квантовая эффективность, mW — мощность импульсов лазера в милливаттах).

Рядом с источником расположено шесть слотов, в которые могут быть установлены различные оптические пластинки. Под каждой пластинкой отображается угол, на который она повернута. Для удобства эти углы привязаны к соответствующим значениям, указанным в рабочей таблице. Если ПО работает не в режиме численного моделирования, то оптические пластинки выполняют только декоративную функцию и служат для удобства исследователя. В противном случае они представляют собой реальную схему для расчета эволюции светового поля. Дальше следует блок измерений, где может быть отображена измеренная оптическая мощность света, коэффициенты пропускания по модам или количество фотоотсчетов. Набор параметров соответствующий различным предложенным режимам работы детекторов представлен на рис. 9.

Нижняя область ПО разделена на рабочую таблицу и блок построения графиков. В таблицу исследователь может автоматическим образом записывать как измеренные данные, так и углы поворота оптических пластинок. Данные могут быть сохранены на ПК. Блок построения графиков используется для отображения регистрируемых данных, а также данных рабочей таблицы. Также здесь присутствуют несколько полезных инструментов, таких как кнопка отображения данных в виде гистограммы и область аппроксимации графиков. В качестве небольшой иллюстрации, на рис. 8 показан сырой секретный ключ для протокола BB84, который был экспериментально распределен с помощью данного ПО (смотрите содержимое рабочей таблицы).

Таким образом, в данном разделе было представлено интуитивно понятное ПО, позволяющее исследователям анализировать протоколы КРК и атаки на них в режиме plug-and-play. ПО также возможно расширить для более широкого спектра применений.

5. ЭКСПЕРИМЕНТ

Мы дополнили представленную систему простым примером экспериментальной реализации однофотонного протокола BB84 с использованием описанных принципов и программного обеспечения. Что касается влияния Евы, то здесь реализована атака приём–перепосылка. Экспериментальная установка показана на рис. 10. Здесь использована сокращенная схема (см. рис. 1), которая может поочередно использоваться для коммуникации между Алисой с Евой и Евы с Бобом.

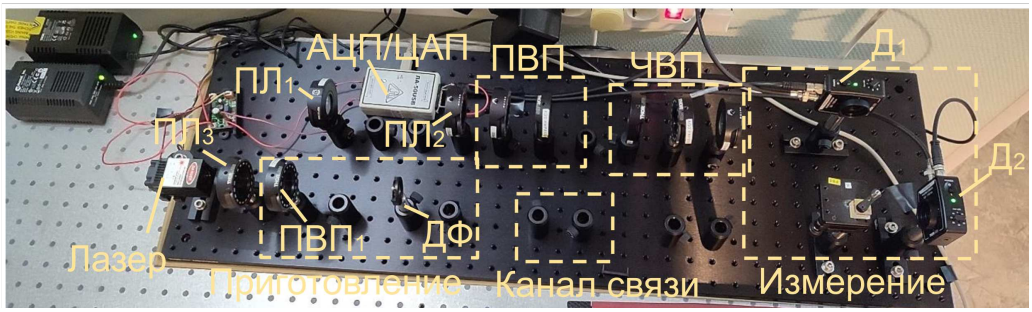

Рис. 10. Экспериментальная установка

Как видно из рис. 10, установка разделена на две области. В верхней области находится набор слотов для установки оптических элементов, которые потребуются для реализации иных протоколов. В этих слотах были установлены в данной конфигурации установки: поляризаторы $ПЛ_1$, $ПЛ_2$, две полуволновые фазовые пластинки (ПВП) и три четвертьволновые фазовые пластинки (ЧВП). Нижняя часть концептуально соответствует основной схеме установки из рис. 1. Она состоит из лазера Komoff (R-250), излучающего в видимом человеческому глазу диапазоне длин волн 650–680 нм, подключенного к ЦАП платы ввода–вывода Руднева–Шиляева LA-50USB. Плата ввода–вывода соединена с компьютером через USB-порт. За лазером установлен поляризатор $ПЛ_3$, отфильтровывающий вертикальную поляризацию лазерного излучения. Далее следует область приготовления произвольного состояния кубита из 4 слотов. Она начинается с первого слота с установленной в нём полуволновой фазовой пластины $ПВП_1$. Она позволяет создать произвольное состояние линейной поляризации. Еще один слот этой области занят диафрагмой (ДФ), сужающей лазерный луч. В оставшиеся два слота может быть установлена пара поляризаторов для добавления потерь в канал. Далее выделена область канала связи с двумя слотами, в которые могут быть установлены четвертьволновая и полуволновая фазовые пластинки для реализации произвольного однокубитного квантового процесса. За ними следует область измерения состояний поляризации с двумя свободными слотами и поляризационным светоделителем. Для реализации протокола BB84, ПВП помещается в один из этих слотов. Поляризационный светоделитель перенаправляет попадающий на него свет в направлении фотодиодных детекторов $Д_1$, $Д_2$ от фирмы Thorlabs (PDA100A2). Сигналы с детекторов поступают в АЦП платы ввода-вывода и, наконец, поступают в ПО, загруженное на ПК.

Используя эту установку, был распределен сырой ключ длиной 525 бит при 8%-м симулируемом темновом шуме в каждом однофотонном детекторе Боба. После просеивания было получено 268 бит ключа, фрагмент которого показан в таблице. Здесь b_s — передаваемый бит Алисы; basis_1 (basis_2) — приготовительный (измерительный) базис, где $\mathrm{basis}_k = 0$ (1) подразумевает базис вертикальной/горизонтальной (диагональной/антидиагональной) поляризации; ϕ_1 (ϕ_2) — угол, под которым была повернута приготовительная (измерительная) полуволновая фазовая пластинка вокруг оси распространения световых импульсов; D_1 (D_2) — отсчет детектора Боба $Д_1$ ($Д_2$); b_r — бит, полученный Бобом. Если D_1 и D_2 равны 1, то бит неопределен, и в таблице формально записывается $b_r = -1$. Соответственно случаи с $b_s \neq b_r$ соответствуют ошибке в передаче Алисой бита b_s.

Как можно видеть из таблицы, длина ключа и значение частоты ошибок около 29.8% соответствуют ожидаемым результатам, основанным на теории.

Таблица. Просеянный ключ

№	b_s	basis_1	basis_2	ϕ_1, град.	ϕ_2, град.	D_2	D_1	b_r
1	0	1	1	22.5	–22.5	1	0	0
2	0	1	1	22.5	–22.5	1	0	0
3	0	1	1	22.5	–22.5	0	1	1
4	0	0	0	45.0	0.0	0	1	1
5	0	1	1	22.5	–22.5	1	0	0
6	1	1	1	–22.5	–22.5	1	1	–1
7	1	1	1	–22.5	–22.5	0	1	1
8	0	0	0	45.0	0.0	0	1	1
9	1	1	1	–22.5	–22.5	1	0	0
10	1	1	1	–22.5	–22.5	1	0	0
11	0	0	0	45.0	0.0	1	0	0
12	1	0	0	0.0	0.0	0	1	1
13	1	0	0	0.0	0.0	0	1	1
14	1	1	1	–22.5	–22.5	0	1	1
15	0	1	1	22.5	–22.5	1	0	0
16	1	1	1	–22.5	–22.5	0	1	1
17	1	1	1	–22.5	–22.5	0	1	1
18	0	0	0	45.0	0.0	1	0	0
19	0	1	1	22.5	–22.5	1	0	0
20	0	1	1	22.5	–22.5	1	0	0
21	1	1	1	–22.5	–22.5	0	1	1
22	0	0	0	45.0	0.0	1	0	0
23	0	1	1	22.5	–22.5	1	0	0
24	1	0	0	0.0	0.0	0	1	1
25	1	1	1	–22.5	–22.5	0	1	1
26	1	1	1	–22.5	–22.5	1	0	0
27	0	1	1	22.5	–22.5	1	1	–1
28	0	1	1	22.5	–22.5	0	1	1
29	1	0	0	0.0	0.0	0	1	1
30	1	1	1	–22.5	–22.5	0	1	1

ЗАКЛЮЧЕНИЕ

В работе предложена методология и соответствующая схема оптического симулятора КРК. Схема позволяет численно моделировать и экспериментально исследовать большое количество протоколов КРК, таких как BB84, B92, протокол на 6 состояниях, включая MDI-подобные системы, а также широкий спектр атак, в простом в применении plug-and-play режиме. Актуальность подобной системы, во-первых, обусловлена растущей потребностью в численном моделировании систем КРК и атак на них для исследовательских целей. Во-вторых, растет потребность в их экспериментальной демонстрации для подготовки специалистов по квантовым коммуникациям. Доступные в предложенном решении атаки варьируются от простой приёма–перепосылки до технически сложных PNS-атак в условиях, когда физическая реализация таких атак крайне затруднена по причинам недостаточного развития соответствующего инструментария. Этот факт отличает предложенную систему от аналогов. Последние позволяют исследователям экспериментально воспроизвести лишь простейшие атаки Евы на протоколы КРК, такие как приём–перепосылка. Кроме того, аналоги позволяют исследователю численно моделировать широкий спектр атак, но достигается это за счет использования достаточно сложных систем компьютерного моделирования. Вместо этого рассматриваемая в работе система рассчитана на работу в простейшем в обращении plug-and-play режиме. Более того, предложенное решение совместимо со всеми основными кодировками кубитов: поляризационной, пространственной и временной. Как и в аналогичных системах, для экспериментальной реализации здесь используются стандартные лабораторные инструменты, такие как диодные лазеры и фотодиодные детекторы общего назначения. Это позволяет экспериментально продемонстрировать системы КРК без необходимости развертывания дорогостоящей и технически сложной реальной системы КРК.

Также представлено программное обеспечение, которое позволило реализовать рассмотренную методологию на примере поляризационного кодирования кубита (см. рис. 8, 9). Данное ПО служит хорошим универсальным прототипом, который можно легко масштабировать для выполнения широкого спектра задач. При использовании этого ПО в работе экспериментально продемонстрированы основные принципы работы систем КРК на примере однофотонного протокола BB84 (см. рис. 10). Что касается учета вмешательства Евы, то для этих целей использована простая атака приём–перепосылка для наглядной иллюстрации. Показана возможность распределения сырого ключа длиной длиной 525 бит при 8%-м заданном темном шуме на каждом детекторе Боба. При просеивании было получено 268 бит секретного ключа, как показано в таблице. Длина ключа и значение частоты ошибок около 29.8% соответствуют ожидаемым результатам.

В качестве перспектив выделяется возможность расширения рассмотренной в работе системы, так чтобы максимально охватить количество реализуемых атак на протоколы КРК. Это связано с гибкостью предлагаемой системы, которая говорит в пользу подобных перспектив. В частности, используя предложенные идеи, можно легко модифицировать представленное ПО и дополнить его иными специальными типами детекторов.

Работа была выполнена в рамках государственного задания Московского государственного университета имени М.В. Ломоносова. Часть работы при создании оптического симулятора квантового распределения ключа была выполнена при поддержке Фонда содействия инновациям в рамках программы «Студенческий стартап» мероприятия «Платформа университетского технологического предпринимательства» федерального проекта «Технологии».

[1] *Kumar M., Mondal B.* // Multimedia Tools and Applications. **84**. 33267 (2025).
[2] *Gisin N., Ribordy G., Tittel W., Zbinden H.* // Rev. Mod. Phys. **74**. 145 (2002).
[3] *Luo W., Cao L., Shi Y.* et al. // Light, science and applications. **2**. N 1. 175 (2023).
[4] *Бигуаа Л.В, Сысоев Н.Н, Кулик С.П.* // Перспективные технологии для систем безопасности. **3**. 66 (2024).
[5] Toshiba's first commercial QKD system. https://asia.toshiba.com/qkd/ [Access date: 26.12.2025].
[6] Russain Infotex QKD system. URL: https://infotecs.ru/products/vipnet-qts-lite/ [Access date: 26.12.2025]
[7] Russain RZD QKD system. https://company.rzd.ru/ru/9401/page/78314?id=221330 [Access date: 26.12.2025]
[8] USA QKD system. URL: https://www.magiqtech.com/solutions/network-security/ [Access date: 26.12.2025]
[9] UK's commercial QKD system. URL: https://www.idquantique.com/quantum-xchange-and-id-quantique-make-ultra-secure-quantum-networks-a-reality-for-leading-us-industries/ [Access date: 26.12.2025]
[10] China's commercial QuantumCTek QKD system // URL: https://www.quantum-info.com/English/case/2017/0901/344.html [Access date: 26.12.2025]
[11] Swiss commercial QKD system // URL: https://www.idquantique.com/ quantum-safe-security/products/ey_exchange_service [Access date: 26.12.2025]
[12] *Abhignan V., Jamunkar A., Nair G.* et al. // Physica Scripta. **99**. 105131 (2024).
[13] OpenQKD simluator // URL: https://openqkd.eu/qkd- network- simulator/ [Access date: 26.12.2025]
[14] QuKayDee simluator // URL: https://qukaydee.com/pages/about [Access date: 26.12.2025]
[15] *Abdelgawad M., Shenouda B., Abdellatif S.* // Cybernetics and Information Technologies. **20**. 21 (2020).
[16] *Escanez-Exposito D., Caballero-Gil P., Martín-Fernández F.* // Wireless Networks. **29**. 3781 (2023).
[17] *Buhari A., Zukarnain Z.A., Subramaniam S.K.* et al. // 2012 IEEE Symposium on Industrial Electronics and Applications 84 (2012).
[18] *Archana B., Krithika S.* // In 2015 2nd International Conference on Electronics. and Communication Systems (ICECS). 457 (2015).
[19] *Mailloux L.O., Morris J.D., Grimaila M.R.* et al. // IEEE Access **3**. 110 (2015).
[20] *Gkouliaras K., Theos V., Evans P., Chatzidakis S.* // Advanced Physics Research. **3**. N 7. 2400016 (2024).
[21] *Zhao S., Raedt H.* // Journal of Computational and Theoretical Nanoscience. **5**. 490 (2008).
[22] *Sethia A., Banerjee A.* // Journal of Modern Optics. **69**. 392 (2022).
[23] *Chatterjee R., Joarder K., Chatterjee S.* et al. // Phys. Rev. Appl. **14**. 024036 (2020).
[24] Infotecs, ViPNet QKDSim QKD system // URL: https://infotecs.ru/products/vipnet-qkdsim/ [Access date: 5.11.2025]
[25] Qiskit programmer's library // URL: https://www.ibm.com/quantum/qiskit [Access date: 26.12.2025]
[26] *Coles P., Metodiev E., Lütkenhaus.* // Nature Communications. **7**. 11712 (2016).
[27] *Mailloux L.O., Hodson D.D., Grimaila M.R.* et al. // IEEE Access. **4**. 2188 (2016).
[28] *Makarov V., Anisimov A., Skaar J.* // Phys. Rev. A. **74**. 022313 (2006).
[29] *Gerhardt I., Liu Q., Lamas-Linares A.* et al. // Nature communications. **2**. 349 (2010)
[30] *Makarov V., Bourgoin J.-P., Chaiwongkhot P.* et al. // Phys. Rev. A. **94**. 030302 (2016).
[31] *Lim J.G., Anisimova E., Higgins B.* et al. // EPJ Quantum Technology. **4**. N 11 (2017).
[32] *Huang A., Navarrete Á., Sun S.-H.* et al. // Phys. Rev. Appl. **12**. 064043 (2019).
[33] *Chaiwongkhot P., Kuntz K.B., Zhang Y.* et al. // Phys. Rev. A. **99**. 062315 (2019). .
[34] *Kulik S.P., Kravtsov K.S., Molotkov S.N.* // Laser Physics Letters. **19**. 025203 (2022).
[35] *Huttner B., Imoto N., Gisin N., Mor T.* // Phys. Rev. A. **51**. 1863 (1995).
[36] Thorlabs, Quantum Cryptography Analogy Demonstration Kit // https://www.thorlabs.com/newgrouppage9.cfm?objectgroup_ID = 9869 [Access date: 10.11.2025]
[37] *Катамадзе К.Г.* Демонстрационный симулятор системы квантового распределения ключа. // патент RU 2795245. (2023).
[38] *Xu F., Ma X., Zhang Q.* et al. // Rev. Mod. Phys. **92**. 025002 (2020).
[39] *Kok P., Munro W.J., Nemoto K.* et al. // Rev. Mod. Phys. **79**. 135 (2007).
[40] *Molotkov S.N., Sushchev I S.* // JETP Lett. **120**. 483 (2024).
[41] *Aigner M.* Combinatorial Theory. Die Grundlehren der mathematischen Wissenschaften : a series of comprehensive studies in mathematics. Springer New York, 1979.
[42] *Lydersen L., Wiechers C., Wittmann C.* et al. // Nature Photonics. **4**. 686 (2010).
[43] *Nielsen M., Chuang I.* Quantum Computation and Quantum Information. 10th Anniversary Edition. Cambridge University Press, 2010.
[44] *Acín A., Gisin N., Scarani V.* // Phys. Rev. A. **69**. 012309 (2004).
[45] *Branciard C., Gisin N., Kraus B., Scarani V.* // Phys. Rev. A. **72**. 032301 (2005).
[46] *BrußD.* // Phys. Rev. Lett. **81**. 3018 (1998).
[47] *Бигуаа Л.В.* Учебный стенд по квантовой криптографии. Свидетельство на ЭВМ 2025613460. 2025.

Optical Simulator For Quantum Key Distribution

L. V. Biguaa[a], S. P. Kulik

Quantum technology centre, Faculty of Physics, Lomonosov Moscow State University
Moscow 119991, Russia
E-mail: [a] leon.006w@yandex.ru

The article proposes a methodology for the construction and operation of a novel optical system for the numerical and experimental study of quantum key distribution (QKD) systems. The system makes it possible to simulate and experimentally implement various attacks on well-known QKD protocols in the plug-and-play mode. The distinctive feature of the system is that it uses only standard laboratory instruments, such as general-purpose diode lasers and photodiode detectors. This makes it allows for demonstrating the operation of the QKD system without the need to deploy an expensive and technically complex full-fledged QKD system in the truly quantum mode. Such a paradigm appears useful for various studies of QKD systems in the context of their intensive development. First, this is associated with the growing need for the numerical simulation of QKD systems for research purposes. Second, the experimental implementation of the proposed approach is necessary for the practical demonstration of the functioning of QKD systems, in particular, in the training of specialists in the field of quantum encryption. At the same time, the analogues currently existing make it possible for researchers to reproduce experimentally only the simplest attacks of an eavesdropper (Eve) on QKD protocols, such as intercept-and-resend attacks. With their aid it is also possible to simulate numerically a wide range of attacks, but using rather sophisticated design systems. In contrast to this, the proposed system allows attacks to be reproduced both numerically and experimentally, ranging from the simplest to technically complex attacks, such as the photon–number-splitting (PNS) ones, for use in the plug-and-play mode.

PACS: 03.67 Dd, 03.67 -a, 03.67 Hk.
Keywords: quantum key distribution, numerical simulations, attacks, qkd protocol.
Received 15 February 2026.
English version: *Moscow University Physics Bulletin*. 2026. **81**, No. 2. Pp. .

Сведения об авторах

1. Бигуаа Леон Вячеславович — магистр; e-mail: leon.006w@yandex.ru.
2. Кулик Сергей Павлович — доктор физ.-мат. наук; профессор, науч. руководитель Центра квантовых технологий МГУ имени М.В.Ломоносова; e-mail: sergei.kulik@physics.msu.ru.