



Московский институт электроники и
математики имени А.Н. Тихонова

Кафедра информационной
безопасности киберфизических
систем

Москва 2025

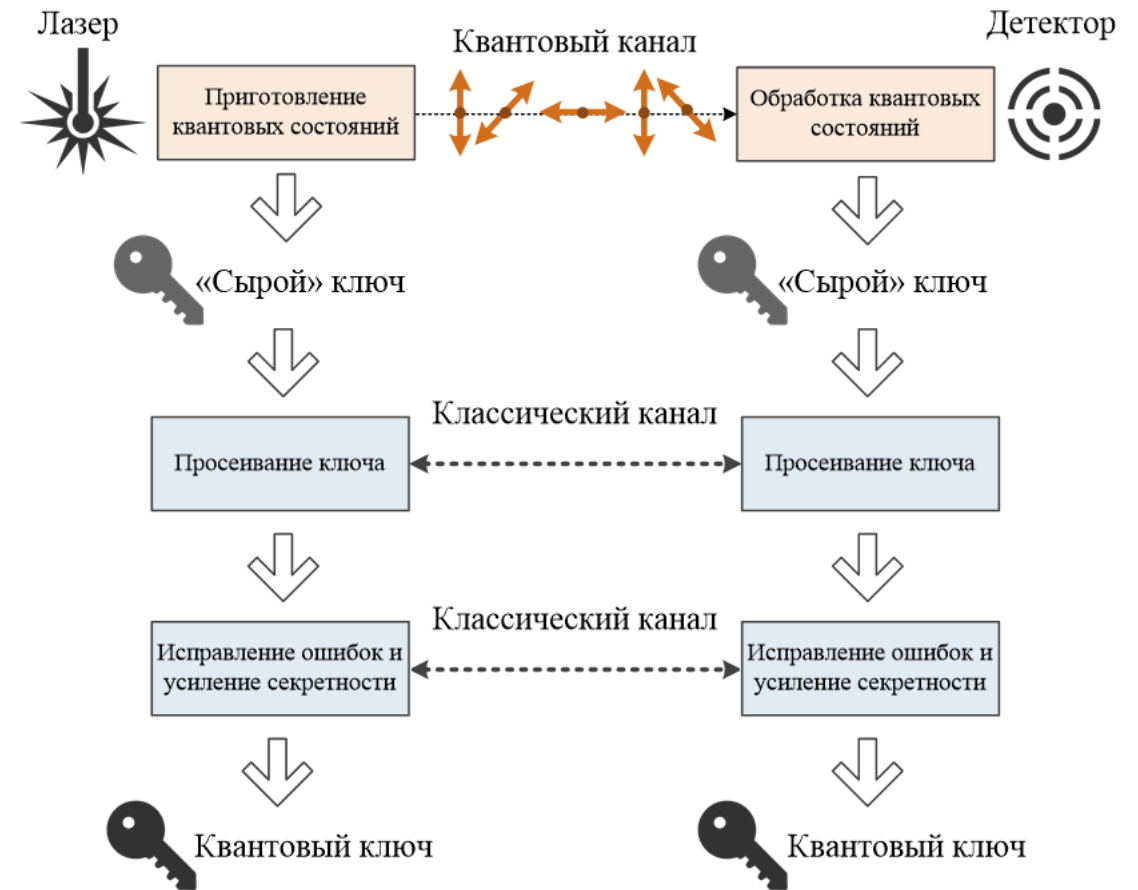
Научный доклад

По теме диссертационного исследования «Разработка алгоритмов повышения эффективности квантового распределения ключей для магистральных линий сверхбольшой протяжённости»

Подготовил:
Аспирант 4 года обучения
Морозов Владимир Игоревич
Научный руководитель:
Евсютин Олег Олегович

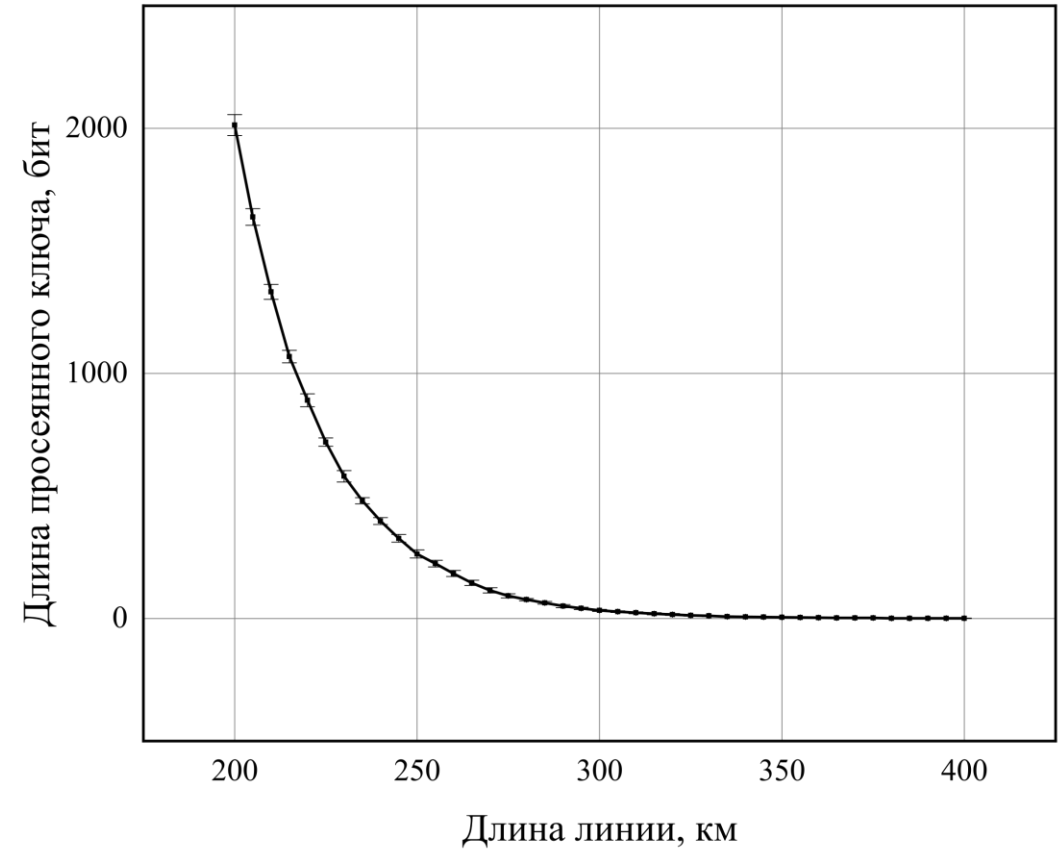
Общая схема квантового распределения ключей

- **Просеивание ключа** – это удаление битов «сырого» ключа значения которых остались неизвестными для принимающей стороны.
- **Очистка ключа** – это исправление ошибок, присутствующих в очищенном ключе в связи с несовершенством принимающей аппаратуры.
- **Усиление секретности** – это хеширование очищенного ключа для уменьшения количества битов на величину, потенциально доступную злоумышленнику.



Недостатки протоколов КРК

- Длина результирующего секретного ключа экспоненциально убывает с ростом длины линии связи
- В просеянном ключе имеется некоторый процент ошибок-инверсий





Обзор существующих работ в области исправления ошибок в КРК

Исследования протоколов BBSS, Cascade, Winnow

Преимущества:

- Высокая эффективность при высоких уровнях ошибки в канале (QBER)
- Простота реализации

Недостатки:

- Высокая нагрузка на сеть
- Большое количество ключевой информации раскрывается злоумышленнику

Исследования протоколов на базе полярных кодов

Преимущества:

- Высокая эффективность при малых уровнях ошибки в канале (QBER)
- Невысокая вычислительная сложность

Недостатки:

- Наибольшая эффективность достигается только при больших размерах кодового слова, что не всегда применимо в КРК

Исследования протоколов на базе LDPC-кодов

Преимущества:

- Высокая эффективность при малом размере кодовых слов
- Невысокая вычислительная сложность

Недостатки:

- На больших размерах кодовых слов проигрывают в эффективности полярным кодам при малых уровнях QBER

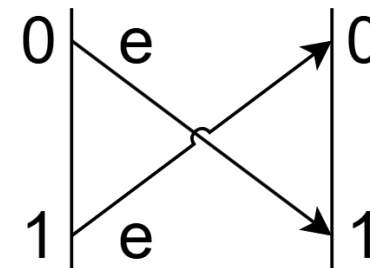
Исследования в области оценки ошибок в квантовом канале

- Метод случайного выбора наиболее универсален, но раскрывает много информации о ключе
- Метод оценки по синдрому раскрывает мало информации, но применим только с LPDC
- Наиболее популярный подход — «слепые» протоколы, в которых оценка ошибки заранее не производится. Могут быть улучшены при наличии оценки ошибки.

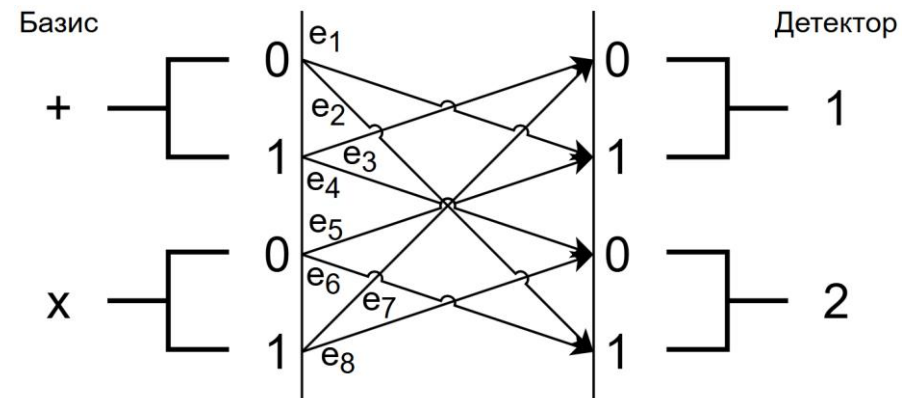
Общая черта существующих работ в области исправления ошибок в КРК

- Рассмотренные в ходе обзора протоколы исправления ошибок применимы к широкому кругу физических реализаций протоколов КРК
- Такая общность не позволяет извлекать пользу из отличительных особенностей отдельных протоколов
- Например, отличительной чертой российского протокола с фазово-временным кодированием является неоднородность ошибок в квантовом канале

Двоичный симметричный канал



Квантовый канал





Тема и цель диссертационного исследования

Тема исследования: разработка алгоритмов повышения эффективности квантового распределения ключей для магистральных линий сверхбольшой протяжённости

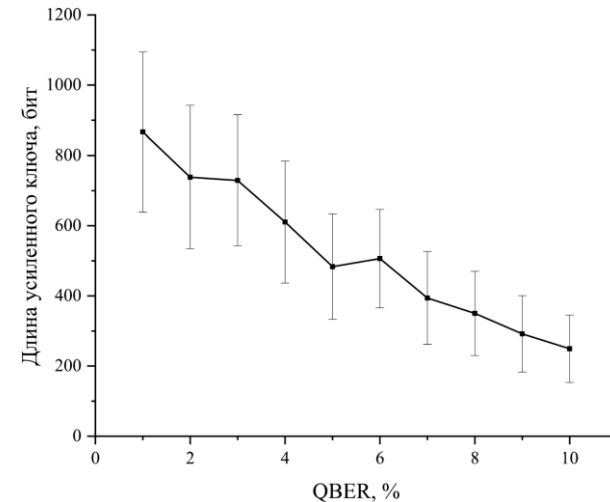
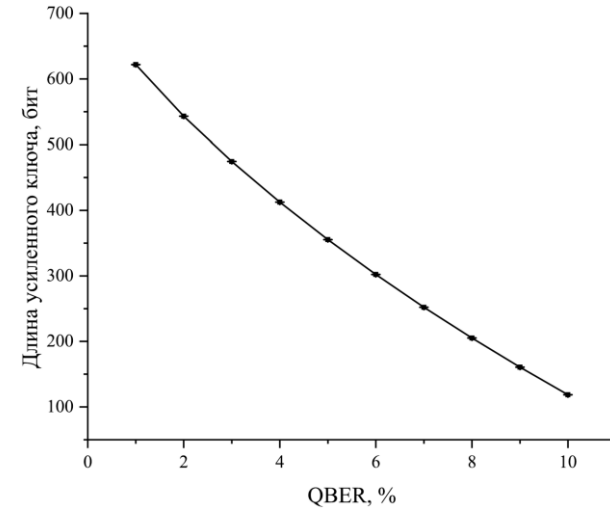
Цель исследования: повышение эффективности протокола квантового распределения ключей с фазово-временным кодированием для магистральных линий сверхбольшой протяжённости за счет разработки новых алгоритмов очистки ключа, отличающихся большей корректирующей способностью.

Задачи:

- Обзор и анализ существующих решений в области алгоритмического обеспечения квантовой криптографии.
- Разработка имитационной модели квантового канала, учитывающей характеристики физической среды передачи.
- Определение возможных модификаций существующих алгоритмов исправления ошибок в протоколах КРК с целью их адаптации к особенностям протокола с фазово-временным кодированием.
- Модификация существующего протокола квантового распределения ключей посредством внедрения адаптированных алгоритмов кодирования с целью увеличения максимальной скорости генерации секретного ключа при заданной протяжённости линии.
- Исследование эффективности полученного решения посредством вычислительной симуляции на программной модели протокола КРК с фазово-временным кодированием.

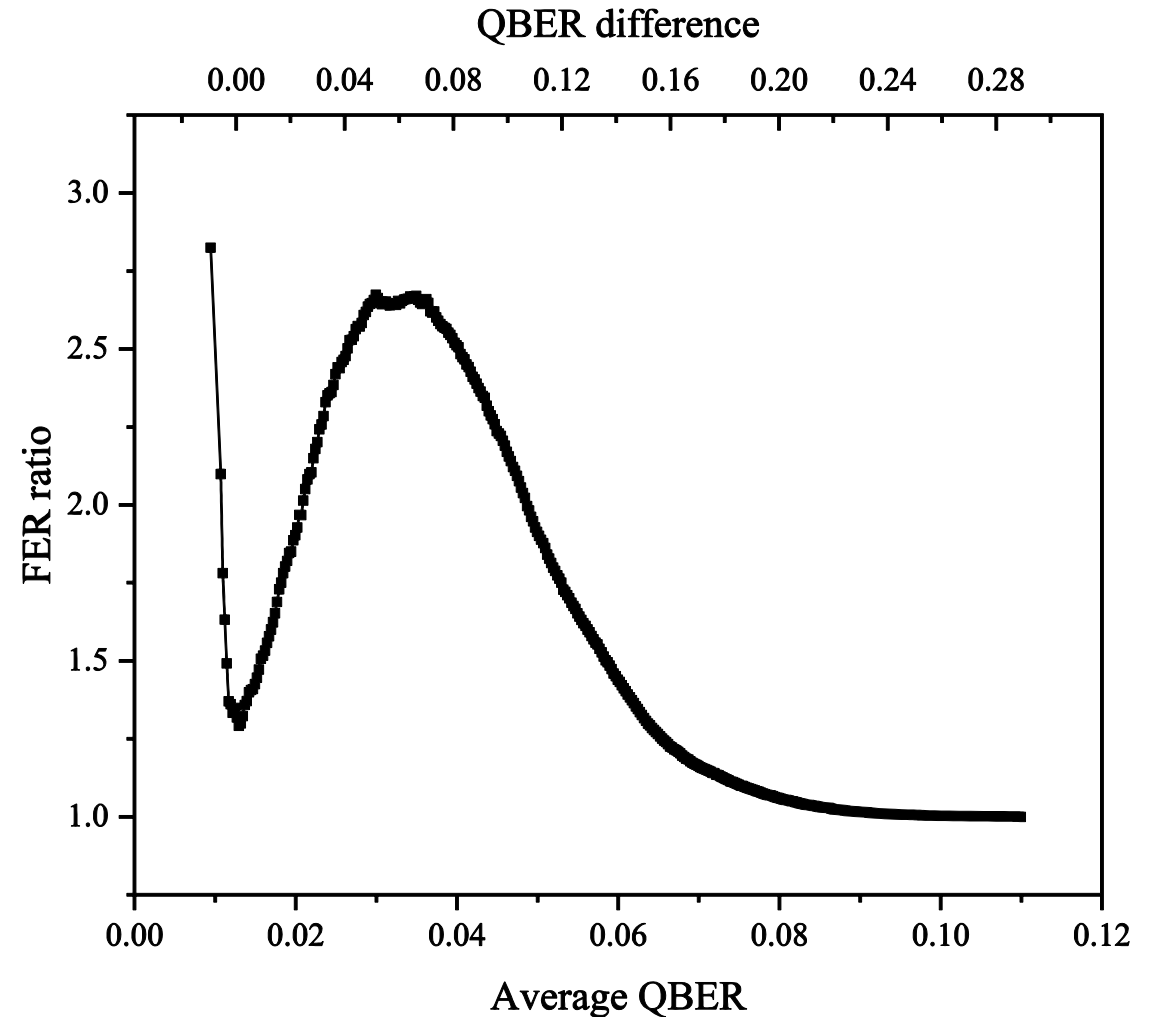
Влияние исправления ошибок на скорость генерации ключа в протоколе с фазово-временным кодированием

- Было экспериментально установлено, что длина результирующего секретного ключа может быть повышена путём использования кодов, более эффективных в заданных условиях
- Для получения зависимости на верхнем рисунке была использована проверочная матрица из стандарта IEEE 802.11n размером 648x1296, на нижнем — 336x672.



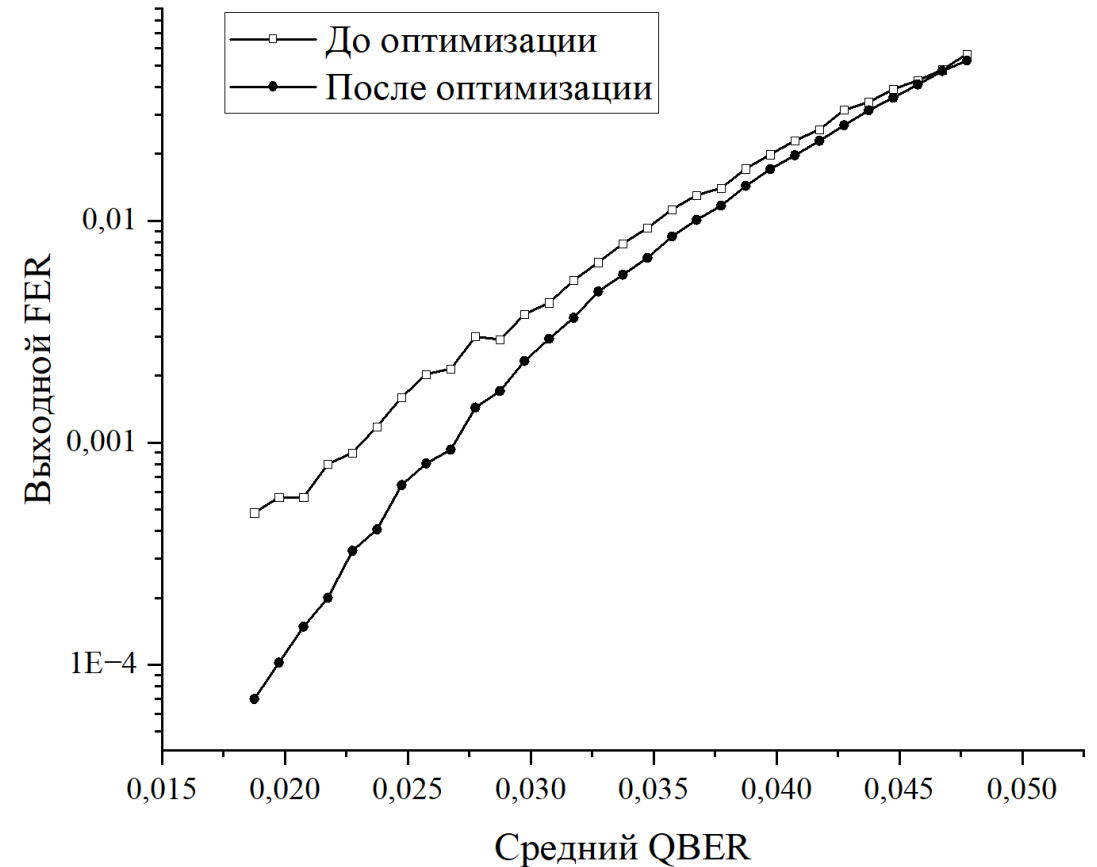
Адаптация процедуры исправления ошибок к особенностям квантового канала

- В результате исследований с макетом системы КРК, реализующей протокол с фазово-временным кодированием, было установлено, что для данного квантового канала характерны следующие уровни QBER: 0.02345, 0.02230, 0.00933 и 0.00910
- На графике представлено отношение выходного FER в подходе без учёта различий в QBER к выходному FER в подходе, где различия учитывались



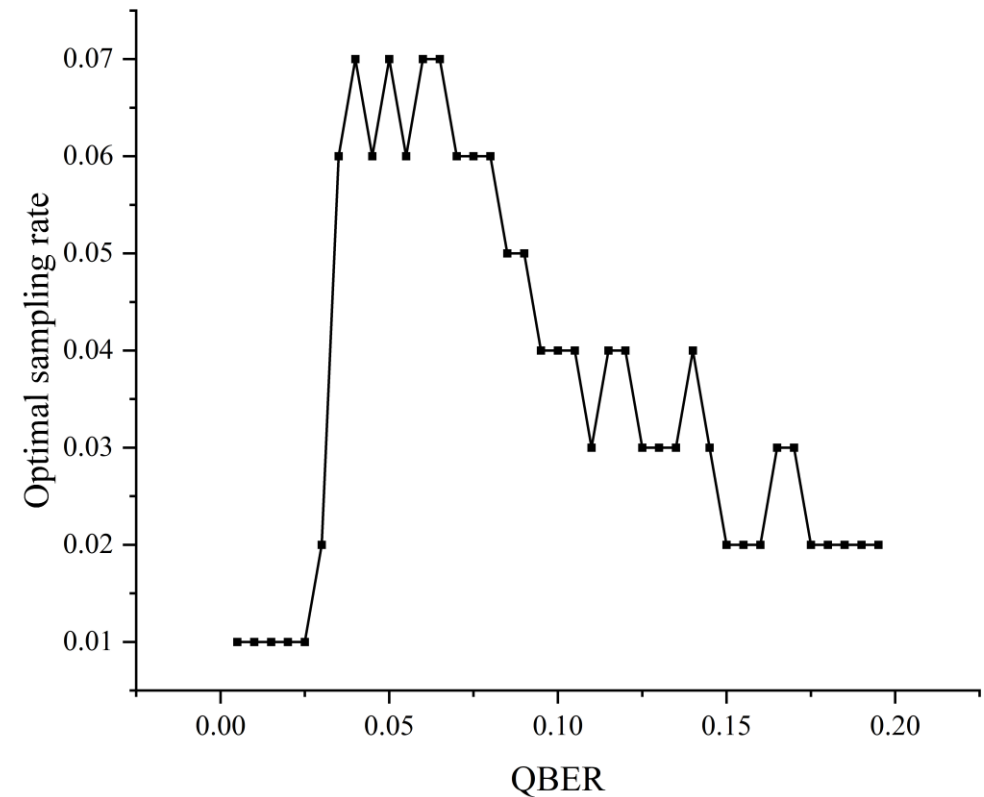
Оптимизация проверочной матрицы LDPC-кода для применения в процедуре исправления ошибок в протоколе КРК

- Для адаптации используемого кода к неоднородности квантового канала был применён жадный алгоритм численной оптимизации
- В качестве стартовой точки оптимизации использовалась проверочная матрица из стандарта 5G размером 88×176
- На рисунке представлен результат 100 итераций оптимизации



Оптимизация доли бит, раскрываемых для оценки ошибок в протоколах КРК, по критерию результирующей длины ключа

- Была экспериментально установлена зависимость оптимальной доли бит ключа, раскрываемых для оценки ошибок, от QBER
- На рисунке представлены результаты для матрицы из стандарта 5G размером 352×1056
- Представленные результаты, а также метод их получения позволяют сократить расход ключевой информации на оценку ошибок





Положения, выносимые на защиту

1. Адаптация процедуры декодирования LDPC-кода к свойствам квантового канала позволяет снизить среднюю вероятность ошибки декодирования на этапе очистки ключа до 2.7 раз на малых входных значениях QBER. Более того такая адаптация всегда даёт коэффициент снижения средней вероятности ошибки больше 1 за пределами области несходимости.
2. Применение жадного алгоритма численной оптимизации проверочной матрицы LDPC-кода BG1 из стандарта 5G позволяет снизить среднюю вероятность ошибки декодирования на этапе очистки ключа до 10 раз на малых входных значениях QBER, что соответствует увеличению метрики эффективности декодирования на 0.3.
3. Предварительная оценка оптимальной доли бит, раскрываемой для оценки ошибки в квантовом канале (QBER), позволяет повысить результирующую длину секретного ключа по сравнению с подходом, где для оценки всегда выбирается фиксированная доля бит ключа.



Апробация результатов исследования

По результатам проведённых исследований были опубликованы следующие работы.

1. Нефедов С. И., Ожегов Р. В., Евсютин О. О., Елезов М. С., Морозов В. И. ПРОБЛЕМЫ СОЗДАНИЯ СИСТЕМ КВАНТОВОГО РАСПРЕДЕЛЕНИЯ КЛЮЧЕЙ ДЛЯ МАГИСТРАЛЬНЫХ ЛИНИЙ БОЛЬШОЙ ПРОТЯЖЕННОСТИ // Наноиндустрия. 2024. Т. 17. № S10-2 (128). С. 553–558. (**Список D**).
2. Морозов В. И., Башара В. О., Емельяненко М. В. Численная оптимизация проверочной матрицы LDPC-кода для применения в протоколе квантового распределения ключей с использованием высокопараллельных вычислений // В кн. : Параллельные вычислительные технологии – XIX всероссийская научная конференция с международным участием, ПаВТ'2025, г. Москва, 8–10 апреля 2025 г. Короткие статьи и описания плакатов. Челябинск: Издательский центр ЮУрГУ, 2025. doi С. 193–210. (**РИНЦ**).
3. V. I. Morozov, O. O. Evsyutin, S. I. Nefedov Study of a Quantum Key Distribution Protocol with Phase-Time Coding Using Simulation Modeling // Problems of Information Transmission. 2025. Vol. 61. No. 1. P. 8–26. (**Список C**).



Апробация результатов исследования

Следующие работы находятся на стадии рецензирования:

1. Vladimir I. Morozov, Mikhail S. Elezov, Oleg O. Evsutin and Roman V. Ozhegov. Adaptation of Error Correction Procedures to the Time-Bin Quantum Key Distribution Protocol Implementation. (На рецензировании в журнале IEEE Access, список A).
2. Vladimir Morozov, Oleg Evsutin, Nikita Yarygin. Sampling Rate Optimization for LDPC-Based Information Reconciliation Protocol in QKD. (На рецензировании для конференции 2025 XIX International Symposium on Problems of Redundancy in Information and Control Systems).

Также результаты данного исследования использовались для выполнения проекта «Разработка научно-технологических принципов сетей связи нового поколения на базе методов квантовой и постквантовой криптографии».



Московский институт электроники и
математики имени А.Н. Тихонова

Кафедра информационной
безопасности киберфизических
систем

Москва 2025

Спасибо за внимание