

УДК 004.94:681.7

Шифр специальности ВАК: 2.3.6

К.И. Чуков, В.А. Фаерман

Программный комплекс для моделирования оптического тракта системы квантовой коммуникации

Актуальность. Представлен программный комплекс для моделирования оптического тракта систем квантовой коммуникации, основанный на дискретно-событийной обработке фотонных посылок на единой временной шкале. Достоверное моделирование квантового канала необходимо для проектирования и исследования систем квантового распределения ключей. **Цель исследования.** Разработка программного комплекса для моделирования оптического канала и оценки влияния его параметров на характеристики системы. **Методы.** Применено дискретно-событийное моделирование. **Научная новизна.** Предложен программный фреймворк, объединяющий физический и протокольный уровни моделирования, а также математическое обеспечение для оценки совместного влияния физических факторов на характеристики системы. **Результаты.** Разработан программный комплекс, позволяющий оценивать влияние параметров канала и оборудования на QBER и скорость генерации ключа; корректность модели подтверждена вычислительными экспериментами. **Практическая значимость.** Комплекс предназначен для проектирования, прототипирования и верификации систем квантового распределения ключей. **Ключевые слова:** квантовый канал, волоконно-оптическая линия связи, моделирование, лазерный импульс, одноканальный детектор, C++.

DOI: 10.21293/1818-0442-2026-29-2-140-147

Введение

Квантовое распределение ключей (КРК) представляет собой технологию, предназначенную для обеспечения защиты коммуникационных каналов в условиях нарастающей угрозы компрометации традиционных криптосистем, основанных на использовании открытого ключа [1].

Развитие данной технологии происходит во всём мире. По данным Kept (входит в перечень организаций «квантовой экосистемы» ОАО «РЖД»), глобальный рынок квантовых коммуникаций растёт на 31% каждый год, его объём оценивается в 600 млн долл. К 2030 г. он достигнет отметки в 3 млрд долл. [2, 3].

Для изучения и совершенствования систем квантовой коммуникации применяется компьютерное моделирование [4]. Оно позволяет исследовать как верхнеуровневое функционирование системы (протоколы выработки общего ключа, коррекция ошибок и др.), так и низкоуровневое (генерация и рассеивание импульсов, срабатывания детекторов и др.). Это открывает широкие возможности для решения ряда актуальных научно-технических задач, однако большинство существующих моделей рассматривают отдельные компоненты или процессы изолированно, без учета функционирования системы в целом.

Целью данной работы является создание программного комплекса, который позволит сформулировать требования при проектировании и прототипировании оптических каналов систем квантовой коммуникации. Программный комплекс позволит как генерировать данные для их непосредственного анализа, так и для дальнейшего использования в других моделях (например, для согласования ключевого материала или усиления секретности). Модернизация комплекса позволит создать платформу, интегрирующую полный технологический стек КРК.

Обзор комплексов для моделирования систем КРК

Исследование характеристик и особенностей функционирования систем КРК требует применения специализированных программных инструментов. В настоящее время существует широкий спектр решений, созданных как на базе универсальных платформ моделирования [5–12] (MatLab Simulink, COMSOL Multiphysics, NS-3, OMNeT++), так и реализованных как самостоятельные программные комплексы на языках C++, Python и др.

Поиск по запросу «QKD simulation software» в поисковой системе Google Scholar за период с 2021 по 2025 г. показывает около 9550 материалов.

Часто встречающимся инструментом является QKDNetSim [5, 6], разработанный на базе симулятора сетевых протоколов NS-3 [7]. Комплекс ориентирован на изучение поведения сетей, использующих КРК, и позволяет моделировать генерацию и распространение ключей между узлами. Однако данный инструмент не включает моделирование физических эффектов в оптическом тракте, что ограничивает его применение.

OpenQKDSecurity [8], представляет собой модель для оценки нижней границы скорости выработки безопасного ключа. Комплекс использует инструменты MatLab Simulink и позволяет исследовать эффективность различных схем КРК. Основным ограничением является зависимость от проприетарного программного обеспечения MatLab Simulink, которое официально не доступно к покупке.

Среди проприетарных решений, которые можно приобрести на территории Российской Федерации, можно выделить ViPNet QKDSim [9], поддерживающий протоколы BB84, B92 и ГОКС [10]. Программа позволяет учитывать параметры подключае-

мой аппаратной периферии, такие как мощность лазерного излучения, чувствительность детекторов и уровень шумов, а также моделировать различные типы атак. Однако данный продукт в основном предназначен больше для обучения специалистов, чем для проведения исследований.

На базе платформы OMNeT++ построен qkdX [11]. Комплекс реализует несколько протоколов КРК и поддерживает моделирование физических эффектов и явлений. Тем не менее исходный код программы не находится в открытом доступе, что делает невозможным расширение модели или адаптацию под исследовательские задачи.

Среди полностью свободных решений выделяется комплекс SeQUeNCe [12], разработанный на языке Python. Он предоставляет широкий набор возможностей для моделирования квантовых коммуникаций, включая протоколы КРК и физические процессы в канале передачи. Ограничением является сравнительно невысокая производительность, характерная для интерпретируемых языков программирования, что осложняет моделирование больших сетей или длительных процессов передачи.

Ниже представлена сравнительная таблица программных решений для моделирования систем КРК.

В ходе обзора было определено, что существующие программные платформы характеризуются значительным разнообразием функциональных возможностей, однако на данный момент не существует универсального и производительного программного решения, которое бы объединяло низкоуровневое и верхнеуровневое функционирование системы.

В связи с этим было решено разработать программный комплекс:

- обеспечивающий одновременный учет физических процессов в оптическом тракте и параметров протокольного уровня;
- реализующий дискретно-событийную обработку фотонных посылок на единой временной шкале, что позволяет учитывать временные эффекты взаимодействия компонентов;
- обладающий открытой архитектурой, допускающей модификацию и расширение модели;
- обеспечивающий более высокую производительность по сравнению с решениями на интерпретируемых языках, что позволяет моделировать интенсивные потоки импульсов.

Программные комплексы для моделирования системы КРК

Название решения	Работа в реальном времени	Функциональные возможности	Ограничения	Среда моделирования	Тип лицензии	Источник
QKDNetSim	Нет	Генерация, управление и распространение ключей среди узлов сети	Отсутствует моделирование физических эффектов и явлений, отсутствует реализация протоколов КРК	NS-3 (разработан на C++)	Свободная	[5, 6]
OpenQKDSecurity	Нет	Расчёт нижней границы скорости выработки ключа	Отсутствует моделирование физических эффектов и явлений, отсутствует реализация протоколов КРК, зависит от библиотек MatLab, нет поддержки многопоточности	MatLab	Модель распространяется под свободной лицензией, однако MatLab распространяется под проприетарной лицензией	[8]
ViPNet QKDSim	Программный продукт позволяет подключать аппаратную платформу и анализировать поступающую информацию в процессе работы	Демонстрация режимов однофотонного и квазиоднофотонного режимов. Поддерживает протоколы BB84, B92 и ГОКС. Демонстрирует влияние параметров оборудования, таких как чувствительность и шумы детектора, а также влияние атак	Является закрытым ПО	Открытой информации нет	Проприетарное ПО	[9]
qkdX	Нет	Поддержка протоколов различных протоколов КРК. Моделирование физических эффектов и явлений	Является закрытым ПО	OMNeT++	Исходный код не был предоставлен в общий доступ	[11]
SeQUeNCe	Нет	Поддержка протоколов различных протоколов КРК. Моделирование физических эффектов и явлений	Производительность ограничена языком программирования Python	Разработан на языке программирования Python	Свободная	[12]

Описание архитектуры программного комплекса

Для реализации программного комплекса было решено логически разделить его на две составляющие: 1) управляющая утилита; 2) сервисы (набор модулей для моделирования с общим API-интерфейсом). Схема взаимодействия на рис. 1.

Управляющая утилита может представлять собой как программу собственной разработки на каком-либо языке программирования (например, Python), так и инструмент командной строки (например, curl). Основное назначение данной утилиты – организовать взаимодействие с сервисами.

Сервис моделирования включает в себя HTTP-сервер для обработки API-запросов и специализированную библиотеку для моделирования. Ключевым условием для обеспечения унифицированного взаимодействия является соответствие REST API. Выбор языка программирования для реализации сервиса определяется исключительно из задач моделирования.

Требования к сервису моделирования

Для реализации сервиса для моделирования оптического тракта системы КРК были составлены следующие требования:

1. *Язык программирования.* Сервис должен обеспечивать высокую производительность за счёт эффективного управления памятью и многопоточностью, так как количество обрабатываемых импульсов может насчитывать миллионы единиц. В связи с этим решено было использовать C++, который является популярным выбором в высоконагруженных системах.

2. *Структура программного обеспечения.* Структура сервиса должна обеспечивать возможность добавления нового функционала и модернизацию старого. Для соответствия этому требованию разрабатываемый комплекс должен соответствовать базовым принципам объектно-ориентированного программирования (ООП) и SOLID в частности.

3. *Контейнеризация.* Разрабатываемый сервис должен работать в контейнере, чтобы обеспечить переносимость и масштабируемость. Это позволит разворачивать программный комплекс на любой платформе без необходимости устанавливать все зависимости на собственной системе или использовать тяжёлую виртуальную машину.

4. *Сторонние библиотеки.* Использование сторонних библиотек может негативно сказаться на читаемости программного кода. Поэтому решено было ограничиться только теми библиотеками, которые необходимы для работы с JSON-файлами и HTTP-сервером.

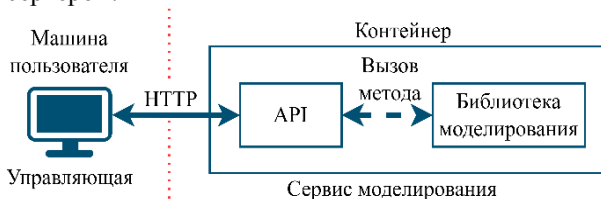


Рис. 1. Схема взаимодействия управляющей утилиты и сервиса моделирования

Описание архитектуры сервиса моделирования

Структура сервиса моделирования представляет собой API-сервер и библиотеку для моделирования (рис. 2), на рис. 3 представлена диаграмма классов. HTTP-сервер представляет собой классы APIRouter и APIController. Библиотека состоит из интерфейсов: ILaser, ISequenceGenerator, IModulator, IQuantumChannel, IBeamSplitter, IPhotodetector, а также классов: AttLaser, mtPNRG, PolarizationModulator, FOCL, PBS, SPAD.

Назначение классов HTTP-сервера:

– APIRouter отвечает за маршрутизацию входящих HTTP-запросов к соответствующим обработчикам API-методов.

– APIController реализует логику обработки запросов. Принимает данные для конфигурации, иницирует запуск выбранного протокола, позволяет получить результаты моделирования и др.

Для реализации HTTP-сервера была выбрана «header-only» библиотека httpplib [13], которая позволяет использовать нужный функционал без необходимости инсталляции различных зависимостей. Данная библиотека открыто распространяется в сети и имеет активное сообщество разработчиков.

Назначение классов сервиса моделирования:

– AttLaser – класс для моделирования лазера с аттенуатором. Учитывается распределение Пуассона для числа фотонов в импульсе, скорость генерации импульсов [14].

– mtPNRG – класс, который реализует интерфейс ISequenceGenerator на основе алгоритма Mersenne Twister. Класс обеспечивает псевдослучайное распределение битов и базисов с большой длиной периода.

– PolarizationModulator – класс, который позволяет моделировать поляризационный модулятор. Реализует преобразование к матрицам Джонса для горизонтальной, вертикальной, диагональной и анти-диагональной поляризаций.

– FOCL – класс для моделирования передачи фотонов через волоконно-оптическую линию связи (ВОЛС). Учитывается влияние затухания сигнала и хроматической дисперсии при различной протяженности канала.

– PBS – класс, который представляет собой реализацию интерфейса IBeamSplitter и моделирует поведение поляризационного светоделителя.

– SPAD – класс, реализующий однофотонный лавинный фотодетектор (ОЛФД). Позволяет задавать основные характеристики ОЛФД, такие как квантовая эффективность, темновой счёт, мёртвое время, вероятность послеимпульса [15].

Описание REST-интерфейса

В предложенной реализации для взаимодействия с библиотекой моделирования предусмотрено 5 основных запросов:

1. *Загрузка конфигурации.* С помощью управляющей утилиты формируется POST-запрос для передачи входных параметров моделирования, например, протокол КРК, мощность лазера, длина квантового канала и др.

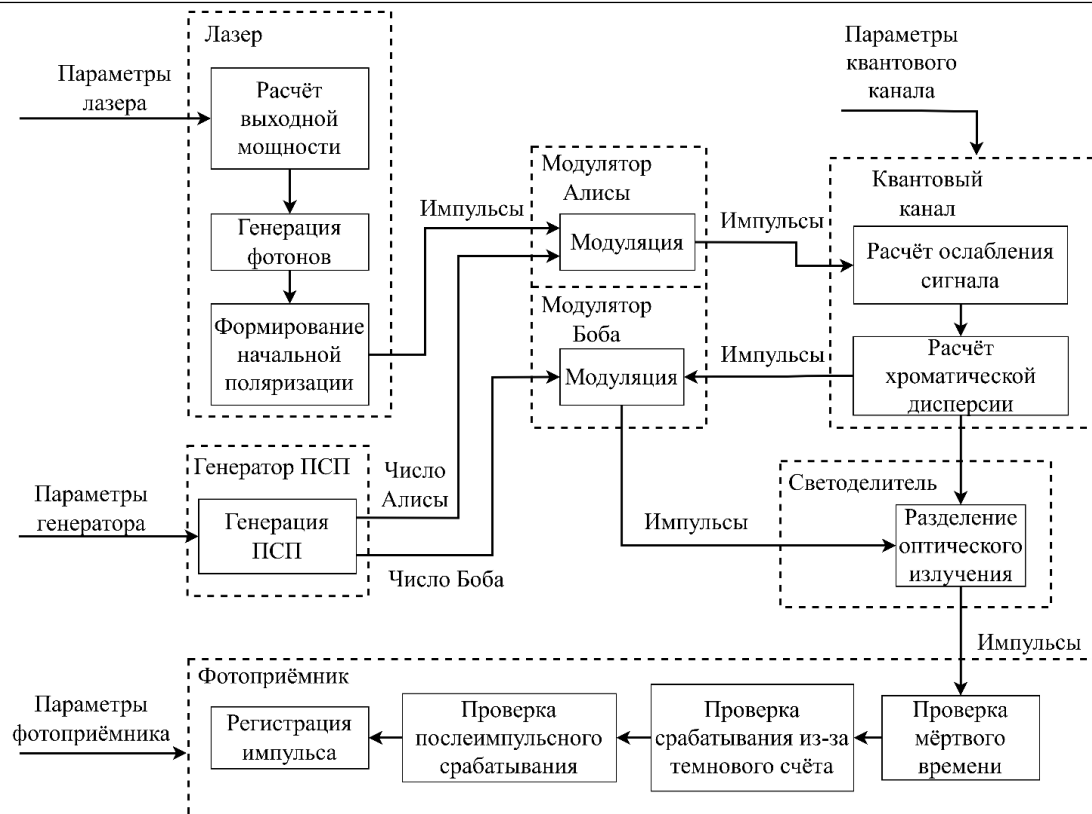


Рис. 2. Архитектура библиотеки моделирования

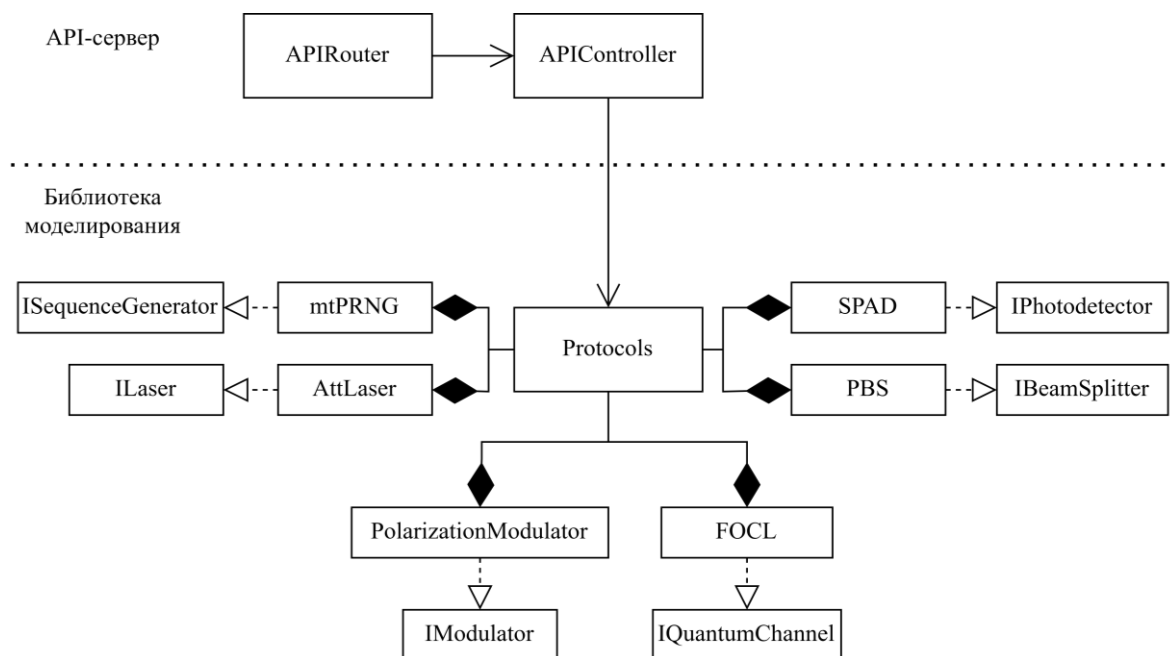


Рис. 3. Диаграмма классов сервиса моделирования

2. *Запуск моделирования.* Для запуска моделирования отправляется простой JSON-объект следующего вида: {"start": true}. В ответ формируется уникальный идентификатор (UUID), соответствующий запущенному сценарию.

3. *Результат моделирования.* По ранее полученному UUID пользователь может получить результаты запущенного сценария. Результаты предоставляются в формате CSV и содержат как входные параметры,

так и выходные: выбранные базисы Алисы и Боба, результат измерения Боба, а также просеянный ключ.

4. *Остановка моделирования.* При работе с сервисом может потребоваться прервать его текущую задачу. Для выполнения данной функции необходимо осуществить отправку соответствующего POST-запроса.

5. *Статус моделирования.* Посредством GET-запроса пользователь может получить информацию,

доступен ли сервис для моделирования в текущий момент.

По завершении моделирования формируется csv-файл с итоговыми результатами. В csv-файле присутствуют входные параметры и следующие заголовки:

- total_pulses – количество отправленных импульсов;
- detected_H – количество зарегистрированных импульсов на детекторе, регистрирующем горизонтальные базисы;
- detected_V – количество зарегистрированных импульсов на детекторе, регистрирующем вертикальные базисы;
- raw_key_length – длина сырого ключевого материала;
- QBER – отношение корректно принятых фотонных посылок к отправленным;
- key_rate – скорость выработки ключа;
- sifted_key – просеянный ключевой материал.

Проведение экспериментов

В рамках работы эксперименты проводились с целью поэтапной верификации разработанной физико-математической модели [16] и программной реализации системы квантового распределения ключей.

Экспериментальная методика строилась на последовательном усложнении условий моделирования: от идеализированных режимов, позволяющих изолированно проверить корректность алгоритмов и протокольной логики, к более реалистичным сценариям, учитывающим затухание в волоконно-оптическом канале, хроматическую дисперсию, конечную квантовую эффективность фотодетекторов, а также ограничения, связанные с временным разрешением и мёртвым временем регистрации детекторов.

Разработанный программный комплекс позволяет проводить параметрические исследования, основанные на систематическом варьировании характеристик основных элементов оптического тракта:

- источника излучения (длина волны, длительность импульса, частота генерации, среднее число фотонов, задаваемое через мощность и аттенюацию), что позволяет анализировать влияние временного перекрытия импульсов и статистики фотонного распределения на вероятность регистрации и уровень ошибок;
- волоконно-оптического канала (длина линии, коэффициент затухания, хроматическая дисперсия), что даёт возможность оценить деградацию сигнала при распространении и её влияние на квантовую битовую ошибку и скорость генерации ключа. При этом предусмотрена возможность изолированного анализа отдельных эффектов за счёт их программного отключения;
- фотодетектора (квантовая эффективность, мёртвое время, вероятность послеимпульсных срабатываний, временное окно регистрации), что позволяет исследовать влияние ограничений однофотонной регистрации на точность измерений и пропускную способность системы.

Помимо однофакторного анализа, комплекс поддерживает проведение многофакторных экспериментов, в рамках которых варьируются несколько параметров одновременно. Это позволяет выявлять нелинейные эффекты и области параметров, в которых наблюдается существенное ухудшение характеристик системы, например, при совместном влиянии длины канала и мёртвого времени детектора.

В результате моделирования формируются выходные данные, на основе которых строятся функциональные зависимости, отражающие поведение системы при изменении параметров, в частности:

$$QBER = f(L), R = f(\nu, \tau), QBER = f(\tau_d, \eta),$$

где L – длина канала, ν – частота генерации импульсов, τ – длительность импульса, τ_d – мёртвое время детектора, η – квантовая эффективность.

На рис. 4 представлен график для эксперимента со следующими параметрами: длина волны лазерного излучения 1550 нм; длина канала 50 км; коэффициент хроматической дисперсии 18 пс/(нм·км); временное окно детектора 2 нс; мёртвое время детектора 4 нс; квантовая эффективность детектора 50%. В качестве основных метрик оценки использовались скорость генерации ключа и отношение зарегистрированных импульсов к отправленным (C_{reg}), что позволяет комплексно охарактеризовать как информационную, так и физическую эффективность системы КРК.

Экспериментальные исследования влияния хроматической дисперсии демонстрируют, что возникающие искажения имеют параметрическую природу и проявляются в характеристиках системы только при определенных сочетаниях длительности импульса, частоты генерации и временного разрешения детектора [16].

Экспоненциальный рост QBER и снижение скорости генерации ключа при увеличении длины канала и при учёте затухания согласуются с теоретическими моделями распространения квантовых состояний в ВОЛС и подтверждают адекватность учёта потерь [17].

Анализ влияния квантовой эффективности фотодетектора и параметров импульсного режима демонстрирует, что модель корректно воспроизводит реальные ограничения однофотонной регистрации, включая влияние временного окна и мёртвого времени детектора.

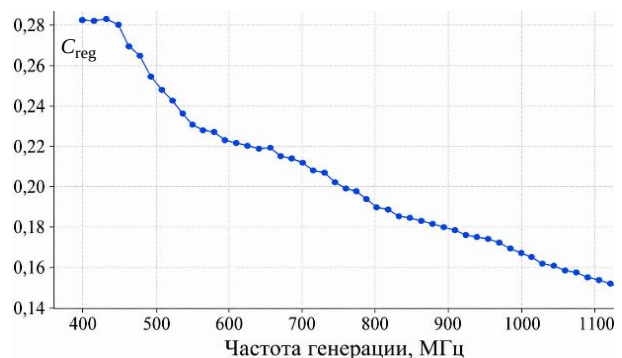


Рис. 4. Зависимость отношения зарегистрированных импульсов от частоты генерации и длительности импульсов

Таким образом, предложенный программный комплекс обеспечивает проведение воспроизводимых вычислительных экспериментов и позволяет исследовать параметрическое пространство модели оптического тракта с учётом временных и вероятностных эффектов, возникающих при передаче и регистрации фотонных посылок, а полученные зависимости подтверждают корректность реализованной модели и алгоритмов.

Заключение

В работе описан разработанный программный комплекс для моделирования оптического тракта системы квантовой коммуникации. Программный комплекс ориентирован на комплексный учёт параметров оптических элементов тракта, на эксплуатационные характеристики системы в целом.

Проведённый обзор существующих решений показал отсутствие универсального и производительного инструмента, объединяющего низкоуровневое моделирование квантового канала и удобные средства интеграции. Предложена архитектура, основанная на сервисной модели с REST API и реализации ключевых компонентов на языке C++, архитектура комплекса ориентирована на эффективную обработку интенсивных потоков событий за счёт реализации на языке C++, модульность и расширяемость, что позволяет адаптировать комплекс под различные исследовательские сценарии.

Предложен дискретно-событийный подход к моделированию оптического тракта систем квантовой коммуникации, основанный на последовательной обработке фотонных посылок на единой временной шкале, что позволяет учитывать взаимное влияние временных характеристик элементов системы (длительности импульсов, мёртвого времени детекторов, временных окон регистрации). Разработана модель представления оптического тракта в виде композиции взаимодействующих компонентов, в которой каждый элемент описывается как преобразование потока событий, что обеспечивает модульное расширение модели без нарушения её целостности. Обеспечена возможность проведения вычислительных экспериментов с высокой интенсивностью потока событий за счёт эффективной реализации алгоритмов обработки посылок на языке C++.

Результаты вычислительных экспериментов подтверждают корректность реализованной физико-математической модели и адекватность учёта основных факторов, влияющих на характеристики систем КРК, включая затухание, дисперсию и параметры однофотонных детекторов. Полученные зависимости квантовой битовой ошибки и скорости генерации ключа согласуются с теоретическими оценками, что позволяет рассматривать разработанный программный комплекс как перспективный инструмент для анализа, верификации и дальнейшего развития систем квантового распределения ключей.

Работа выполнена при финансовой поддержке Министерства науки и высшего образования Российской Федерации в рамках базовой части государ-

ственного задания ТУСУРа на 2026–2028 гг. (проект FEWM-2026-0009).

Литература

1. Реализация средства криптографической защиты информации, использующего квантовое распределение ключей / А.Г. Втюрина, В.Л. Елисеев, А.Е. Жилиев, А.С. Николаева, В.Н. Сергеев, А.В. Уривский // Доклады ТУСУР. – 2018. – Т. 21, № 2. – С. 15–21.
2. 50-кубитный компьютер, шифратор в ЦОД и генераторы для 5G. Как развивалась квантовая индустрия в 2024 году // СберПро [Электронный ресурс]. – URL: https://sber.pro/publication/50-kubitnii-kompyuter-shifrador-v-tsod-i-generatori-dlya-5g-kak-razvivalas-quantovaya-industriya-v-2024-godu/?utm_source=vc_sberpro (дата обращения: 12.11.2025).
3. Центр экспертизы в области квантовых технологий // Kept. – 2024 [Электронный ресурс]. – URL: <https://assets.kept.ru/upload/pdf/2023/09/ru-kept-quantum-services.pdf> (дата обращения: 12.11.2025).
4. Система массового обслуживания в сетях квантового распределения ключей / Д.С. Гекк, В.Д. Пинчук, Д.В. Ожигов, А.О. Терехин // Электронные средства и системы управления: материалы докладов XX Междунар. науч.-практ. конф. (20–22 ноября 2024 г.): в 2 ч. – Ч. 2. – Томск: В-Спектр (ИП В.М. Бочкарева); ТУСУР, 2024. – С. 78–80.
5. Dervisevic E. Large-scale quantum key distribution network simulator / E. Dervisevic, M. Voznak, M. Mehic // Journal of Optical Communications and Networking. – 2024. – Vol. 16, No. 4. – P. 449–462.
6. Soler D. QKDNetSim+: Improvement of the quantum network simulator for NS-3 / D. Soler, I. Cillero et al. // SoftwareX. – 2024. – Vol. 26. – P. 101685.
7. Riley G.F. The ns-3 network simulator. Chapter in Modeling and tools for network simulation / G.F. Riley, T.R. Henderson. – Berlin, Heidelberg: Springer Berlin Heidelberg, 2010. – 537 p.
8. Winick A. Reliable numerical key rates for quantum key distribution / A. Winick, N. Lütkenhaus, P.J. Coles // Quantum. – 2018. – Vol. 2. – P. 77.
9. ViPNet QKDSim. Программный комплекс симуляции квантового распределения ключей [Электронный ресурс]. – URL: <https://infotecs.ru/products/vipnet-qkdsim/> (дата обращения: 12.11.2025).
10. Жилиев А.Е. Сети квантового распределения ключей в кибербезопасности / А.Е. Жилиев, А.Г. Сабанов, А.А. Шелупанов, А.А. Конев, Д.С. Брагин. – М.: Горячая линия – Телеком, 2023. – 152 с.
11. Engle R.D.L. Modeling quantum optical components, pulses and fiber channels using om-net++ / R.D.L. Engle, D.D. Hodson, et al. / arXiv e-prints. arXiv preprint. – 2015. – Art. no. arXiv:1509.03091. DOI: 10.48550/arXiv.1509.03091.
12. Wu X. SeQUeNCe: a customizable discrete-event simulator of quantum networks / X. Wu, A. Kolar, et al. // Quantum Science and Technology. – 2021. – Vol. 6, No. 4. – P. 045027.
13. cpp-http lib // github.com. – URL: <https://github.com/yhirose/cpp-http lib> (дата обращения: 24.10.2025).
14. Махорин Д.А. Статистический контроль распределения числа фотонов в информационных сообщениях в системе квантового распределения ключа с временным кодированием / Д.А. Махорин, А.С. Задорин, С.Ю. Решетников // Электронные средства и системы управления: матер. докладов междунар. науч.-практ. конф. – Томск: ТУСУР, 2015. – № 1-1. – С. 270–273.

15. Курочкин Ю.В. Детекторы одиночных фотонов на основе лавинных фотодиодов / Ю.В. Курочкин, В.Л. Курочкин // Известия вузов. Физика. – 2011. – Т. 54, № 2-2. – С. 202–205.

16. Динамическая модель оптического канала системы квантового распределения ключей в среде MatLab Simulink / К.И. Чуков, В.А. Фаерман, Д.В. Курков, Е.В. Антропов // Известия Том. политехн. ун-та. Промышленная кибернетика. – 2025. – Т. 3, № 2. – С. 24–35.

17. Ландсберг Г.С. Оптика: учеб. пособие. – 6-е изд., стер. – М.: Физматлит, 2003. – 848 с.

18. A practical transmitter device for passive state BB84 quantum key distribution / Yu. Kurochkin, M. Papadovasilakis, A. Trushechkin, R. Piera, J.A. Grieve // arXiv e-prints. – 2024. – Art. no. arxiv.org/html/2405.08481v1.

Чуков Кирилл Игоревич

Аспирант каф. безопасности информационных систем (БИС) Томского государственного университета систем управления и радиоэлектроники (ТУСУР) Ленина пр-т, 40, г. Томск, Россия, 634050
ORCID: 0009-0005-5029-3504
Тел.: +7 (382-2) 70-15-29
Эл. почта: kl-chukov@yandex.ru

Фаерман Владимир Андреевич

Ст. преп. каф. комплексной информационной безопасности электронно-вычислительных систем ТУСУРа Ленина пр-т, 40, г. Томск, Россия, 634050
ORCID: 0000-0002-9643-0245
Тел.: +7 (382-2) 70-15-29
Эл. почта: fva@fb.tusur.ru

Поступила в редакцию: 28.01.2026.

Принята к публикации: 17.07.2026.

Chukov K.I., Fayerman V.A.

Software package for modeling the optical path of a quantum communication system

The paper presents a software package for modeling the optical path of quantum communication systems based on discrete event processing of photonic packets on a unified time scale.

Relevance. Reliable modeling of a quantum channel is essential for the design and investigation of quantum key distribution systems. **Purpose of the study.** Development of a software package for modeling an optical channel and evaluating the effect of its parameters on system characteristics. **Methods.** Discrete event modeling was employed. **Scientific novelty.** A software framework is proposed that integrates the physical and protocol levels of modeling, together with mathematical support for assessing the combined influence of physical factors on system performance. **Results.** A software package has been developed to assess the influence of channel and equipment parameters on the quantum bit error rate (QBER) and key generation rate; the model's validity has been confirmed through computational experiments. **Practical significance.** The software package is intended for the design, prototyping and verification of quantum key distribution systems.

Keywords: quantum channel, fiber-optic communication line, simulation, laser pulse, single-photon detector, C++.

Funding: The work was supported by the Ministry of Science and Higher Education of the Russian Federation within the framework of the basic part of the TUSUR state assignment for 2026-2028 (project FEWM-2026-0009).

DOI: 10.21293/1818-0442-2026-29-2-140-147

References

1. Vtyurina A.G., Eliseev V.L., Zhilyaev A.E., Nikolaeva A.S., Sergeev V.N., Urvskiy A.V. [On the principal decisions of the practical implementation of the cryptographic devices with quantum key distribution]. *Doklady Tomskogo gosudarstvennogo universiteta sistem upravleniya i radioelektroniki*, 2018, vol. 21, no. 2, pp. 15–21.

2. 50-kubitnyy komp'yuter, shifrator v TSOD i generatory dlya 5G. Kak razvivalas' kvantovaya industriya v 2024 godu [50-qubit computer, data center encoder and generators for 5G. How the quantum industry developed in 2024]. Available at: https://sber.pro/publication/50-kubitniy-kompyuter-shifrator-v-tsod-i-generatori-dlya-5g-kak-razvivalas-quantovaya-industriya-v-2024-godu/?utm_source=vc_sberpro (accessed: 11 December 2025) (in Russ.).

3. Tsentral'naya ekspertiza v oblasti kvantovykh tekhnologiy [Center of expertise in the field of quantum technologies]. Kept, 2024. Available at: <https://assets.kept.ru/upload/pdf/2023/09/ru-kept-quantum-services.pdf> (accessed: 12 November 2025).

4. Gekk D.S., Pinchuk V.D., Ozhigov D.V., Terekhin A.O. Sistema massovogo obsluzhivaniya v setyakh kvantovogo raspredeleniya klyuchey [Queueing system in quantum key distribution networks]. *Elektronnyye sredstva i sistemy upravleniya [Electronic means and control systems]*. Proc. of the International Scientific and Practical Conference, Tomsk, V-Spektr (Bochkareva V.M.), TUSUR, 2024, 2 part, pp. 78–80 (in Russ.).

5. Dervisevic E., Voznak M., Mehic M. Large-scale quantum key distribution network simulator. *Journal of Optical Communications and Networking*, 2024, vol. 16, no. 4, pp. 449–462.

6. Soler D. et al. QKDNetSim+: Improvement of the quantum network simulator for NS-3. *SoftwareX*, 2024, vol. 26, pp. 101685.

7. Riley G. F., Henderson T. R. The ns-3 network simulator. In book: Modeling and tools for network simulation. Berlin, Heidelberg, Springer Berlin Heidelberg, 2010, pp. 15–34.

8. Winick A., Lutkenhaus N., Coles P. J. Reliable numerical key rates for quantum key distribution. *Quantum*, 2018, vol. 2, pp. 77.

9. ViPNet QKDSim. Programmnyy kompleks simulyatsii kvantovogo raspredeleniya klyuchey. Available: <https://infotechs.ru/products/vipnet-qkdsim> (accessed: 11 December 2025) (in Russ.).

10. Zhilyaev A.E., Sabanov A.G., Shelupanov A.A., Konev A.A., Bragin D.S. Quantum key distribution networks in cybersecurity. Moscow: Goryachaya liniya – Telekom Publ., 2023, 152 p. (in Russ.).

11. Engle R. D. L. et al. Modeling quantum optical components, pulses and fiber channels using om-net++. arXiv preprint, 2015, Art. no. arXiv:1509.03091, 2015. DOI: 10.48550/arXiv.1509.03091.

12. Wu X. et al. SeQUeNCe: a customizable discrete-event simulator of quantum networks. *Quantum Science and Technology*, 2021, vol. 6, no. 4, pp. 045027.

13. cpp-http-lib. Available: <https://github.com/yhirose/cpp-http-lib> (accessed: 24 October 2025).

14. Makhorin D.A., Zadorin A.S., Reshetnikov S.Y. Statisticheskiy kontrol' raspredeleniya chisla fotonov v infor-

matsionnykh soobshcheniyakh v sisteme kvantovogo raspredeleniya klyucha s vremennym kodirovaniyem [Statistical control of the distribution of the number of photons in information messages in the system of quantum key distribution with time coding] *Elektronnyye sredstva i sistemy upravleniya [Electronic means and control systems]*. Proc. of the International Scientific and Practical Conference, Tomsk: TUSUR, 2015, no. 1-1, pp. 270–273 (in Russ.).

15. Kurochkin Yu.V., Kurochkin V.L. *Detektory odinichnykh fotonov na osnove lavinnykh fotodiodov* [Single photon detectors based on avalanche photodiodes]. *Izvestiya vuzov. Fizika*, 2011, vol. 54, no. 2-2, pp. 202–205 (in Russ.).

16. Chukov K.I., Fayerman V.A., Kurkov D.V., Antropov E.V. [Dynamic model of an optical channel for a quantum key distribution system in MatLab Simulink]. *Bulletin of the Tomsk Polytechnic University. Industrial cybernetics*, 2025, vol. 3, no. 2, pp. 24–35 (in Russ.).

17. Landsberg G.S. *Optika* [Optics]. A textbook, 6th ed., reprinted, Moscow, Fizmatlit, 2003, 848 p (in Russ.).

18. Kurochkin Yu., Papadovasilakis M., Trushechkin A., Piera R., Grieve J.A. A practical transmitter device for passive state BB84 quantum key distribution. arXiv e-prints, 2024, Art. no. arxiv.org/html/2405.08481v1.

Kirill I. Chukov

Postgraduate student, Department of Television and Control, Tomsk State University of Control Systems and Radioelectronics (TUSUR)
40, Lenin Ave., Tomsk, Russia, 634050
ORCID: 0009-0005-5029-3504
Phone: +7 (382-2) 70-15-29
Email: kl-chukov@yandex.ru

Vladimir A. Fayerman

Senior Lecturer, Department of Radio Engineering Systems, TUSUR
40, Lenin Ave., Tomsk, Russia, 634050
ORCID: 0000-0002-9643-0245
Phone: +7 (382-2) 70-15-29
Email: fva@fb.tusur.ru

Received: 28.01.2026.

Accepted: 17.07.2026.