УДК 004.942:004.056.55
DOI: 10.18799/29495407/2025/2/89
Шифр специальности ВАК: 2.3.6

# Обзор и моделирование типовых аппаратных архитектур систем квантового распределения ключей

**А.А. Лукашов✉, В.А. Фаерман**

*Томский государственный университет систем управления и радиоэлектроники, Россия, г. Томск*

✉laa@fb.tusur.ru

**Аннотация.** ***Актуальность*** исследования обусловлена предстоящим широким внедрением квантовых технологий в существующую информационно-телекоммуникационную инфраструктуру. Эффективное внедрение невозможно без предварительного анализа и обоснования достаточности и безопасности систем квантового распределения ключей. Это в свою очередь предполагает исследование и формализованное сравнение аппаратных архитектур, положенных в основу этих систем. Эффективным инструментом для решения последней задачи является компьютерное моделирование. ***Цель*** состоит в исследовании и систематизации типовых аппаратных архитектур систем квантового распределения ключей, их моделировании и верификации созданных моделей. ***Объектом*** являются практические архитектуры систем квантового распределения ключей. ***Методы:*** математическое описание оптических систем на основе формализма Джонса, имитационное моделирование в среде Simulink Matlab. ***Результаты.*** Реализована имитационная модель типовой системы квантового распределения ключей, использующей архитектуру Plug-n-Play. Корректность модели показана путём демонстрации толерантности к искажениям поляризации при передаче в волоконно-оптическом канале связи. Созданные модели оптических компонентов в Simulink могут использоваться для построения моделей систем других архитектур.

**Ключевые слова:** квантовое распределение ключей, фазовое кодирование, протокол BB84, архитектура PnP, Plug-n-Play, Simulink Matlab

**Для цитирования:** Лукашов А.А., Фаерман В.А. Обзор и моделирование типовых аппаратных архитектур систем квантового распределения ключей // Известия Томского политехнического университета. Промышленная кибернетика. – 2025. – Т. 3. – № 2. – С. 8–23. DOI: 10.18799/29495407/2025/2/89

---

UDC 004.942:004.056.55
DOI: 10.18799/29495407/2025/2/89

# Review and modeling of typical hardware architectures of quantum key distribution systems

**A.A. Lukashov✉, V.A. Faerman**

*State University of Control Systems and Radioelectronics, Tomsk, Russian Federation*

✉laa@fb.tusur.ru

**Abstract.** ***Relevance.*** The upcoming widespread implementation of quantum technologies into the existing information and telecommunication infrastructure. Effective deployment is impossible without a preliminary analysis and justification of the adequacy and security of quantum key distribution systems. This, in its turn, necessitates the investigation and formalized comparison of the hardware architectures underlying these systems. An effective tool for addressing this challenge is computer modeling. ***Aim.*** To investigate, classify, and model typical hardware architectures of the quantum key distribution systems, as well as to verify the accuracy of the developed models. ***Object.*** Practical hardware architectures of the quantum key distribution systems. ***Methods.*** Mathematical modeling of optical systems based on Jones formalism, simulations in Simulink Matlab. ***Results.*** The authors have developed a simulation model of a typical quantum key distribution system utilizing the Plug-and-Play architecture. The model validity is confirmed by its robustness against polarization distortions in fiber-optic

transmission. The developed optical component models in Simulink can also be applied to the simulation of other quantum key distribution system architectures.

**Keywords:** quantum key distribution, phase encoding, BB84 protocol, PnP architecture, Plug-n-Play, Simulink Matlab

**For citation:** Lukashov A.A., Faerman V.A. Review and modeling of typical hardware architectures of quantum key distribution systems. *Bulletin of the Tomsk Polytechnic University. Industrial Cybernetics*, 2025, vol. 3, no. 2, pp. 8–23. DOI: 10.18799/29495407/2025/2/89

## Введение

Научный прогресс, появление новых технических и технологических решений служат фундаментом для продолжающейся информатизации общества. Сегодня каждая сфера деятельности так или иначе связана с применением информационно-телекоммуникационных систем, будь то автоматизированное управление производствами, бизнес-процессами, онлайн образование, электронный документооборот на уровне предприятий и государственных сервисов, социальные сети и другие объекты цифрового медиапространства. Современные тенденции развития телекоммуникационных технологий, в частности развёртывание сетей 5G, связаны с двумя основными трендами – увеличением объёма передаваемой информации и повышением требований к её защищённости [1].

В современных общедоступных системах связи, которые на разных уровнях сочетают в себе применение проводных и беспроводных технологий, криптографические методы имеют определяющую роль в обеспечении целостности и конфиденциальности передаваемых данных. Как правило, в основу защиты положено создание криптографическими средствами виртуального тоннеля между рассредоточенными по глобальной сети узлами (так называемое «сквозное шифрование»). Такие тоннели предполагают применение симметричных криптографических систем, использующих идентичный секретный ключ на передающей и принимающей стороне, а также алгоритмов блочного шифрования, основанных на многократном повторении раундов, сводящихся к чередующимся операциям подстановки и перемешивания входных данных, составляющих блок.

Симметричные криптосистемы считаются безопасными, поскольку основаны на алгоритмах, обладающих математически доказанной надёжностью. Однако их безопасное применение предполагает наличие на обеих сторонах обмена заранее распределённого общего секрета, который может быть использован для создания идентичных секретных сеансовых ключей. В условиях общедоступных сетей, предварительное распределение общего секрета между всеми возможными парами узлов практически неосуществимо. По этой причине для создания общего секрета между двумя узлами используется ассиметричные криптографические системы и широко известная схема Диффи–Хелмана [2].

В отличии от блочных алгоритмов шифрования, алгоритмы в основе ассиметричных криптографических систем используют односторонние функции с лазейкой, для которых не имеется строгого математического доказательства их надёжности. В целом для достижения в асимметричных криптографических системах уровня надёжности, который можно определить как вычислительную сложность атаки на алгоритм шифрования, сопоставимого с симметричными криптографическими системами, требуется использование существенно более длинных ключевых последовательностей (например, согласно [3], эквивалентом AES-128 можно считать RSA с длинной простых чисел в 3072 бита). Несмотря на существенные вычислительные сложности, связанные с реализацией ассиметричных криптографических систем, в настоящее время они получили повсеместное распространение, в особенности в сфере Интернет-технологий.

В настоящее время, принимая во внимание успехи в области квантовых вычислений [4], появились дополнительные основания рассматривать асимметричные криптосистемы как потенциально ненадёжные. Так, в 1994 г. Питером Шором был разработан квантовый алгоритм, который способен скомпрометировать любые из распространённых ассиметричных криптографических систем и обладает полиномиальной вычислительной сложностью [5]. По этой причине для обеспечения приемлемого уровня защищённости с использованием имеющихся алгоритмов потребовалось бы экспоненциально увеличивать длину ключей, что сделало бы применение ассиметричных систем непрактичным [6].

Одной из очевидных альтернатив асимметричным криптосистемам в области распределения общего секрета является использование для этой цели выделенного защищённого канала. При непосредственной реализации такое решение непрактично, поскольку оно, во-первых, предполагает наличие децентрализованной и развитой инфраструктуры защищённых каналов, а во-вторых, предполагает наличие взаимного доверия между субъектами, владеющими сегментами этой инфраструктуры. Системы квантового распределения ключей (КРК) можно рассматривать как развитие способа приме-

нения защищённых каналов, частично устраняющего обозначенные выше проблемы.

Технология КРК позволяет двум абонентам создать общий секретный ключ путем отправки фотонов по оптическому каналу связи [7]. Принципы квантовой механики, предполагая корректное применение оборудования, исключающее утечки по побочным каналам, и следование участниками протоколу, делают перехват распределяемого секрета физически невозможным:

- правило Борна предполагает, что состояние произвольной квантовой системы может быть измерено однократно, поскольку при этом исходное состояние системы будет необратимо утрачено вследствие этого измерения [8];
- принцип неопределённости Гейзенберга запрещает точное измерение параметров, одновременно и однозначно характеризующих положение и импульс частицы [9];
- теорема о запрете клонирования постулирует невозможность создания идентичной копии произвольного и неизвестного квантового состояния [10].

С практической точки зрения, перечисленные законы квантовой механики приводят к тому, что при попытке перехвата фотонов в оптическом канале злоумышленник неизбежно будет привносить ошибки, которые зарегистрируют легитимные участники обмена. Отталкиваясь от порогового значения доли присутствия ошибок, который определяется протоколом, стороны или примут решение о создании гарантированно секретного ключа, или вовсе откажутся от создания ключа [11, 12].

Необходимо отметить, что, несмотря на абсолютную теоретическую надёжность, атаки на системы КРК возможны и их исследование в настоящее время представляет собой актуальную научную область [13]. Широкий класс атак основан на несовершенстве и уязвимостях к нештатным воздействиям физических элементов, формирующих оптическую цепь передачи фотонных импульсов. По этой причине для анализа защищённости действующих и перспективных систем КРК целесообразно создание их моделей, учитывающих некоторые физические свойства и особенности представленных в них оптических элементов. Кроме того, поскольку аппаратный состав системы КРК в значительной степени определяется её архитектурой, необходимым этапом решения обозначенной выше задачи является исследование и сравнительная оценка известных архитектур.

В данной работе представлен обзор и сравнительная оценка некоторых типовых практических архитектур систем КРК, в частности вариантов архитектуры Plug-n-Play (PnP). Предложена реализация математической модели системы КРК на основе одного из базовых вариантов архитектуры PnP в Simulink Matlab. Для описания преобразований поляризации в цепи распространения оптического сигнала использовался формализм Джонса. Корректность созданных моделей оптических элементов, а также модели системы КРК в целом продемонстрированы путём воспроизведения характерного для архитектуры PnP свойства толерантности к искажениям поляризации в оптоволоконном канале.

Разработанная модель и библиотека оптических элементов могут быть использованы в дальнейшем для оценки подверженности различных вариантов реализации систем КРК атакам, эксплуатирующим уязвимости оптических компонентов, а также для моделирования таких атак. Кроме этого, модель может быть адаптирована для оценки эксплуатационных характеристик различных систем КРК с учётом качества используемой компонентной базы.

## Аналитический обзор систем квантового распределения ключей

По типу представления квантовых состояний существует два различных подхода: первый, основанный на свойствах света как частицы и формализуемый дискретными переменными (*Discrete Variable Quantum Key Distribution*, DV-QKD), а также второй, разработанный позднее и опирающийся на волновую природу света, формализуемый непрерывными переменными (*Continuous Variable Quantum Key Distribution*, CV-QKD).

В протоколах на дискретных переменных Алиса кодирует свою случайную последовательность побитово в одиночные фотоны. Соответственно, Боб должен использовать детекторы одиночных фотонов при измерении квантовых состояний. В данном подходе могут быть использованы для кодирования следующие свойства частицы: поляризация, фазовый сдвиг, время отправки фотона, а также комбинация данных характеристик [7].

Поляризационное кодирование широко применяется в реальных КРК системах (например, такими компаниями, как ID Quantique (IDQ), QuantumCTek, Qubitekk, Toshiba Europe Ltd.) из-за того, что фотонные импульсы легко передаются как по оптоволоконным линиям, так и в свободном пространстве, и впоследствии регистрируются приёмником [14]. Основной проблемой в эксплуатации таких систем является необходимость сохранения стабильной поляризации на расстояниях в десятки километров, в особенности в типовых телекоммуникационных кабелях. В результате преломления света в оптическом волокне и воздействия внешней среды выходная поляризация изменяется произвольно. Для её стабилизации в сетях КРК применяются электронные поляризационные контроллеры, которые поддерживают постоянную корректи-

ровку углов поляризации для обеспечения корректного кодирования данных [15]. При этом задача прецизионной настройки параметров поляризационного контроллера для компенсации искажений поляризации в канале на этапе первичного запуска сети КРК в заданной конфигурации является трудоёмкой и нетривиальной задачей [15].

Первым протоколом, который был предложен для систем на дискретных переменных и использовал поляризационное кодирование, является протокол BB84, разработанный Чарльзом Беннеттом и Жилем Брассаром в 1984 г. [16]. Кодирование происходит за счёт поляризации фотонов, которые могут находиться в различных состояниях поляризации (базисах), а именно прямоугольных (0° или 90°) или диагональных (±45°). Алиса случайным образом выбирает базис и поляризацию для каждого бита и отправляет фотон Бобу. Поскольку Боб не знает, в каком базисе были закодированы фотоны, он выбирает случайный базис для измерения. Когда Боб измеряет все фотоны, он связывается с Алисой по общедоступному классическому каналу с целью согласования базисов. После того как обе стороны узнали в какой поляризации проводилась отправка и считывание, они оставляют только те случаи, в которых выбранные базисы совпали. Секретный ключ впоследствии будет состоять только из битов, для которых наблюдалось совпадение базисов во время передачи [16].

В использующих фазовое кодирование протоколах информация кодируется в разности фаз между двумя путями в интерферометре Маха–Цендера. Алиса модулирует фазу фотона, создавая определённый сдвиг, соответствующий кодируемому биту информации. Боб использует интерферометр для измерения разности фаз и восстановления переданной информации. Этот метод особенно полезен в оптоволоконных системах связи, где поляризация может быть нестабильной.

Временное кодирование основывается на отправке фотонов в определенные моменты времени. Алиса посылает фотоны в различные временные окна, соответствующие различным значениям кодируемых информационных битов. Боб измеряет время прибытия фотонов и определяет переданные биты на основе зарегистрированных временных интервалов. Этот метод требует высокоточной синхронизации между Алисой и Бобом, а также детекторов с высоким временным разрешением [7].

В идеальных условиях расстояние между абонентами в системах КРК на DV-QKD может достигать дистанций более 100 км в оптоволоконных сетях без усилителей [17–20]. Однако с увеличением расстояния число детектированных фотонов резко уменьшается в связи с потерями в оптоволоконном кабеле. Одним из подходов увеличения дальности КРК является использование квантовых повторителей, которые усиливают или восстанавливают квантовые состояния, но такие технологии, во-первых, все еще находятся в стадии разработки, а во-вторых, их практическое внедрение потребует ревизии требований по безопасности, предъявляемых к сетям [21–24]. Другим подходом является использование спутников в качестве посредников. Последнее позволяет заменить оптическую линию на свободную среду в квантовом канале, что в свою очередь изменяет характер затухания сигналов с расстоянием с экспоненциального на квадратический [25].

Протоколы квантового распределения ключей с непрерывными переменными (CV-QKD) используют параметры электромагнитного поля, такие как амплитуды и фазы, для кодирования информации. Алиса модулирует когерентное лазерное излучение, а Боб измеряет изменения опорного сигнала, над которым проводилась модуляция [26–28].

В 2024 г. успешно был реализован CV-QKD на рекордном расстоянии 100 км с использованием опорного сигнала, сгенерированного локальным осциллятором, и методов машинного обучения для контроля фазового шума [29]. Главным преимуществом CV-QKD является возможность работать на стандартных оптических линиях связи, приёмниками в которых выступают типичные фотоэлектронные преобразователи, не являющиеся детекторами одиночных фотонов. Однако практическое применение CV-QKD на больших дистанциях все также проблематично в связи с потерями в оптических волокнах и влиянием шума, ограничивающими дальность и скорость передачи. Для преодоления этих ограничений продолжаются исследования в области разработки более эффективных методов модуляции, детектирования и компенсации потерь в канале [30, 31].

Подход DV-QKD обычно более устойчив к фазовому шуму, тогда как CV-QKD чувствителен к нему, особенно в каналах с тепловыми потерями. Однако в условиях низкого фазового шума и высокого теплового шума CV-QKD может выдерживать большие потери по сравнению с DV-QKD [32].

CV-QKD имеет потенциал для более высокой скорости передачи ключей на коротких расстояниях, особенно в городских сетях [33, 34]. DV-QKD обеспечивает стабильную скорость на больших расстояниях, при этом ограничение накладывается технологическими особенностями однофотонных детекторов.

DV-QKD более надежен с точки зрения безопасности, так как даже при увеличении расстояния дискретные переменные позволяют лучше контролировать попытки перехвата квантовых состояний [35], что обусловлено однофотонным представлением передаваемых в канал символов. Одна-

ко для его реализации требуется более сложное оборудование.

Системы квантового распределения ключей, вне зависимости от применяемого метода кодирования и формата квантовых состояний (CV-QKD или DV-QKD), могут быть отнесены к одному из трёх типов на основе используемых квантово-механических принципов и количества узлов, участвующих в обмене информацией [36]:

- Системы, предполагающие подготовку и измерение квантовых состояний (*prepare and measure*) (рис. 1, *а*). Это наиболее распространенный тип систем, в которых используются единственный источник фотонов и единственный приёмник фотонов, распределённые между сторонами-участниками обмена (между Алисой и Бобом) [16].

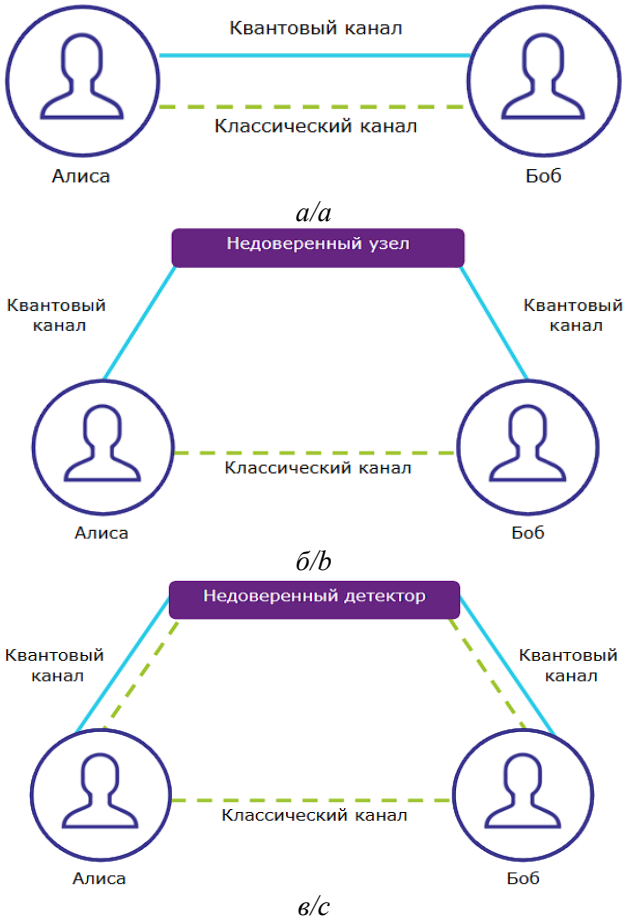


***Рис. 1.*** *Схемы систем: а) с недоверенным детектором; б) EB-QKD; в) MDI-QKD*

***Fig. 1.*** *Scheme of the system: a) with an untrusted detector; b) EB-QKD; c) MDI-QKD*

- Системы, основанные на использовании запутанных фотонов (*entanglement-based quantum key distribution*, EB-QKD) (рис. 1, *б*). [37]. В таких системах недоверенный узел сети функционирует как источник фотонов, который генерирует запутанные фотонные пары, отправляя один фотон Алисе, а другой – Бобу. Даже если источник находится под контролем злоумышленника, безопасность протокола остаётся гарантированной благодаря свойствам квантовой механики. Любое вмешательство в передачу фотонов приводит к разрушению квантовой запутанности, что нарушает статистические корреляции результатов измерений у Алисы и Боба. Путём анализа статистики этих корреляций и применения неравенства Белла абоненты могут обнаружить наличие перехватчика и предотвратить утечку информации [4].
- Системы с недоверенным детектором (*measurement-device-independent quantum key distribution*, MDI-QKD) представляют собой один из вариантов реализации EB-QKD, который отличается отсутствием требования к доверию сторонам, владеющим измерительными устройствами (рис. 1, *в*) [37, 38]. В таких системах Алиса и Боб независимо подготавливают квантовые состояния и передают их к центральному узлу (Чарли), выполняющему измерения. Генерация секретного ключа основана на анализе корреляций результатов измерений с учётом неравенства Белла. Преимущество MDI-QKD заключается в том, что даже при компрометации центрального узла злоумышленник не сможет получить информацию о передаваемом квантовом ключе, поскольку безопасность основана на фундаментальных свойствах квантовой физики, а не на доверии к измерительным устройствам.

Среди практических реализаций одним из наиболее распространённых классов систем квантового распределения ключей являются архитектуры, основанные на концепции Plug-and-Play QKD (PnP-QKD). В литературе встречаются различные варианты архитектур систем, которые характеризуются авторами как реализующие концепцию PnP-QKD. Среди определяющих признаков таких архитектур можно выделить следующие:

- всё наиболее сложное и дорогостоящее оборудование обычно сосредоточено в одном из узлов, который можно условно считать сервером, при этом второй (абонентский) узел отличается простотой;
- после подключения обоих узлов к оптическому каналу не требуется продолжительная и трудоёмкая процедура их конфигурирования, в частности тонкой подстройки параметров поляризационных контроллеров для компенсации искажений в канале;
- задача синхронизации решается тривиально, поскольку и приёмник, и передатчик локализованы в одном из узлов.

В системах PnP-QKD Боб сначала отправляет не подготовленный световой импульс к Алисе, а Алиса возвращает модифицированный импульс, кодирующий информационный символ, обратно Бобу. Поскольку световой сигнал проходит по одному и тому же каналу связи дважды (в прямом и обратном направлениях), такая архитектура естественным образом компенсирует поляризационные и фазовые искажения в канале. Подобная система впервые была предложена в 1997 г. в варианте, представленном на рис. 2, *а* [39]. Предпосылки её создания были связаны прежде всего с отсутствием затрат на синхронизацию работы модулей Алисы и Боба, которая в то время представляла серьёзную технологическую проблему в архитектурах, в которых источник фотонов и приёмник фотонов находились в разных узлах [39].

В классической схеме PnP-QKD Боб формирует лазерный импульс, который на светоделителе BS1 разделяется на две части: прямую и задержанную. Задержка второго импульса создается вследствие прохождения света через плечи, создаваемые зеркалами FM1 и FM2, после чего он отправляется на сторону Алисы через оптический канал. После того как импульсы достигают Алисы, первый из них отражается от зеркала FM3 и возвращается в оптический канал без дополнительных преобразований, в то время как на задержанный импульс, посредством фазового модулятора PM2, накладывается фазовое смещение. После чего оба импульса возвращаются на сторону Боба. Первый импульс разделяется на светоделителе BS2, и его часть задерживается при прохождении через плечи, образованные зеркалами FM1 и FM2. Это приводит к тому, что задержанная часть импульса интерферирует с частью второго импульса [40], что фиксируется детектором SPD [39].

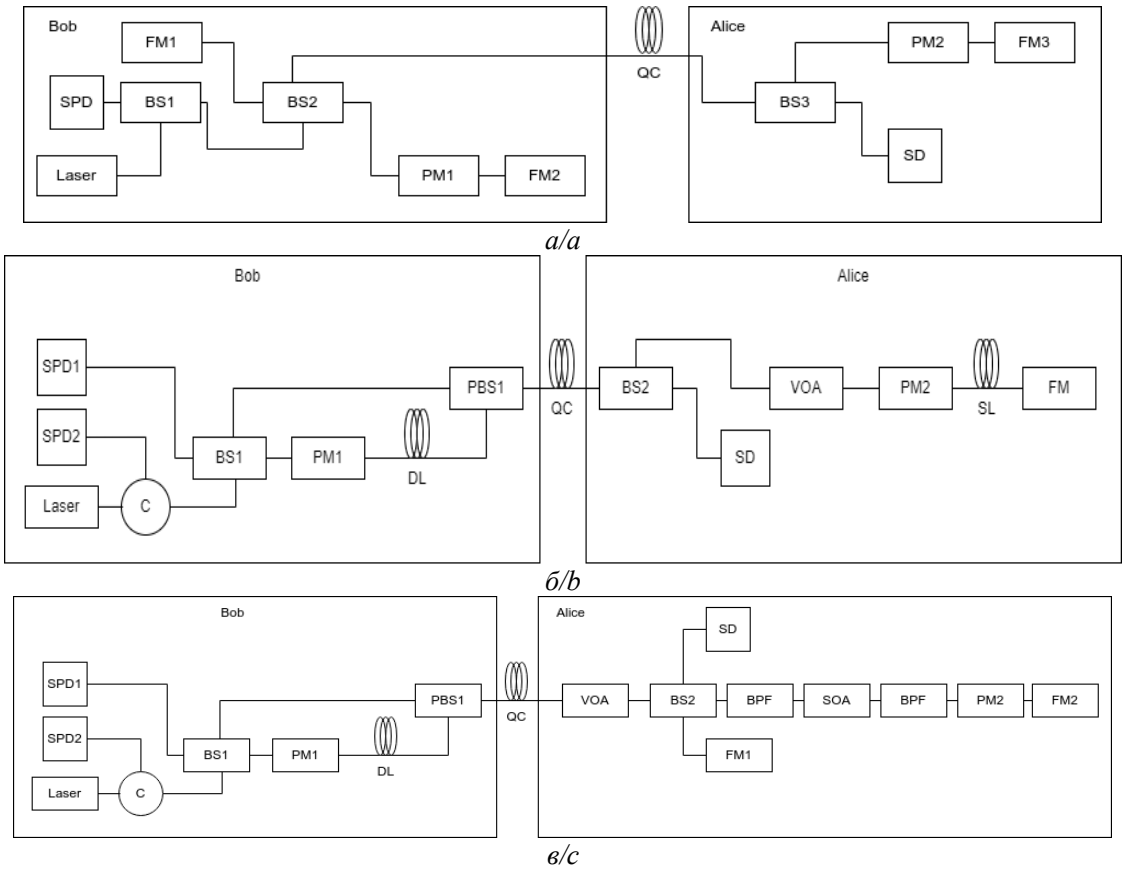


***Рис. 2.*** *Схемы: а) классическая схема PnP-QKD; б) двухпроходная автокорреляционная оптоволоконная схема PnP-QKD; в) PnP-QKD с генератором оптических импульсных последовательностей. На схемах обозначены: Laser – лазерный модуль; C – оптический циркулятор; SPD – детектор одиночных фотонов; SD – синхронизирующий детектор; BS – неполяризационый светоделитель; PBS – поляризационный светоделитель; PM – фазовый модулятор; DL – линия задержки; VOA – переменный оптический аттенюатор; SOA – полупроводниковый фотоусилитель; BPF – полосовой фильтр; FM – зеркало Фарадея; SL – линия хранения; QC – квантовый канал*

***Fig. 2.*** *Schemes: a) classic PnP-QKD; b) two-pass autocorrelation fiber-optic PnP-QKD; c) PnP-QKD circuit with optical pulse sequence generator. The notation used as follows: Laser – laser module; C – circulator; SPD – single photon detector; SD – synchro detector; BS – beam splitter; PBS – polarizing beam splitter; PM – phase modulator; DL – delay line; VOA – variable optical attenuator; SOA – semiconductor optical amplifier; BPF – bandpass filter; FM – Faraday mirror; SL – storage line; QC – quantum channel*

На рис. 2, *б* представлена двухпроходная автокорреляционная оптоволоконная схема PnP-QKD, функционирующая следующим образом. Инициируется начало выработки битовой информации лазерным импульсом, который с циркулятора C попадает на светоделитель BS1 и расходится с разной мощностью по двум плечам интерферометра. Из-за наличия линии задержки на одном плече интерферометра один импульс света обгоняет другой. Вследствие этого они, последовательно проходя через поляризационный светоделитель PBS1 и оптический канал, попадают на сторону Алисы. Большая часть света, проходя через светоделитель BS2, способствует срабатыванию синхродетектора SD, что интерпретируется Алисой как сигнал о том, что до неё дошли импульсы, изменяя параметры которых она впоследствии закодирует информационный символ [39].

Частично импульсы, проходя через светоделитель BS2, попадают в верхнее плечо, где ослабляются переменным оптическим аттенюатором VOA. После чего на один из них при помощи фазового модулятора PM2 Алиса накладывает фазовое смещение. Отражаясь от зеркала Фарадея FM, импульсы в очередной раз ослабляются аттенюатором VOA до состояния, близкого к однофотонному, и затем возвращаются на сторону Боба [39].

После прохождения через PBS импульс, который ранее проходил по верхнему плечу интерферометра, пойдет по нижнему, а второй импульс – по верхнему. Это обусловлено тем, что изначально все импульсы, исходящие от Боба, были ортогонально поляризованы, но, когда они отразились от зеркала Фарадея FM, они поменяли свою поляризацию на ортогональную. Таким образом, к светоделителю BS1 оба импульса прибудут одновременно, так как на протяжении прямого и обратного проходов они преодолели одинаковый оптический путь, и, следовательно, их интерференция произойдет на одном из детекторов – SPD1 или SPD2. Срабатывание того или иного детектора будет обусловлено выбором фазовых сдвигов, которые накладываются Алисой и Бобом. Так, Боб модулятором PM1 накладывает фазовый сдвиг на импульс, проходящей в обратном направлении по нижнему плечу интерферометра, выбирая таким образом базис измерений. Алиса определяет базис кодирования и значение кодируемого символа, применяя модулятор PM2 ко второму импульсу в ходе прямого прохождения [39].

В 2022 г. была предложена архитектура PnP-QKD с генератором оптических импульсных последовательностей (*optical pulse train gernerator*, OPTG PnP-QKD) [41]. Данная схема отличается прежде всего реализацией модуля Алисы (рис. 2, *в*), в который вводится подсистема, позволяющая генерировать последовательность оптических импульсов, с использованием изначального импульса Боба. В работе отмечается, что за счёт предложенных изменений можно достичь миниатюризации систем и увеличения скоростей производства ключевого материала.

Схема OPTG PnP-QKD функционирует следующим образом. Боб посылает Алисе пару последовательно идущих импульсов, как и в ранее описанных реализациях. На стороне Алисы, после ослабления, импульс делится на две части в BS2. Одна из частей передается на SD для генерации сигнала синхронизации, а другая – в оптический резонатор, реализованный зеркалами FM1 и FM2, для принятия в качестве инициирующего сигнала для генератора OPTG. Собственно, генератор OPTG представляет собой совокупность элементов, через которые проходит импульс в оптическом резонаторе. Полосовые оптические фильтры BPF устраняют компоненты сигнала, отличающиеся по длине волны от рабочей. Требуемый уровень сигнала поддерживается с помощью полупроводникового оптического усилителя SOA. Затем усиленный сигнал передается на зеркало FM2 через модулятор PM2 так же, как это происходило в описанных ранее вариантах. На обратном пути импульс вновь проходит фильтры и усилитель, после чего вновь делится на две части в BS2. Одна из частей ослабляется с помощью VOA и передаётся Бобу через оптический канал, в то время как вторая поступает на оптический резонатор, и весь цикл повторяется. Таким образом, используя начальный импульс Боба, Алиса по мере собственный потребности может генерировать множественные импульсы, направляя в оптический резонатор очередной импульс, проходящий светоделитель BS2 в обратном направлении.

Натурные эксперименты, описанные в статье, показывают, что подобный генератор делает возможным получение до десяти импульсов из исходного, что позволяет повысить скорость выработки ключевого материала при сохранении QBER около 5 %.

**Построение компьютерной модели**

При построении модели в Simulink Matlab двухпроходная схема PnP-QKD была разделена на три функциональных блока, границы которых отражены на рис. 2, *б*: модуль Боба (Bob), модуль Алисы (Alice), квантовый канал (QC). Модель на верхнем уровне представлена на рис. 3. Связи между блоками верхнего уровня отражают то, что сигнал проходит путь как прямом направлении, так и в обратном. В силу ограничений среды в дальнейшем было принято решение для каждого из блоков реализовать две модели, одна из которых определяет преобразование сигнала в прямом направлении, а другая в обратном.

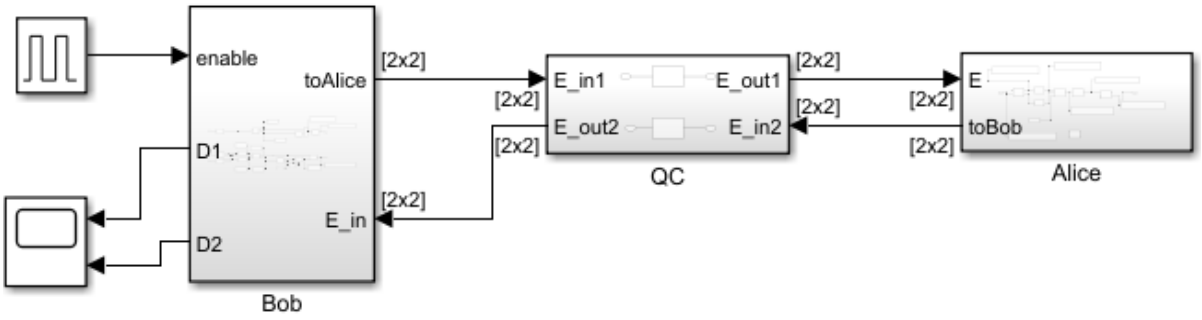


***Рис. 3.*** *Общий вид схемы модели в Simulink Matlab*
***Fig. 3.*** *General view of the model diagram in Simulink Matlab*

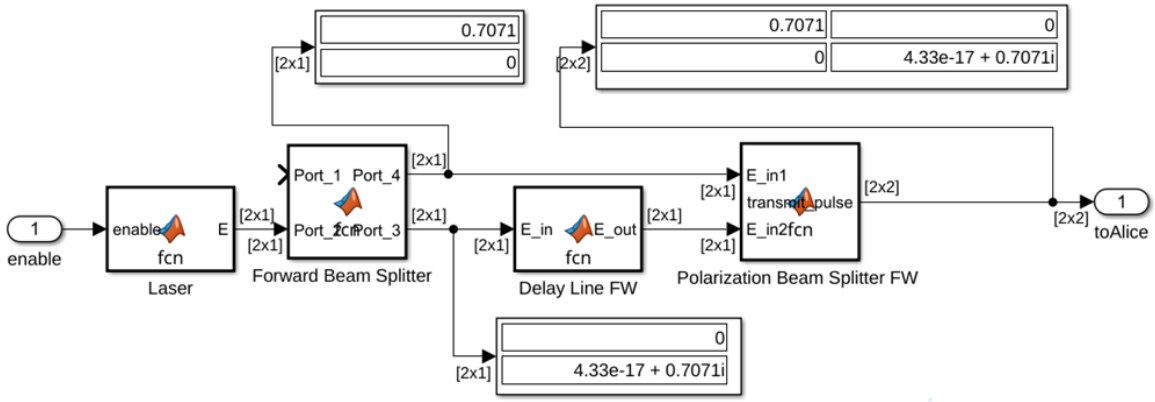


***Рис. 4.*** *Прямой проход через блок Боба*
***Fig. 4.*** *Direct pass-through Bob's block*

Компонент для генерации прямоугольных импульсов используется для имитации включения источника светового пучка, а осциллограф визуализирует срабатывание детекторов при симуляции протокола BB84.

Декомпозиция функционального блока модуля Боба при прохождении импульса в прямом направлении представлена на рис. 4. Все оптические элементы модуля реализованы с применением функциональных блоков «Fcn block», описанных посредством S-функций. Модель, описывающая преобразование импульса при прохождении в обратном направлении, представлена на рис. 5. Не сложно заметить, что при обратном прохождении оптической цепи к импульсу применяется фазовый модулятор Боба. Преобразования, производимые блоками, описаны далее.

После поступления на вход блока разрешающего сигнала с генератора прямоугольных импульсов блок «Laser» формирует оптический импульс, интенсивность, поляризация и фазовое смещение которого описываются с применением формализма Джонса:

$$\mathrm{E}(t)=\begin{pmatrix} E_x\cdot e^{i\cdot\varphi_x} \\ E_y\cdot e^{i\cdot\varphi_y}\end{pmatrix}\cdot e^{-i\cdot\omega_0\cdot t}=$$

$$=E_0\cdot e^{i\cdot(\varphi_0-\omega_0\cdot t)}\cdot\begin{pmatrix}\cos(\alpha)\\ \sin(\alpha)\cdot e^{i\cdot\Delta\varphi}\end{pmatrix}=$$

$$=E_0\cdot e^{-i\cdot\omega_0\cdot(t-\tau_0)}\cdot J(\alpha,\Delta\varphi), \qquad (1)$$

где $E_0$ – интенсивность монохроматического света с частотой $\omega_0$; $\tau_0$ – временная задержка, определяющая начальное фазовое смещение колебания $\varphi_0$; $\alpha$ – угол поляризации, определяющий соотношение энергий вертикально и горизонтально поляризованных компонентов волны; $\Delta\varphi$ – фазовое смещение вертикального поляризационного компонента относительно горизонтального. Векторный множитель $J(\alpha,\Delta\varphi)$ в (1) представляет собой единичный вектор Джонса, который однозначным образом определяет поляризацию сигнала. Само по себе значение $\mathbf{E}(t)$ можно рассматривать как двумерный комплекснозначный вектор Джонса. На выходе лазера импульсы имеют горизонтальную поляризацию, то есть

$$J(\alpha,\Delta\varphi)=\begin{pmatrix}1\\0\end{pmatrix}.$$

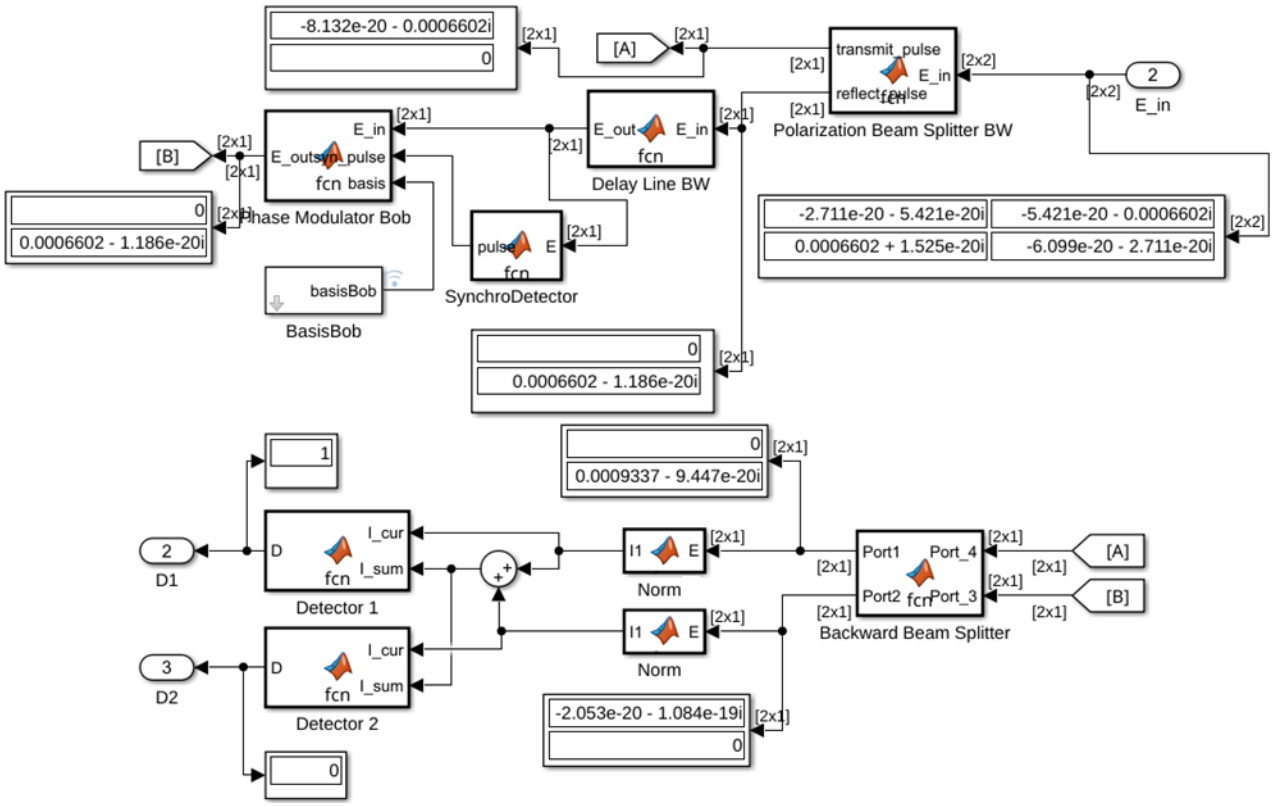


***Рис. 5.*** *Обратный проход через блок Боба*
***Fig. 5.*** *Reverse pass-through Bob's block*

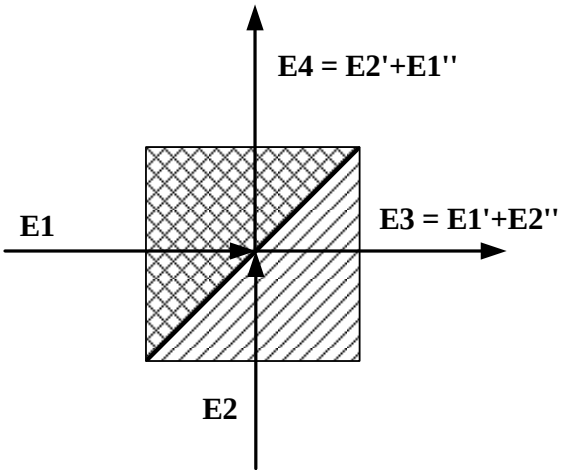


***Рис. 6.*** *Схема работы светоделителя*
***Fig. 6.*** *Beam splitter operation diagram*

Блоки «Forward Beam Splitter» и «Backward Beam Splitter» описывают преобразования, производимые светоделителями. Поступающий на светоделитель импульс частично проходит разделяющую пластинку, расположенную по центру, напрямую, а частично отражается от неё, как это показано на рис. 6. Блоки «Forward Beam Splitter» и «Backward Beam Splitter» имеют по два входных порта и два выходных порта и различаются лишь сопоставлением между входами элемента модели и расположением соответствующих граней на физическом объекте. Последнее имеет значение, поскольку при отражении импульса от границы раздела двух сред на переходе из менее оптически плотной среды в более плотную отражённая компонента импульса терпит фазовый сдвиг равный половине волны, а в обратном случае фазового сдвига не происходит [40]. Таким образом, модель светоделителя при прямом прохождении

$$\mathbf{E}_3(t)=\begin{pmatrix} p & 0 \\ 0 & p \end{pmatrix}\cdot\mathbf{E}_1(t)+\begin{pmatrix} 1-p & 0 \\ 0 & 1-p \end{pmatrix}\cdot\mathbf{E}_2(t),$$

$$\mathbf{E}_4(t)=\begin{pmatrix} 1-p & 0 \\ 0 & 1-p \end{pmatrix}\cdot\mathbf{E}_1(t)+\begin{pmatrix} p & 0 \\ 0 & p \end{pmatrix}\cdot\mathbf{E}_2(t),$$

а при обратном прохождении

$$\mathbf{E}_1(t)=\begin{pmatrix} p & 0 \\ 0 & p \end{pmatrix}\times\mathbf{E}_3(t)+$$

$$+\begin{pmatrix} (1-p)\cdot e^{-i\cdot\pi} & 0 \\ 0 & (1-p)\cdot e^{-i\cdot\pi} \end{pmatrix}\times\mathbf{E}_4(t),$$

$$\mathbf{E}_2(t)=\begin{pmatrix} 1-p & 0 \\ 0 & 1-p \end{pmatrix}\times\mathbf{E}_1(t)+\begin{pmatrix} p & 0 \\ 0 & p \end{pmatrix}\times\mathbf{E}_4(t),$$

где $p$ – коэффициент прямого прохождения.

Блок «Delay Line» моделирует линию задержки, внося дополнительное фазовое смещение в сигналы, описанные вектором Джонса, при этом изменяя параметр τd согласно описанию в (1), то есть

$$\mathrm{E}_{\text{вых}}(t)=\begin{pmatrix} e^{i\cdot\tau_d\cdot\omega_0} & 0 \\ 0 & e^{i\cdot\tau_d\cdot\omega_0}\end{pmatrix}\times \mathrm{E}_{\text{вх}}(t).$$

Блоки «Polarization Beam Splitter FW» и «Polarization Beam Splitter BW» описывают поляризационный светоделитель, который разделяет входящий свет на два луча, поляризованных ортогонально друг к другу. Аналогично со светоделителем, представленным на рис. 6, направление падения импульса имеет значение. В случае с «Polarization Beam Splitter FW» используются два входных порта и один выходной

$$\mathbf{E}_3(t)=\begin{pmatrix}1 & 0\\ 0 & 0\end{pmatrix}\cdot\mathbf{E}_1(t)+\begin{pmatrix}0 & 0\\ 0 & 1\end{pmatrix}\cdot\mathbf{E}_2(t),$$

а в «Polarization Beam Splitter BW» – один входной и два выходных

$$\mathbf{E}_1(t)=\begin{pmatrix}1 & 0\\ 0 & 0\end{pmatrix}\cdot\mathbf{E}_3(t),\ \mathbf{E}_2(t)=\begin{pmatrix}0 & 0\\ 0 & 1\end{pmatrix}\cdot\mathbf{E}_3(t).$$

Блок «SynchroDetector» имитирует формирование синхроимпульсов при прибытии очередной посылки из оптического канала. В настоящей модели он представлен исключительно для обеспечения большего структурного соответствия схеме на рис. 2, *б* и не вносит значимого вклада в логику работы модели.

Математическое описание фазовых модуляторов, в том числе «Phase Modulator Bob», приводится далее, при рассмотрении модели модуля Алисы.

Модель приёмника оптических сигналов на стороне Боба представляет собой комбинацию пар блоков «Norm», производящих оценку интенсивности импульса, а также блоков «Detector», моделирующих датчики, находящиеся в плечах интерферометра. В ответ на импульс, представленный вектором Джонса, на выходе блока «Norm» формируется скалярное комплексное значение, равное $E_0\cdot e^{i\varphi_0}$, в соответствии с (1).

Блоки «Detector» имитируют реакцию детекторов одиночных фотонов с помощью вероятностного подхода следующим образом:

$$A=\begin{cases}1, \left|E_{01}\cdot e^{i\cdot\varphi_{01}}+E_{02}\cdot e^{i\cdot\varphi_{02}}\right|^2\ge X,\\ 0, \left|E_{01}\cdot e^{i\cdot\varphi_{01}}+E_{02}\cdot e^{i\cdot\varphi_{02}}\right|^2< X,\end{cases}$$

$$B=\begin{cases}1,1-\left|E_{01}\cdot e^{i\cdot\varphi_{01}}-E_{02}\cdot e^{i\cdot\varphi_{02}}\right|^2\le X,\\ 0,1-\left|E_{01}\cdot e^{i\cdot\varphi_{01}}-E_{02}\cdot e^{i\cdot\varphi_{02}}\right|^2> X,\end{cases}$$

где $X$ – случайная величина, равномерно распределённая на интервале [0; 1] и генерируемая каждый раз при поступлении нового импульса.

При отсутствии потерь в канале выполняется условие

$$E_{01}^2+E_{02}^2=1,$$

что гарантирует срабатывание одного и только одного из датчиков при поступлении импульса.

Блок верхнего уровня «QC», показанный на рис. 3, моделирует искажения сигналов в квантовом канале и представляет собой комбинацию линии задержки («Delay Line»), линейного ослабления (блок «Attenuator») и универсального поляризационного контроллера («Polarization Controller»).

Блок «Attenuator», который ослабляет интенсивность оптического сигнала в соответствии с заданным передаточным коэффициентом $T$ ($0\le T\le 1$):

$$\mathbf{E}_{\text{вых}}(t)=\begin{pmatrix}1/\sqrt{T} & 0\\ 0 & 1/\sqrt{T}\end{pmatrix}\times\mathbf{E}_{\text{вх}}(t).$$

Поляризационный контроллер в свою очередь представляет собой комбинацию из трёх последовательно соединённых волновых пластик (четвертьволновой–полуволновой–четвертьволновой), которые формально описываются матрицами Джонса

$$\mathrm{H}^{\lambda/4}(\theta)=R(\theta)\times\begin{pmatrix}1 & 0\\ 0 & i\end{pmatrix}\times R^{-1}(\theta),$$

$$\mathrm{H}^{\lambda/2}(\theta)=R(\theta)\times\begin{pmatrix}1 & 0\\ 0 & -1\end{pmatrix}\times R^{-1}(\theta),$$

где $R(\theta)$ – матрицы поворота.

Таким образом, манипулируя углами поворота каждой из трёх пластин, можно преобразовывать поляризацию импульса произвольным образом

$$\mathbf{E}_{\text{вых}}(t)=\mathrm{PC}(\theta_1,\theta_2,\theta_3)\times\mathbf{E}_{\text{вх}}(t),$$
$$\mathrm{PC}(\theta_1,\theta_2,\theta_3)=\mathrm{H}_3^{\lambda/4}(\theta_3)\times\mathrm{H}_2^{\lambda/2}(\theta_2)\times\mathrm{H}_1^{\lambda/4}(\theta_1).$$

За счёт этого блок квантового канала «QC» позволяет имитировать произвольные поляризационные искажения в оптоволоконной линии [15].

При прохождении импульса по квантовому каналу в обратном направлении вносимые средой поляризационные искажения происходят в обратном порядке, то есть последовательность матриц Джонса, описывающая поляризационный контроллер, инвертируется, что можно выразить следующим образом

$$\mathbf{E}_{\text{вых}}(t)=\mathrm{PC}(\theta_3,\theta_2,\theta_1)\times\mathbf{E}_{\text{вх}}(t).$$

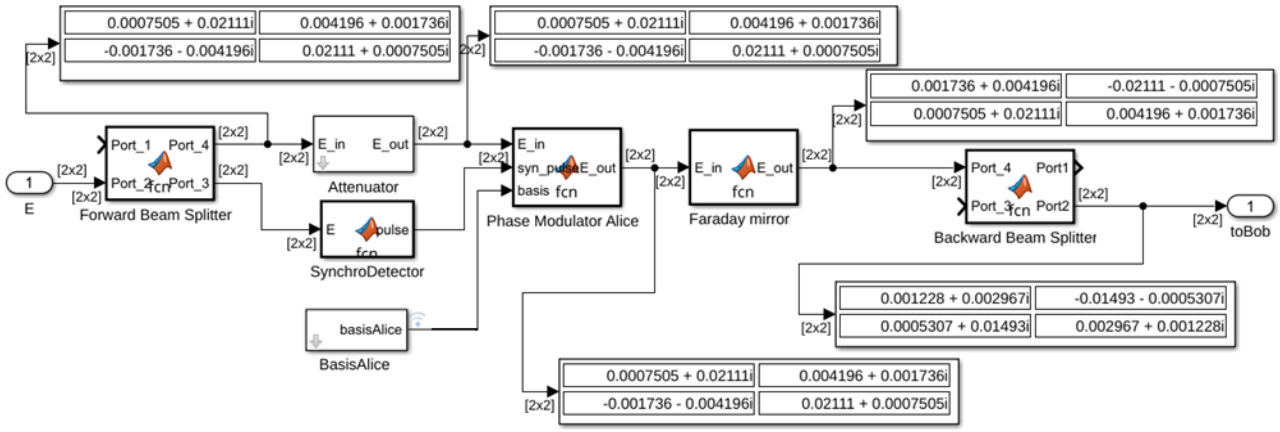


***Рис. 7.*** *Проход через блок Алисы*
***Fig. 7.*** *Pass through Alice's block*

Декомпозиция функционального блока модуля Алисы при прохождении импульса в прямом и обратном направлениях представлена на рис. 7. Из рисунка видно, что существенная часть моделей оптических элементов, задействованных в модуле Алисы, была рассмотрена ранее. Ранее не были рассмотрены модели фазовых модуляторов и зеркала Фарадея.

Блок «Faraday Mirror» изменяет поляризацию падающего на него сигнала на ортогональную при отражении, то есть с учётом фазового сдвига

$$\mathbf{E}_{\text{вых}}(t) = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \times \mathbf{E}_{\text{вх}}(t).$$

Блоки «Phase Modulator Alice» и «Phase Modulator Bob» описывают фазовые модуляторы Алисы и Боба. За исключением синхроимпульсов, каждый из них принимает на вход вектор Джонса, описывающий модулируемый импульс, а также двоичное кодовое значение, определяющее фазовый сдвиг в соответствии с протоколом BB84. Формально преобразование модулятора можно описать фазовым сдвигом, зависимым от значения $B$ на кодовом входе:

$$\mathbf{E}_{\text{вых}}(t, Y) = \begin{pmatrix} e^{i\cdot\varphi(Y)} & 0 \\ 0 & e^{i\cdot\varphi(Y)} \end{pmatrix} \times \mathbf{E}_{\text{вх}}(t),$$

значения $\varphi(Y)$ представлены в табл. 1. Логика выбора величины фазового сдвига в зависимости от значений на выходе генераторов случайных кодов определяется в модели в блоках «BasisAlice», «BasisBob».

**Верификация модели**

Для верификации модели было проведено исследование, направленное на проверку известного свойства систем архитектуры PnP-QKD, которое состоит в толерантности поляризационных искажений в канале.

***Таблица 1.*** *Логика работы модели системы КРК для протокола BB84*

***Table 1.*** *QKD system model operational principles for BB84 protocol*

| Модуль Алисы Alice module | | | Модуль Боба Bob module | | | Вероятность срабатывания Probability of triggering | |
|---|---|---|---|---|---|---|---|
| Базис $Y$ Basis $Y$ | Битовый символ Bit character | Модулятор $\varphi_A(Y)$ Modulator $\varphi A(Y)$ | Базис $Y$ Basis $Y$ | Модулятор $\varphi_B(Y)$ Modulator $\varphi A(Y)$ | Принятый бит Received bit | Детектор $A$ Detector $A$ | Детектор $B$ Detector $B$ |
| HV | 0 | 0 | HV | 0 | 0 | 1 | 0 |
| HV | 0 | 0 | DA | π / 2 | – | 1/2 | 1/2 |
| HV | 1 | π | HV | 0 | 1 | 0 | 1 |
| HV | 1 | π | DA | π / 2 | – | 1/2 | 1/2 |
| DA | 0 | π / 2 | HV | 0 | – | 1/2 | 1/2 |
| DA | 0 | π / 2 | DA | π / 2 | 0 | 1 | 0 |
| DA | 1 | 3π / 2 | HV | 0 | – | 1/2 | 1/2 |
| DA | 1 | 3π / 2 | DA | π / 2 | 1 | 0 | 1 |

Для проверки воспроизводимости этого свойства в модели в блоке, моделирующем оптический канал «QC», произвольным образом задавались поляризационные искажения, после чего оценивались вероятности срабатывания датчиков для различных положений фазовых модуляторов Алисы и Боба при произвольных настройках поляризационного контроллера. Для каждого из положений опыт производился 1000 раз. Результаты моделирования сведены в табл. 2.

Согласно результатам, представленным в табл. 2, поляризационные искажения в оптическом канале не оказывают какого-либо влияния на работу системы, а вероятности срабатывания детекторов соответствуют предписанным по протоколу BB84. Таким образом, проведённый эксперимент свидетельствует о корректности воспроизведения цепочки оптических преобразований в модели и её адекватности.

***Таблица 2.*** *Результаты численной проверки модели*
***Table 2.*** *Summary of model numerical verification*

| Положения модуляторов Modulator positions | | Настройки поляризационного контроллера Polarization controller settings | | | Число срабатываний Number of hits | |
|---|---|---|---|---|---|---|
| $\varphi_A$ | $\varphi_B$ | $\theta_1$ | $\theta_2$ | $\theta_3$ | Детектор A Detector A | Детектор B Detector B |
| 0 | 0 | 48,3 | 163,2 | 55,0 | 1000 | 0 |
| 0 | 0 | 53,1 | 72,8 | 21,1 | 1000 | 0 |
| 0 | π/2 | 33,7 | 145,5 | 115,4 | 509 | 491 |
| 0 | π/2 | 100,8 | 64,8 | 20,4 | 489 | 511 |
| π | 0 | 39,7 | 124,5 | 160,9 | 0 | 1000 |
| π | 0 | 44,9 | 21,5 | 101,9 | 0 | 1000 |
| π | π/2 | 117,9 | 62,5 | 157,3 | 514 | 486 |
| π | π/2 | 127,5 | 166,1 | 78,5 | 521 | 479 |
| π/2 | 0 | 17,5 | 140,1 | 112,9 | 512 | 488 |
| π/2 | 0 | 64,5 | 33,9 | 19,3 | 508 | 492 |
| π/2 | π/2 | 155,5 | 44,0 | 129,3 | 1000 | 0 |
| π/2 | π/2 | 49,8 | 129,8 | 118,0 | 1000 | 0 |
| 3π/2 | 0 | 48,3 | 163,2 | 55,0 | 498 | 502 |
| 3π/2 | 0 | 53,1 | 72,8 | 21,1 | 518 | 482 |
| 3π/2 | π/2 | 33,7 | 145,5 | 115,4 | 0 | 1000 |
| 3π/2 | π/2 | 100,8 | 64,8 | 20,4 | 0 | 1000 |

**Выводы**

Развитие квантовых технологий и их интеграция в информационно-телекоммуникационные сети делают системы КРК особенно актуальными [42]. Это подтверждается не только академическими исследованиями, но и ростом рынка специализированного оборудования [13, 25, 36]. Современные разработки направлены на масштабируемость [22, 29], увеличение дальности передачи [17–20] и повышение устойчивости к атакам [38, 43, 44], что требует тщательного анализа аппаратных решений. В этом контексте важно рассматривать различные архитектуры систем КРК, оценивая их технологическую зрелость и потенциал к практическому внедрению.

Проведённый аналитический обзор известных архитектур систем КРК опирался на различные критерии классификации и позволил оценить уровень технологической готовности многих классов систем. В результате исследования было установлено, что одной из наиболее практичных и широко распространённых архитектур является PnP-QKD, представленная несколькими вариантами реализации. Учитывая их особенности, а также практическую применимость, в качестве базового варианта для дальнейших исследований была выбрана двухпроходная автокорреляционная схема. Однако для объективной оценки её характеристик требуется моделирование, позволяющее воспроизвести ключевые процессы и выявить потенциальные уязвимости.

Имитационное моделирование играет ключевую роль в исследовании и оптимизации систем КРК. Оно позволяет быстро тестировать новые архитектуры и выявлять их уязвимости ещё до практического внедрения. В условиях растущих требований к безопасности и надёжности квантовых коммуникаций моделирование становится необходимым инструментом для совершенствования технологий и ускорения их коммерциализации. Применение этого метода особенно важно для PnP-QKD, поскольку такая архитектура характеризуется сложной компенсацией искажений, что требует точного количественного анализа её параметров.

Разработанная имитационная модель системы КРК на основе архитектуры PnP позволила формально воспроизвести её устойчивость к искажениям поляризации в волоконно-оптическом канале связи. Это подтверждает корректность модели и её применимость для анализа характеристик систем КРК в предполагаемых условиях эксплуатации. Применение математического формализма Джонса и имитационного моделирования в среде Simulink Matlab позволило описать работу оптических компонентов системы. Разработанные модели компонентов могут служить базой для дальнейшего моделирования других архитектур систем КРК, что полезно как в учебных приложениях, так и для оптимизации эксплуатационных характеристик и оценки безопасности разрабатываемых и внедряемых систем.

Дальнейшее развитие работы может включать расширение спектра исследуемых архитектур, а также усложнение моделей оптических компонентов для имитации их неидеальности. В совокупности эти нововведения позволят с высокой физической достоверностью моделировать уязвимости, демонстрировать влияние атак на целостность системы и конфиденциальность генерируемого ключевого материала, а также предварительно оценивать влияние выбираемой компонентной базы на производительность системы. В частности, важное значение для оценки практической применимости систем PnP-QKD имеет анализ их устойчивости к атакам типа «человек посередине», чему будут посвящены последующие исследования.

**СПИСОК ЛИТЕРАТУРЫ**

1. Поткина Е.С., Холопова Л.А. Развитие информационных технологий // Концепт. – 2014. – Спецвыпуск № 09. – ART 14612.
2. Васильева И.Н. Криптографические методы защиты информации. – М.: Изд-во «Юрайт», 2024. – 310 с.

3. Barker E. Recommendation for key management. Part 1: General (NIST Special Publication 800-57 Part 1 Revision 5). – National Institute of Standards and Technology, May 2020. – 170 p. DOI: https://doi.org/10.6028/NIST.SP.800-57pt1r5
4. Quantum computing: progress and prospects / Eds. E. Grumbling, M. Horowitz. – Washington, DC: The National Academies Press, 2019. DOI: https://doi.org/10.17226/25196
5. Shor P.W. Algorithms for quantum computation: discrete logarithms and factoring // Proceedings of the 35th Annual Symposium on Foundations of Computer Science. – 1994. – P. 124–134. DOI: 10.1109/SFCS.1994.365700
6. Магомадов В.С. Квантовые вычисления, квантовая теория и искусственный интеллект // Инженерный вестник Дона. – 2018. – № 4 (51). – 155 с. EDN: YUBSPC
7. Quantum cryptography / N. Gisin, G. Ribordy, W. Tittel, H. Zbinden // Reviews of Modern Physics. – 2002. – Vol. 74. – № 1. – P. 145–195. DOI: 10.1103/RevModPhys.74.145 EDN: LXJNVR
8. Клышко Д.Н., Липкин А.И. О коллапсе волновой функции, квантовой теории измерений и непонимаемости квантовой механики // Исследовано в России. URL: https://cyberleninka.ru/article/n/o-kollapse-volnovoy-funktsii-kvantovoy-teorii-izmereniy-i-neponimaemosti-kvantovoy-mehaniki/viewer (дата обращения: 24.01.2025).
9. Arevalo Aguilar L.M., Garcia Quijas C.P., Robledo C. The improvement of the Heisenberg uncertainty principle // Advanced in Quantum Mechanics. – 2013. – Vol. 4. – P. 67–77. DOI: http://dx.doi.org/10.5772/54530
10. Wootters W., Zurek W. A Single quantum cannot be cloned // Nature. – 1982. – Vol. 299. – P. 802–803. DOI: 10.1038/299802a0
11. Tomamichel M., Leverrier A. A largely self-contained and complete security proof for quantum key distribution // Quantum. – 2017. – Vol. 1. – P. 14. DOI: 10.22331/q-2017-07-14-14. DOI: https://doi.org/10.22331/q-2017-07-14-14
12. Portmann C., Renner R. Cryptographic security of quantum key distribution // arXiv preprint. – 2014. DOI: https://doi.org/10.48550/arXiv.1409.3525
13. Жиляев А.Е., Сабанов А.Г., Шелупанов А.А. Сети квантового распределения ключей в кибербезопасности. – М.: Горячая линия–Телеком, 2023. – 152 с.
14. Resource-efficient real-time polarization compensation for MDI-QKD with rejected data / Olinka Bedroya, Chenyang Li, Wenyuan Wang, Jianyong Hu, Hoi-Kwong Lo, Li Qian // Quantum. – 2024. – Vol. 8. – P. 1435. DOI: https://doi.org/10.22331/q-2024-08-08-1435
15. Experimental demonstration of polarization encoding measurement-device-independent quantum key distribution / Zhiyuan Tang, Zhongfa Liao, Feihu Xu, Bing Qi, Li Qian, Hoi-Kwong Lo // Phys. Rev. Lett. – 2014. – Vol. 112. – Article number 190503. DOI: https://doi.org/10.1103/PhysRevLett.112.190503
16. Bennett C.H., Brassard G. Quantum cryptography: public key distribution and coin tossing // Theoretical Computer Science. – 2014. – Vol. 560. – Part 1. – P. 7–11. DOI: https://doi.org/10.1016/j.tcs.2014.05.025
17. 2 GHz clock quantum key distribution over 260 km of standard telecom fiber / Shuang Wang, Wei Chen, Jun-Fu Guo, Zhen-Qiang Yin, Hong-Wei Li, Zheng Zhou, Guang-Can Guo, and Zheng-Fu Han // Optics Letters. – 2012. – Vol. 37. – Iss. 6. – P. 1008–1010. DOI: https://doi.org/10.1364/OL.37.001008
18. Secure quantum key distribution over 421 km of optical fiber / A. Boaron, G. Boso, D. Rusca, C. Vulliez, C. Autebert, M. Caloz, M. Perrenoud, G. Gras, F. Bussières, M.-J. Li, D. Nolan, A. Martin, H. Zbinden // Phys. Rev. Lett. – 2018. – Vol. 121. – Iss. 19. – Article number 190502. DOI: https://doi.org/10.1103/PhysRevLett.121.190502
19. Phase encoded quantum key distribution up to 380 km in standard telecom grade fiber enabled by baseline error optimization / N.K. Pathak, S. Chaudhary, Sangeeta, B. Kanseri // Scientific Reports. – 2023. – Vol. 13. – № 1. – P. 15868. DOI: 10.1038/s41598-023-42445-y.
20. Twin-field quantum key distribution over 830-km fibre / S. Wang, Z.-Q. Yin, D.-Y. He et al. // Nature Photonics. – 2022. – Vol. 16. – № 2. – P. 154–161 DOI: https://doi.org/10.1038/s41566-021-00928-2 EDN: SRXUKG
21. Данеев О.В. О проблеме квантового распределения ключей: состояние и перспективы // Хроноэкономика. – 2020. – № 2 (23). – С. 19–23.
22. Калачев А.А. Квантовые повторители: текущие разработки и перспективы // Квантовая электроника. – 2023. – Т. 53. – № 8. – С. 609–619. URL: https://openrepository.mephi.ru/handle/123456789/10458 (дата обращения: 24.01.2025).
23. Баринов И.О. Передача квантовых состояний по оптическим каналам связи на основе поляритонов: автореф. дис. … канд. наук. – Владимир, 2013. – 18 с. URL: https://www.dissercat.com/content/peredacha-kvantovykh-sostoyanii-po-opticheskim-kanalam-svyazi-na-osnove-polyaritonov (дата обращения: 24.01.2025).
24. Quantum repeater for continuous-variable entanglement distribution / J. Dias, M.S. Winnel, N. Hosseinidehaj, C.T. Ralph // Phys. Rev. A. – 2020. – Vol. 102. – article number 052425. DOI: https://doi.org/10.1103/PhysRevA.102.052425 EDN: ZEFQEQ
25. Qiu J. Quantum communications leap out of the lab // Nature. – 2014. – Vol. 508. – P. 441–442. DOI: https://doi.org/10.1038/508441a
26. Ralph T.C. Continuous variable quantum cryptography // Physical Review A. – 1999. – Vol. 61. – article number 010303(R). DOI: https://doi.org/10.1103/PhysRevA.61.010303
27. Hillery M. Quantum cryptography with squeezed states // Physical Review A. – 2000. – Vol. 61. – article number 022309. DOI: https://doi.org/10.1103/PhysRevA.61.022309
28. Quantum key distribution using gaussian-modulated coherent states / F. Grosshans, G.V. Assche, J. Wenger, R. Brouri, N.J. Cerf, Ph. Grangier // Nature. – 2003. – Vol. 421. – P. 238–241. DOI: https://doi.org/10.1038/nature01289 EDN: GNJMQN
29. Long-distance continuous-variable quantum key distribution over 100 km fiber with local oscillator / A.A.E. Hajomer, I. Derkach, N. Jain, H.-M. Chin, U.L. Andersen, T. Gehring // arXiv preprint. – 2023. DOI: https://doi.org/10.48550/arXiv.2305.08156
30. Alshaer N., Ismail T., Mahmoud H. Enhancing performance of Continuous-Variable Quantum Key Distribution (CV-QKD) and Gaussian Modulation of Coherent States (GMCS) in Free-Space Channels under Individual Attacks with Phase-Sensitive Amplifier (PSA) and Homodyne Detection (HD) // Sensors. – 2024. – Vol. 24. – № 16. – article number 5201. DOI: https://doi.org/10.3390/s24165201 EDN: FLJYZB
31. Pirandola S., Papanastasiou P. Improved composable key rates for CV-QKD // PhysRevResearch. – 2024. – Vol. 6. – article number 023321. DOI: https://doi.org/10.1103/PhysRevResearch.6.023321

32. Comparison of discrete variable and continuous variable quantum key distribution protocols with phase noise in the thermal-loss channel / S.P. Kish, P.J. Gleeson, A. Walsh, P.K. Lam, S.M. Assad // Quantum. – 2024. – Vol. 8. – P. 1382. DOI: https://doi.org/10.22331/q-2024-06-20-1382
33. High key rate continuous-variable quantum key distribution with a real local oscillator / T. Wang, P. Huang, Y. Zhou, W. Liu, H. Ma, S. Wang, G. Zeng // Optics Express. – 2018. – Vol. 26. – № 3. – P. 2794–2806. DOI: https://doi.org/10.1364/OE.26.002794 EDN: YGCDVZ
34. High-Rate Continuous Variable Quantum Key Distribution Based on Probabilistically Shaped 64 and 256-QAM / F. Roumestan, A. Ghazisaeidi, J. Renaudier, L.T. Vidarte, E. Diamanti, P. Grangier // European Conference on Optical Communication (ECOC) – 2021. – P. 1–4. DOI: 10.1109/ECOC52684.2021.9606013
35. Performance comparison of CV-QKD vs. DV-QKD for access and metro networks. URL: https://www.researchgate.net/figure/Performance-comparison-of-CV-QKD-vs-DV-QKD-for-access-and-metro-networks_fig1_319207301 (дата обращения: 24.01.2025).
36. Прикладные квантовые технологии для защиты информации / под ред. А.Г. Втюриной, В.Л. Елисеева. – М.: Горячая линия – Телеком, 2024. – 148 с.
37. Ekert A.K. Quantum cryptography based on Bell's theorem // Physical Review Letters. – 1991. – Vol. 67. – P. 661–663. DOI: https://doi.org/10.1103/PhysRevLett.67.661
38. Lo H.-K., Curty M., Qi B. Measurement-device-independent quantum key distribution // Physical Review Letters. – 2012. – Vol. 108. – Article number 130503. DOI: https://doi.org/10.1103/PhysRevLett.108.130503
39. "Plug and play" systems for quantum cryptography / A. Muller, T. Herzog, B. Huttner, W. Tittel, H. Zbinden, N. Gisin // Applied Physics Letters. – 1997. – Vol. 70. – P. 793–795. DOI: https://doi.org/10.1063/1.118224
40. Born M., Wolf E. Principles of optics: electromagnetic theory of propagation, interference and diffraction of light. – Cambridge: Cambridge University Press, 1999. – 952 p. DOI: 10.1017/CBO9781139644181
41. Plug-and-play QKD architecture with a self-optical pulse train generator / Min Ki Woo, Chang Hoon Park, Byung Kwon Park, Hojoong Jung, Dongyeon Kang, Seung-Woo Jeon, Sangin Kim, and Sang-Wook Han // Optics Express. – 2022. – Vol. 30. – № 16. – P. 29461–29471. DOI: https://doi.org/10.1364/OE.463283 EDN: LVCAOJ
42. Данеев О.В. О проблеме квантового распределения ключей: состояние и перспективы // Хроноэкономика. – 2020. – № 2 (23). URL: https://cyberleninka.ru/article/n/o-probleme-kvantovogo-raspredeleniya-klyuchey-sostoyanie-i-perspektivy (дата обращения: 24.01.2025).
43. Experimental asymmetric plug-and-play measurement-device-independent quantum key distribution / G.-Z. Tang, S.-H. Sun, F. Xu, H. Chen, C.-Y. Li, L.-M. Liang // Physical Review A. – 2016. – Vol. 94. – № 3. – article number 032326. DOI: https://doi.org/10.1103/PhysRevA.94.032326
44. Source monitoring for plug-and-play continuous-variable quantum key distribution / Yu. Shao, Ya. Pan, H. Wang, A.O. Sun, Zh. Gan, Ya. Pi, T. Ye, J. Liu, Ya. Li, Y. Zhang, W. Huang, B. Xu // Physical review applied. – 2024. – Vol. 22. – № 2. – article number 024033. DOI: https://doi.org/10.1103/PhysRevApplied.22.024033 EDN: KNIHRK

**Информация об авторах**

**Артём Аркадьевич Лукашов**, студент факультета безопасности Томского государственного университета систем управления и радиоэлектроники, Россия, 634050, г. Томск, пр. Ленина, 40. laa@fb.tusur.ru

**Владимир Андреевич Фаерман**, старший преподаватель кафедры комплексной информационной безопасности электронно-вычислительных систем факультета безопасности Томского государственного университета систем управления и радиоэлектроники, Россия, 634050, г. Томск, пр. Ленина, 40. fva@fb.tusur.ru, https://orcid.org/0000-0002-9643-0245

Поступила в редакцию: 17.03.2025
Поступила после рецензирования: 28.05.2025
Принята к публикации: 29.06.2025

**REFERENCES**

1. Potkina E.S., Kholopova L.A. Development of Information Technologies. *Concept*, 2014, Special Issue no. 09, ART 14612. (In Russ.)
2. Vasilieva I.N. *Cryptographic methods of information protection*. Moscow, Yurayt Publ., 2024. 310 p. (In Russ.)
3. Barker E. *Recommendation for key management. Part 1: General (NIST Special Publication 800-57 Part 1 Revision 5)*. National Institute of Standards and Technology, May 2020. 170 p. DOI: https://doi.org/10.6028/NIST.SP.800-57pt1r5
4. *Quantum computing: progress and prospects*. Eds. E. Grumbling, M. Horowitz. Washington, DC, The National Academies Press, 2019. DOI: https://doi.org/10.17226/25196
5. Shor P.W. Algorithms for quantum computation: discrete logarithms and factoring. *Proc. of the 35th Annual Symposium on Foundations of Computer Science*, 1994. pp. 124–134. DOI: 10.1109/SFCS.1994.365700
6. Magomadov V.S. Quantum computing, quantum theory, and artificial intelligence. *Engineering journal of Don*, 2018, no. 4, p. 155. (In Russ.) EDN: YUBSPC
7. Gisin N., Ribordy G., Tittel W., Zbinden H. Quantum cryptography. *Reviews of Modern Physics*, 2002, vol. 74, no. 1, pp. 145–195. DOI: 10.1103/RevModPhys.74.145 EDN: LXJNVR
8. Klyshko D.N., Lipkin A.I. On the collapse of the wave function, quantum theory of measurements and the incomprehensibility of quantum mechanics. *Researched in Russia*. (In Russ.) Available at: https://cyberleninka.ru/article/n/o-kollapse-volnovoy-funktsii-kvantovoy-teorii-izmereniy-i-neponimaemosti-kvantovoy-mehaniki/viewer (accessed: 24 January 2025).

9. Arevalo Aguilar L.M., Garcia Quijas C.P., Robledo C. The improvement of the Heisenberg uncertainty principle. *Advanced in Quantum Mechanics*, 2013, vol. 4, pp. 67–77. DOI: http://dx.doi.org/10.5772/54530.
10. Wootters W., Zurek W. A Single quantum cannot be cloned. *Nature*, 1982, vol. 299, pp. 802–803. DOI: 10.1038/299802a0
11. Tomamichel M., Leverrier A. A largely self-contained and complete security proof for quantum key distribution. *Quantum*, 2017, vol. 1, pp. 14. DOI: 10.22331/q-2017-07-14-14.
12. Portmann C., Renner R. Cryptographic security of quantum key distribution. *arXiv preprint*, 2014. DOI: https://doi.org/10.48550/arXiv.1409.3525
13. Zhiljaev A.E., Sabanov A.G., Shelupanov A.A. *Quantum key distribution networks in cybersecurity*. Moscow, Goryachaya Liniya–Telekom Publ., 2023. 152 p. (In Russ.)
14. Olinka Bedroya, Chenyang Li, Wenyuan Wang, Jianyong Hu, Hoi-Kwong Lo, Li Qian. Resource-efficient real-time polarization compensation for MDI-QKD with rejected data. *Quantum*, 2024, vol. 8, p. 1435. DOI: https://doi.org/10.22331/q-2024-08-08-1435
15. Zhiyuan Tang, Zhongfa Liao, Feihu Xu, Bing Qi, Li Qian, Hoi-Kwong Lo. Experimental demonstration of polarization encoding measurement-device-independent quantum key distribution. *Phys. Rev. Lett*., 2014, vol. 112, article number 190503. DOI: https://doi.org/10.1103/PhysRevLett.112.190503
16. Bennett C.H., Brassard G. Quantum cryptography: public key distribution and coin tossing. *Theoretical Computer Science*, 2014, vol. 560, P. 1, pp. 7–11. DOI: https://doi.org/10.1016/j.tcs.2014.05.025
17. Shuang Wang, Wei Chen, Jun-Fu Guo, Zhen-Qiang Yin, Hong-Wei Li, Zheng Zhou, Guang-Can Guo, Zheng-Fu Han. 2 GHz clock quantum key distribution over 260 km of standard telecom fiber. *Optics Letters*, 2012, vol. 37, Iss. 6, pp. 1008–1010. DOI: https://doi.org/10.1364/OL.37.001008
18. Boaron A., Boso G., Rusca D., Vulliez C., Autebert C., Caloz M., Perrenoud M., Gras G., Bussières F., Li M.-J., Nolan D., Martin A., Zbinden H. Secure quantum key distribution over 421 km of optical fiber. *Phys. Rev. Lett*., 2018, vol. 121, Iss. 19, article number 190502. DOI: https://doi.org/10.1103/PhysRevLett.121.190502
19. Pathak N. K., Chaudhary S., Sangeeta, Kanseri B. Phase encoded quantum key distribution up to 380 km in standard telecom grade fiber enabled by baseline error optimization. *Scientific Reports*, 2023, vol. 13, no. 1, 33. 15868. DOI: 10.1038/s41598-023-42445-y.
20. Wang S., Yin Z.-Q., He D.-Y. Twin-field quantum key distribution over 830-km fibre. *Nature Photonics*, 2022, vol. 16, no. 2, pp. 154–161 DOI: https://doi.org/10.1038/s41566-021-00928-2 EDN: SRXUKG
21. Daneev O.V. On the problem of quantum key distribution: current state and prospects. *Chronoeconomics*, 2020, no. 2 (23), pp. 19–23. (In Russ.)
22. Kalachev A.A. Quantum repeaters: current developments and prospects. *Quantum Electronics*, 2023, vol. 53, no. 8, pp. 609–619. (In Russ.) Available at: https://openrepository.mephi.ru/handle/123456789/10458 (accessed: 24 January 2025).
23. Barinov I.O. *Transmission of quantum states via optical communication channels based on polaritons*. Cand. Diss. Abstract. Vladimir, 2013. 18 p. (In Russ.) Available at: https://www.dissercat.com/content/peredacha-kvantovykh-sostoyanii-po-opticheskim-kanalam-svyazi-na-osnove-polyaritonov (accessed: 24 January 2025).
24. Dias J., Winnel M.S., Hosseinidehaj N., Ralph C.T. Quantum repeater for continuous-variable entanglement distribution. *Phys. Rev. A*, 2020, vol. 102, article number 052425. DOI: https://doi.org/10.1103/PhysRevA.102.052425 EDN: ZEFQEQ
25. Qiu J. Quantum communications leap out of the lab. *Nature*, 2014, vol. 508, pp. 441–442. DOI: https://doi.org/10.1038/508441a
26. Ralph T.C. Continuous variable quantum cryptography. *Physical Review A*, 1999, vol. 61, article number 010303(R). DOI: https://doi.org/10.1103/PhysRevA.61.010303
27. Hillery M. Quantum cryptography with squeezed states. *Physical Review A*., 2000, vol. 61, article number 022309. DOI: https://doi.org/10.1103/PhysRevA.61.022309
28. Grosshans F., Assche G.V., Wenger J., Brouri R., Cerf N.J., Grangier Ph. Quantum key distribution using gaussian-modulated coherent states. *Nature*, 2003, vol. 421, pp. 238–241. DOI: https://doi.org/10.1038/nature01289 EDN: GNJMQN
29. Hajomer A.A.E., Derkach I., Jain N., Chin H.-M., Andersen U.L., Gehring T. Long-distance continuous-variable quantum key distribution over 100 km fiber with local oscillator. *arXiv preprint*, 2023. DOI: https://doi.org/10.48550/arXiv.2305.08156.
30. Alshaer N., Ismail T., Mahmoud H. Enhancing Performance of Continuous-Variable Quantum Key Distribution (CV-QKD) and Gaussian Modulation of Coherent States (GMCS) in Free-Space Channels under Individual Attacks with Phase-Sensitive Amplifier (PSA) and Homodyne Detection (HD). *Sensors*, 2024, vol. 24, no. 16, article number 5201. DOI: https://doi.org/10.3390/s24165201 EDN: FLJYZB
31. Pirandola S., Papanastasiou P. Improved composable key rates for CV-QKD. *PhysRevResearch*, 2024, vol. 6, article number 023321. DOI: https://doi.org/10.1103/PhysRevResearch.6.023321
32. Kish S.P., Gleeson P.J., Walsh A., Lam P.K., Assad S.M. Comparison of discrete variable and continuous variable quantum key distribution protocols with phase noise in the thermal-loss channel. *Quantum*, 2024, vol. 8, pp. 1382. DOI: https://doi.org/10.22331/q-2024-06-20-1382
33. Wang T., Huang P., Zhou Y., Liu W., Ma H., Wang S., Zeng G. High key rate continuous-variable quantum key distribution with a real local oscillator. *Optics Express*, 2018, vol. 26, no. 3, pp. 2794–2806. DOI: https://doi.org/10.1364/OE.26.002794 EDN: YGCDVZ
34. Roumestan F., Ghazisaeidi A., Renaudier J., Vidarte L.T., Diamanti E., Grangier P. High-rate continuous variable quantum key distribution based on probabilistically shaped 64 and 256-QAM. *European Conference on Optical Communication (ECOC)*, 2021, pp. 1–4. DOI: 10.1109/ECOC52684.2021.9606013
35. *Performance comparison of CV-QKD vs. DV-QKD for access and metro networks*. Available at: https://www.researchgate.net/figure/Performance-comparison-of-CV-QKD-vs-DV-QKD-for-access-and-metro-networks_fig1_319207301 (accessed: 24 January 2025).
36. *Applied quantum technologies for information security*. Eds. A.G. Vtyurina, V.L. Eliseev. Moscow, Goryachaya Liniya – Telecom Publ., 2024. 148 p. (In Russ.)

37. Ekert A.K. Quantum cryptography based on Bell's theorem. *Physical Review Letters*, 1991, vol. 67, pp. 661–663. DOI: https://doi.org/10.1103/PhysRevLett.67.661
38. Lo H.-K., Curty M., Qi B. Measurement-device-independent quantum key distribution. *Physical Review Letters*, 2012, vol. 108, article number 130503. DOI: https://doi.org/10.1103/PhysRevLett.108.130503
39. Muller A., Herzog T., Huttner B., Tittel W., Zbinden H., Gisin N. "Plug and play" systems for quantum cryptography. *Applied Physics Letters*, 1997, vol. 70, pp. 793–795. DOI: https://doi.org/10.1063/1.118224
40. Born M., Wolf E. *Principles of optics: electromagnetic theory of propagation, interference and diffraction of light*. Cambridge, Cambridge University Press, 1999. 952 p. DOI: 10.1017/CBO9781139644181
41. Min Ki Woo, Chang Hoon Park, Byung Kwon Park, Hojoong Jung, Dongyeon Kang, Seung-Woo Jeon, Sangin Kim, Sang-Wook Han. Plug-and-play QKD architecture with a self-optical pulse train generator. *Optics Express*, 2022, vol. 30, no. 16, pp. 29461–29471. DOI: https://doi.org/10.1364/OE.463283 EDN: LVCAOJ
42. Daneev O.V. On the problem of quantum key distribution: current state and prospects. *Chronoeconomics*, 2020, no. 2 (23). (In Russ.) Available at: https://cyberleninka.ru/article/n/o-probleme-kvantovogo-raspredeleniya-klyuchey-sostoyanie-i-perspektivy (accessed: 24 January 2025).
43. Tang G.-Z., Sun S.-H., Xu F., Chen H., Li C.-Y., Liang L.-M. Experimental asymmetric plug-and-play measurement-device-independent quantum key distribution. *Physical Review A*, 2016, vol. 94, no. 3, article number 032326. DOI: https://doi.org/10.1103/PhysRevA.94.032326
44. Shao Yu., Pan Ya., Wang H., Sun A.O., Gan Zh., Pi Ya., Ye T., Liu J., Li Ya., Zhang Y., Huang W., Xu B. Source monitoring for plug-and-play continuous-variable quantum key distribution. *Physical review applied*, 2024, vol. 22, no. 2, article number 024033. DOI: https://doi.org/10.1103/PhysRevApplied.22.024033 EDN: KNIHRK

**Information about the authors**

**Artem A. Lukashov**, Student, Tomsk State University of Control Systems and Radioelectronics, 40, Lenin avenue, Tomsk, 634050, Russian Federation. laa@fb.tusur.ru

**Vladimir A. Faerman**, Senior Lecturer, Tomsk State University of Control Systems and Radioelectronics, 40, Lenin avenue, Tomsk, 634050, Russian Federation. fva@fb.tusur.ru, https://orcid.org/0000-0002-9643-0245

Received: 17.03.2025
Revised: 28.05.2025
Accepted: 29.06.2025