На правах рукописи

Зеленецкий Алексей Сергеевич

Постквантовый механизм инкапсуляции ключа на основе алгебраических решеток для сетевых протоколов установления защищенного соединения

2.3.2. Вычислительные системы и их элементы

2.3.6. Методы и системы защиты информации, информационная безопасность

АВТОРЕФЕРАТ

диссертации на соискание ученой степени

кандидата технических наук

Москва — 2026

Работа выполнена на кафедре информационной безопасности федерального государственного автономного образовательного учреждения высшего образования «Московский государственный технический университет имени Н.Э. Баумана (национальный исследовательский университет)».

Научный руководитель: **Ключарёв Петр Георгиевич**,
доктор технических наук

Официальные оппоненты: **Сельвесюк Николай Иванович**,
доктор технических наук, доцент, профессор РАН; Федеральное автономное учреждение «Государственный научно-исследовательский институт авиационных систем», заместитель генерального директора — руководитель научного комплекса

Коренева Алиса Михайловна,
кандидат физико-математических наук; Общество с ограниченной ответственностью «Код Безопасности», заместитель руководителя службы сертификации по научно-техническому сотрудничеству

Ведущая организация: Федеральное государственное автономное образовательное учреждение высшего образования «Национальный исследовательский ядерный университет «МИФИ»»

Защита состоится 28 мая 2026 г. в 13:00 на заседании диссертационного совета 24.2.331.19 на базе МГТУ им. Н.Э. Баумана по адресу: 105005, г. Москва, ул. 2-я Бауманская, д. 5, стр. 1, зал Учёного совета ГУК МГТУ им. Н.Э. Баумана.

С диссертацией можно ознакомиться в библиотеке МГТУ им. Н.Э. Баумана и на сайте `bmstu.ru`.

Отзывы на автореферат, заверенные печатью учреждения, просьба направлять по адресу: 105005, г. Москва, ул. 2-я Бауманская, д. 5, стр. 1, Учёному секретарю диссертационного совета 24.2.331.19, кафедра ИУ3.

Автореферат разослан «____» _____ 2026 г.

Ученый секретарь
диссертационного совета 24.2.331.19,
кандидат технических наук, доцент С. А. Сакулин

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Актуальность темы исследования. Сетевые протоколы установления защищённого соединения играют важную роль в обеспечении информационной безопасности в компьютерных сетях. К таким протоколам относятся TLS, SSH, IKEv2 и другие. В ходе своей работы они вызывают протоколы выработки общего секретного ключа, существующие варианты которых уязвимы к атакам с применением квантового компьютера. Поэтому особую актуальность приобретает разработка квантово-устойчивых альтернатив. К числу таких альтернатив относятся постквантовые механизмы инкапсуляции ключа (МИК), представляющие собой протоколы передачи секретного ключа по открытому каналу. Постквантовые криптосистемы обладают стойкостью к атакам с применением как классических, так и квантовых компьютеров. Исследованиями в области постквантовой криптографии занимаются такие отечественные и зарубежные ученые, как Бернштейн Д., Бос Й., Высоцкая В. В., Гребнев С. В., Д'Анверси Ж.-П., Дюкас Л., Киршанова Е. А., Ключарев П. Г., Кудинов М. А., Ланге Т., Любашевский В., Малыгина Е. С., Миччанчо Д., Набоков Д. А., Пейкерт К., Регев О., Турченко О. Ю., Хевельманнс К., Хуслинг А., Чижов И. В. и др.

На сегодняшний день предложено множество постквантовых МИК, отличающихся размерами ключей и шифртекстов, производительностью и криптографической стойкостью. Несмотря на существующее многообразие постквантовых МИК, все они характеризуются большими размерами ключей и шифртекстов и/или низкой производительностью. Также стоит отметить, что некоторые из предложенных постквантовых МИК были успешно взломаны на классических компьютерах, что связано с низкой степенью изученности части методов построения постквантовых криптосистем. Вследствие этого задача разработки нового постквантового МИК остается актуальной. Дополнительным аргументом в пользу актуальности этой задачи является требование российского законодательства об использовании отечественных криптографических стандартов при защите ряда информационных систем. Среди постквантовых МИК особый интерес представляют МИК на решетках. В настоящее время они демонстрируют наилучший баланс между производительностью и размерами ключей и шифртекстов. Более того, их криптографическая стойкость обеспечивается вычислительной сложностью хорошо изученных задач из теории решеток. Таким образом, разработка механизма инкапсуляции ключа на решетках для сетевых

протоколов установления защищенного соединения является актуальной задачей на стыке криптографии и теории сетевых протоколов.

Цели и задачи диссертационной работы. Целью данной диссертации является обеспечение стойкости протоколов выработки общего секретного ключа, используемых в составе сетевых протоколов, к атакам с применением квантового компьютера. Для достижения поставленной цели в диссертационной работе должны быть решены следующие **задачи**:

1. Определить модель злоумышленника для МИК при условии его использования в сетевых протоколах.
2. На основе выбранной модели злоумышленника определить метод построения постквантового МИК на решетках.
3. Разработать постквантовый МИК на основе выбранного метода.
4. Провести оценку теоретико-сложностной стойкости разработанного МИК.
5. Составить наборы параметров для разработанного МИК, провести оценку соответствующей им практической стойкости МИК.
6. Программно реализовать разработанный МИК и сравнить его с известными аналогами по эксплуатационным характеристикам.
7. Исследовать возможность интеграции разработанного МИК в современные сетевые протоколы установления защищенного соединения.

Научная новизна.

1. Разработан новый постквантовый МИК на основе задачи M-LWE, предназначенный для использования в сетевых протоколах установления защищенного соединения.
2. Предложен способ оценки влияния атак, эксплуатирующих ошибки при декапсуляции, на теоретико-сложностную стойкость МИК на основе задачи M-LWE.
3. Предложен способ оценки вычислительной сложности атак, эксплуатирующих ошибки при декапсуляции, на МИК на основе задачи M-LWE.
4. Впервые получена формула, определяющая точное значение показателя рассеивания для систем асимметричного шифрования на основе задачи M-LWE.

Теоретическая значимость. Разработан новый постквантовый МИК на основе задачи M-LWE и обоснована его криптографическая стойкость. Кроме того, предложена новая оценка влияния атак, эксплуатирующих ошибки

при декапсуляции, на теоретико-сложностную стойкость МИК на основе задачи M-LWE. Также в работе впервые получена формула, определяющая точное значение показателя рассеивания для систем шифрования на основе задачи M-LWE. Данные результаты могут быть использованы при анализе криптографической стойкости постквантовых МИК на основе задачи M-LWE.

Практическая значимость. В диссертационной работе продемонстрировано, что реализация разработанного МИК на языке `C` превосходит аналогичные реализации распространенных МИК Kyber и Saber по ряду эксплуатационных характеристик. Кроме того, установлено, что разработанный МИК может быть интегрирован в протоколы TLS 1.3 и IKEv2 без изменения структур сообщений и расширений, определенных их спецификациями. Также разработано оригинальное ПО, позволяющее оценить вычислительную сложность атак, эксплуатирующих ошибки при декапсуляции, на МИК на основе задачи M-LWE.

Методы исследования. Использовались методы теории алгебраических решеток, криптографии, криптографического анализа, теории алгоритмов, теории колец, теории групп и теории вероятностей. Для разработки программного обеспечивания использовались языки программирования `C` и `Python`.

На защиту выносится:

1. Новый постквантовый МИК на основе задачи M-LWE, в котором впервые использованы модуль q, равный степени двойки, и явное оповещение об ошибке при декапсуляции.
2. Результаты анализа криптографической стойкости разработанного МИК.
3. Способ оценки влияния ошибок при декапсуляции на теоретико-сложностную стойкость МИК на основе задачи M-LWE.
4. Формула, определяющая точное значение показателя рассеивания для систем асимметричного шифрования на основе задачи M-LWE.
5. Способ оценки вычислительной сложности атак, эксплуатирующих ошибки при декапсуляции, на МИК на основе задачи M-LWE.
6. Результаты вычислительных экспериментов, подтверждающих преимущество разработанного МИК над механизмами инкапсуляции ключа Kyber и Saber по ряду характеристик.

Достоверность результатов работы подтверждается корректным применением математического аппарата, совокупностью доказанных теорем, а также результатами проведенных вычислительных экспериментов.

Апробация результатов. Результаты диссертации докладывались на Десятой, Одиннадцатой, Двенадцатой и Тринадцатой международной научно-технической конференции «Безопасные информационные технологии» (Москва, 2023 и 2024); на Двадцать третьей международной конференции «Сибирская научная школа-семинар „Компьютерная безопасность и криптография“» (Бийск, 2024); Двадцать восьмой научно-практической конференции «РусКрипто'2025» (Москва, 2025). Результаты диссертации обсуждались в рамках совещаний Рабочей группы «Постквантовые криптографические механизмы» Технического комитета по стандартизации «Криптографическая защита информации» (ТК 26), а также на научных семинарах в МГТУ им. Н. Э. Баумана и НИЯУ МИФИ.

Научные публикации и поддержка. По теме диссертации автором опубликовано 10 научных работ. Из них в изданиях, индексируемых международной системой научного цитирования Scopus, опубликованы 3 научные статьи, в изданиях из перечня ВАК РФ — 2 научные статьи, в сборниках трудов научных конференций — 5 научных публикаций. Работа выполнялась при поддержке гранта в составе стратегического проекта «DeepAnalytics» в рамках государственной программы «Приоритет 2030».

Личный вклад автора. Все представленные в диссертации научные результаты получены лично автором. А именно, новый постквантовый МИК на основе задачи M-LWE, способ оценки влияния атак, эксплуатирующих ошибки при декапсуляции, на теоретико-сложностную стойкость МИК на основе задачи M-LWE, способ оценки вычислительной сложности атак, эксплуатирующих ошибки при декапсуляции, на МИК на основе задачи M-LWE и формула, определяющая точное значение показателя рассеивания для систем асимметричного шифрования на основе задачи M-LWE. На заимствованный материал даны ссылки.

Структура и объем диссертации. Диссертация состоит из введения, четырех глав, заключения, списка литературы и приложения. Полный объем диссертации составляет 234 страницы, включая 28 рисунков и 9 таблиц. Список литературы содержит 157 наименований.

СОДЕРЖАНИЕ РАБОТЫ

Во введении обоснована актуальность диссертационной работы, поставлены цель и задачи, сформулирована научная новизна и показана практическая значимость полученных результатов, представлены выносимые на защиту на-

учные результаты, приведены сведения об апробации и внедрении результатов диссертации.

В первой главе проведен краткий обзор современного состояния предметной области. В рамках диссертации ключевой интерес представляют протоколы формирования общего секретного ключа, используемые во всех современных протоколах установления защищенного соединения. Сегодня в качестве таких протоколов используются различные варианты протокола Диффи–Хеллмана. Однако все они уязвимы к атакам с применением квантового компьютера. Таким образом, возникает потребность в разработке квантово-устойчивой альтернативы.

На сегодняшний день существует два основных подхода к построению таких протоколов. Первый подход, развиваемый в рамках квантовой криптографии, заключается в использовании протокола квантового распределения ключей, криптографическая стойкость которого обеспечивается законами квантовой механики. Однако такой подход обладает рядом существенных ограничений, что делает его применение оправданным лишь в ограниченном числе сценариев. Второй подход является более универсальным и состоит в использовании постквантового механизма инкапсуляции ключа (МИК). Постквантовые криптосистемы обладают стойкостью к атакам с применением как классических, так и квантовых компьютеров.

МИК представляет собой протокол передачи секретного ключа по открытому каналу и относится к асимметричным криптосистемам. Формально, МИК — это тройка полиномиальных алгоритмов KeyGen, Encaps, Decaps и ассоциированное с ней множество сеансовых ключей $\mathcal{K}$. Алгоритм выработки ключевой пары KeyGen — это вероятностный алгоритм, возвращающий пару открытого и секретного ключей (pk, sk). Алгоритм инкапсуляции ключа Encaps является вероятностным алгоритмом, принимающим на вход открытый ключ pk, и возвращающим сеансовый ключ $K \in \mathcal{K}$ и его шифртекст c. Алгоритм декапсуляции ключа $\mathrm{Decaps}(sk, c)$ — это детерминированный алгоритм, принимающий на вход секретный ключ sk и шифртекст c, и возвращающий либо сеансовый ключ $K \in \mathcal{K}$, либо специальный символ $\perp \notin \mathcal{K}$ при возникновении ошибки при декапсуляции. Пример использования МИК для передачи сеансового ключа K от клиента серверу описан на Рис. 1. Современные сетевые протоколы ориентированы на классические криптосистемы, тогда как постквантовые ха-

рактеризуются существенно большими размерами ключей и шифртекстов, что осложняет их интеграцию. Проведенный сравнительный анализ постквантовых МИК показывает, что МИК на решетках достигают наилучшего баланса между производительностью и размерами ключей и шифртекстов. К криптосистемам на решетках относятся криптосистемы, чья стойкость обеспечивается сложностью некоторых задач на решетках. Далее приводится краткий обзор сложных задач на решетках.

Решеткой в конечномерном евклидовом пространстве E называется множество $\Lambda = \{\boldsymbol{x} = \sum_{i=1}^{n} x_i \cdot \boldsymbol{b_i} | x_i \in \mathbb{Z}\}$, где $\boldsymbol{b_1}, \ldots, \boldsymbol{b_n} \in E$ — базис Λ. Ранг Λ равен n, а ее размерностью называется размерность E. У одной и той же решетки бесконечное число базисов. В рамках криптографии на решетках рассматриваются задачи, сводящиеся к поиску «достаточно коротких» векторов некоторой решетки, задаваемой одним из своих базисов. К таким задачам относятся задачи SVP_γ, GapSVP_γ и SIVP_γ. Здесь γ является коэффициентом приближения, выражающимся в виде функции от размерности решетки n. При $\gamma(n) = \mathrm{const}$ перечисленные задачи являются NP-трудными, а при $\gamma(n) = \exp(n)$ для них известны эффективные алгоритмы решения. Вопрос существования эффективных алгоритмов их решения при $\gamma(n) = \mathrm{poly}(n)$ остается открытым. Современные МИК на решетках построены на основе задач, сложность которых ограничена снизу сложностью одной из упомянутых задач с $\gamma(n) = \mathrm{poly}(n)$ на некотором семействе решеток. К таким задачам относятся задачи NTRU, LWE, LWR, а также их частные случаи.

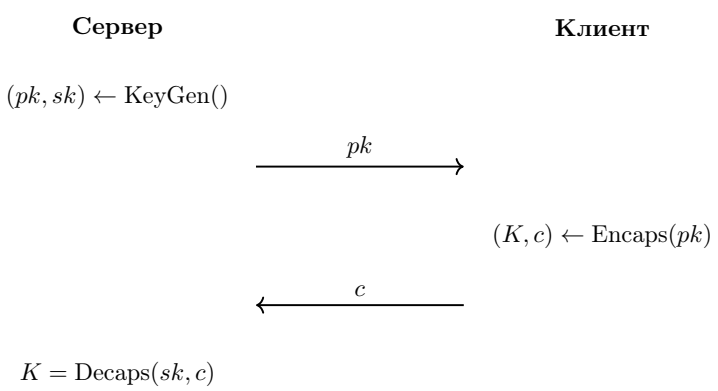

Рис. 1. Передача сеансового ключа K от клиента серверу с использованием МИК

В рамках настоящей работы ключевой интерес представляет модульная версия задачи обучения с ошибками (Module-LWE, M-LWE). Параметрами задачи M-LWE являются кольцо $R = \mathbb{Z}[x]/(x^n + 1)$, где n — степень двойки, целые $q, k, m \geq 2$ и вероятностные распределения χ_s и χ_e над множеством $\mathbb{Z}$. Пусть $R_q = R/(q)$, секретный вектор $\boldsymbol{s} \leftarrow \chi_s^{n \cdot k}$ и вектор шума $\boldsymbol{e} \leftarrow \chi_e^{m \cdot k}$. В задаче

M-LWE по известным параметрам задачи, матрице $\boldsymbol{A} \leftarrow R_q^{m \times k}$ и вектору $\boldsymbol{b} \in R_q^m$ требуется определить, либо $\boldsymbol{b} \leftarrow R_q^m$, либо $\boldsymbol{b} = \boldsymbol{A} \cdot \boldsymbol{s} + \boldsymbol{e}$. Сложность задачи M-LWE ограничена снизу сложностью решения задачи SIVP_γ для полиномиального $\gamma(nk)$ на любой модульной решетке в $L^k = (\mathbb{Q}[x]/(x^n+1))^k$. Модульной решеткой в L^k называется любой R-модуль в L^k.

Во второй главе проводится поэтапное описание разработки постквантового МИК на решетках, предназначенного для использования в сетевых протоколах установления защищенного соединения. Следуя традициям наименования постквантовых криптосистем в Российской Федерации, разработанный постквантовый МИК назван в честь растения, а именно в честь земляники. «Земляника» представляет собой постквантовый IND-CCA стойкий МИК Zemlyanika.KEM, построенный на основе постквантовой IND-CPA стойкой системы асимметричного шифрования Zemlyanila.PKE. Для компактности изложения материала обозначим Zemlyanika.KEM за П, а Zemlyanila.PKE за Σ.

Первым этапом разработки является определение модели злоумышленника, действующего против МИК П. Для описания модели злоумышленника используется наиболее распространенная сегодня теоретико-игровая модель. Так как П ориентирован на применение в сетевых протоколах, он должен обеспечивать стойкость к атакам активного злоумышленника. Более того, передаваемый с помощью МИК сеансовый ключ используется для выработки секретного ключа протокола. Раскрытие хотя бы одного бита сеансового ключа нарушает безопасность протокола. В данных условиях наиболее подходящей моделью злоумышленника является модель IND-CCA. МИК, обладающий стойкостью к атакам IND-CCA злоумышленника, называется IND-CCA стойким.

Вторым этапом разработки является определение метода построения IND–CCA стойкого МИК П. По результатам исследований выбор сделан в пользу следующей конструкции. МИК П получается путем применения преобразования $\mathrm{FO}_m^\perp$ к IND-CPA стойкой системе асимметричного шифрования Σ. Преобразование $\mathrm{FO}_m^\perp$ относится к модификациям преобразования Фуджисаки-Окамото. Такие преобразования обладают рядом преимуществ, что подтверждается их использованием при построении многих современных МИК. В данной работе впервые использовано именно преобразование $\mathrm{FO}_m^\perp$. В сравнении со схожими преобразованиями, оно привносит наименьшее число дополнительных операций в алгоритмы системы шифрования. Его использование стало возможным

благодаря недавним работам по анализу стойкости получаемого МИК к атакам квантового злоумышленника.

Третьим этапом разработки является определение метода построения IND–CPA стойкой системы асимметричного шифрования Σ. По результатам исследований выбор сделан в пользу ее построения на основе задачи M-LWE. Описание Σ представлено на Рис. 2. Ее основными параметрами выступают: (1) кольцо

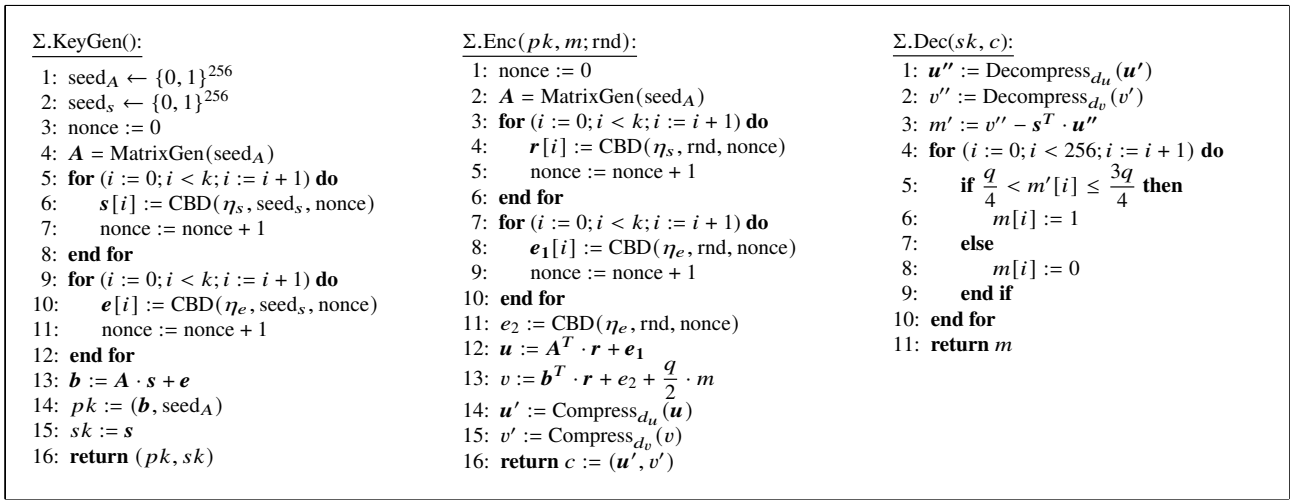

Рис. 2. Описание системы асимметричного шифрования Σ (Zemlyanika.PKE)

$R = \mathbb{Z}[x]/(x^n + 1)$, где $n = 256$, (2) модуль $q = 2^t$, где $t > 1$, (3) ранг модуля $k > 1$, (4) параметры сжатия $0 \leq d_u, d_v < t$ и (5) распределения B_{η_s} и B_{η_e}. За B_η, где $\eta > 0$, обозначается биномиальное распределение, центрированное относительно нуля. Под ним понимается вероятностное распределение над множеством $\{-\eta, \ldots, 0, \ldots, \eta\}$ с функцией вероятности $B_\eta(t) = \binom{2\eta}{\eta+t}/2^{2\eta}$. Также вводится обозначение $R_q = R/(q)$. Сообщение $m \in R/(2)$, оно однозначно представляется в виде двоичной строки длины n. Таким образом, его размер составляет 32 байта. Под набором параметров Σ понимается кортеж $(q, k, \eta_s, \eta_e, d_u, d_v)$.

Открытая матрица $\boldsymbol{A}$ выбирается случайно и равномерно из $R_q^{k \times k}$ с помощью алгоритма MatrixGen. Он принимает на вход случайную бинарную строку длиной 256, обозначаемую за seed_A. Такой способ генерации матрицы выбран с целью сокращения размера pk: вместо целой матрицы передается seed_A. Матрица $\boldsymbol{A}$ генерируется на основе псевдослучайной бинарной строки, полученной путем применения функции расширения входа (eXtendable Output Function, XOF) $\mathcal{X}$ к seed_A.

Компонентами секретных векторов $\boldsymbol{s}, \boldsymbol{r}$ и векторов шума $\boldsymbol{e}, \boldsymbol{e_1}$ являются многочлены из R, распределенные согласно $B_{\eta_s}^{256}$ и $B_{\eta_e}^{256}$, соответственно. Выработка таких многочленов производится с помощью алгоритма CBD, принима-

ющего на вход параметр распределения η, случайную бинарную строку длиной 256 (seed_s, rnd) и одноразовое число nonce. Выборка осуществляется на основе псевдослучайной бинарной строки, полученной с помощью псевдослучайной функции (PseudoRandom Function, PRF) $\mathcal{P}$. Эта функция принимает на вход seed_s (или rnd) и nonce.

Операции $\text{Compression}_d(x)$ и $\text{Decompression}_d(x)$ с параметром $0 \leq d < t$ применяются для сокращения размера шифртекста за счет частичной потери информации. Когда $d = 0$, считается, что эти операции не применяются. Пусть $0 \leq x < q$, тогда $\text{Compression}_d(x) = ((x + 2^{d-1}) \gg d) \bmod 2^{t-d}$, где $\gg$ обозначает битовый сдвиг вправо. Теперь пусть $0 \leq x < 2^{t-d}$, тогда $\text{Decompression}_d(x) = x \ll d$, где $\ll$ обозначает битовый сдвиг влево. Доказано, что применение этих операций вносит дополнительный шум, значение которого распределено равномерно на множестве $\{-2^{d-1} + 1, \ldots, 2^{d-1}\}$. Обе операции применяются к многочленам из R_q и векторам из R_q^k покомпонентно.

Ошибкой при расшифровании называется событие, при котором

$$m \neq \Sigma.\text{Dec}(sk, \Sigma.\text{Enc}(pk, m; r)). \tag{1}$$

Показателем корректности δ называется вероятность возникновения ошибки при расшифровании в среднем. Показатель корректности Σ рассчитывается по формуле

$$\delta = \Pr[\|\boldsymbol{e}^T \cdot \boldsymbol{r} - \boldsymbol{s}^T \cdot (\boldsymbol{e_1} + \boldsymbol{e_u}) + e_2 + e_v\|_\infty < q/4], \tag{2}$$

где $\boldsymbol{s}, \boldsymbol{r} \leftarrow B_{\eta_s}^{n \cdot k}$, $\boldsymbol{e}, \boldsymbol{e_1} \leftarrow B_{\eta_e}^{n \cdot k}$, $e_2 \leftarrow B_{\eta_e}$, $\boldsymbol{e_u} \leftarrow \{-2^{d_u-1} + 1, \ldots, 2^{d_u-1}\}^{n \cdot k}$ и $e_v \leftarrow \{-2^{d_v-1} + 1, \ldots, 2^{d_v-1}\}^n$. Для расчета δ используется ПО, разработанное на `Python`.

Ключевой особенностью Σ является выбор в качестве модуля q степени двойки. Во всех аналогичных системах шифрования q выбирается простым числом для применения эффективного умножения многочленов на основе NTT. С другой стороны, такой выбор избавляет от необходимости приведения чисел по модулю. Оно выполняется автоматически за счёт особенностей машинной арифметики. Автором было показано, что в случае МИК Kyber, для которого модуль q — простое число, наличие операций приведения по модулю заметно влияют на производительность. Кроме того, степень двойки обеспечивает более эффективную генерацию открытой матрицы $\boldsymbol{A}$. Таким образом, выдвину-

та гипотеза, что преимущества данного выбора могут перевесить недостаток, связанный с более медленным умножением многочленов.

Описание построенного МИК П представлено на Рис. 3. Сеансовый ключ,

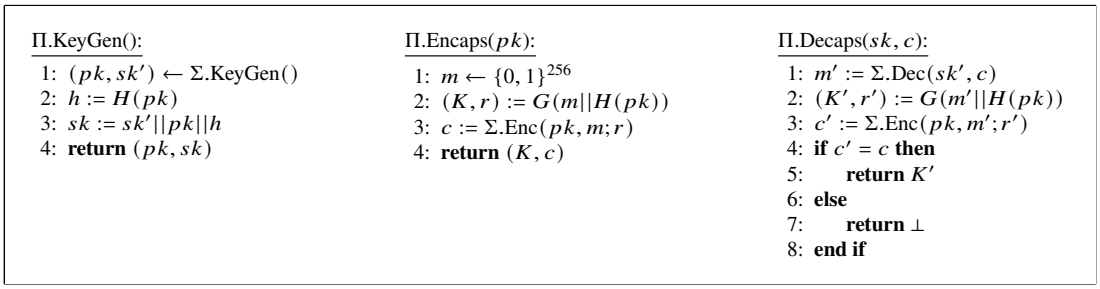

Рис. 3. Описание МИК П (Zemlyanika.KEM)

передаваемый с помощью П, имеет длину 32 байта, что соответствует требованиям современных сетевых протоколов. $G : \{0,1\}^* \to \{0,1\}^{512}$ и $H : \{0,1\}^* \to \{0,1\}^{256}$ являются криптографическими хэш-функциями. Под набором параметров П понимается набор параметров Σ. Ошибкой при декапсуляции называется событие, при котором на корректно сформированном шифртексте алгоритм декапсуляции возвращает $\perp$. Ошибка при декапсуляции происходит тогда и только тогда, когда происходит ошибка при расшифровании.

В третьей главе представлены результаты анализа криптографической стойкости МИК П, на основе которого предложено четыре набора параметров. Они приведены в Таблице 1. Остальные параметры П одинаковы для всех наборов

Таблица 1.

Наборы параметров для МИК П (Zemlyanika.KEM)

#	q	k	η_s	η_e	d_u	d_v	$\log_2(\delta)$	λ
Z512	1024	2	1	1	0	6	-149	128 (64)
Z768-R	1024	3	1	1	0	0	-125	192 (96)
Z768-C	2048	3	2	1	1	5	-156	192 (96)
Z1024	2048	4	2	1	0	6	-168	256 (128)

параметров и определены следующим образом. В качестве хэш-функций H и G используется отечественная хэш-функция «Стрибог». В качестве PRF $\mathcal{P}$ используется отечественная PRF «Streebog-K». В качестве XOF $\mathcal{X}$ используется модификация «Стрибог», принимающая на вход конкатенацию входа $\mathcal{X}$ и счетчика.

Наборы параметров для построенного МИК выбирались таким образом, чтобы они обеспечивали практическую стойкость МИК на уровнях 128 (64), 192 (96) и 256 (128) бит при условии действия классического (квантового) злоумышленника. Уровень практической стойкости, соответствующий набору парамет-

ров, указан в столбце λ Таблицы 1. Под практической стойкостью понимается вычислительная сложность алгоритма, реализующего наилучшую в определенном смысле атаку на криптосистему. Практическая стойкость криптосистемы, обладающей уровнем практической стойкости λ бит, равна $O(2^{\lambda})$.

Для выявления возможных сценариев атак проводится анализ теоретико–сложностной стойкости П. Этот анализ сводится к оценке преимущества IND–CCA злоумышленника $\mathcal{A}$. МИК П считается IND-CCA стойким, если это преимущество пренебрежимо мало относительно λ. При его оценке необходимо учитывать влияние ошибок при декапсуляции. Это связано с тем, что каждая ошибка при декапсуляции раскрывает малую часть информации о секретном ключе. Атаки, нацеленные на получение секретной информации за счет вызова ошибок при декапсуляции, называются атаками, эксплуатирующими ошибки при декапсуляции. Возможность осуществления таких атак увеличивает преимущество злоумышленника. Существует два основных подхода к оценке их влияния на преимущество злоумышленника. Достоинство первого подхода заключается в том, что для его применения достаточно знать показатель корректности δ. Однако он исходит из избыточных возможностей злоумышленника. Это влечет завышенные требования к δ, что негативно сказывается на эксплуатационных характеристиках МИК.

Второй подход позволяет получить более точную оценку. Однако для его применения требуется оценка вероятности генерации пассивным злоумышленником $\mathcal{B}$ сообщения m, приводящего к ошибке при расшифровании. При этом аргумент rnd алгоритма зашифрования определен значением $G(m||H(pk))$. Предложен новый способ оценки рассмотренной вероятности. Пусть m — произвольное сообщение, тогда $\mathcal{B}$ может рассчитать вероятность $p(m)$ того, что m вызовет ошибку при расшифровании:

$$p(m) = \Pr[||\boldsymbol{e}^T \cdot \boldsymbol{r} - \boldsymbol{s}^T \cdot (\boldsymbol{e_1} + \boldsymbol{e_u}) + e_2 + e_v||_\infty \geq q/4], \tag{3}$$

где $\boldsymbol{e} \leftarrow B_{\eta_e}^{n \cdot k}$, $\boldsymbol{s} \leftarrow B_{\eta_s}^{n \cdot k}$, а остальные члены определены значением m. Введем также две функции на множестве $(0, 1)$:

$$\alpha(f) = \Pr_{m \leftarrow \mathcal{M}}[p(m) > f] \tag{4}$$

и

$$\beta(f) = \frac{\sum\limits_{q>f} q \cdot \Pr\limits_{m \leftarrow \mathcal{M}}[p(m) = q]}{\alpha(f)}. \tag{5}$$

Функция $\alpha(f)$ является вероятностью генерации сообщения m с $p(m) > f$, а $\beta(f)$ — математическим ожиданием вероятности возникновения ошибки при расшифровании такого сообщения. Доказано, что при условии сложности задачи M-LWE искомая вероятность равна $\beta(f)$. При этом $\mathcal{B}$ использует порядка $\alpha(f)^{-1}$ ($\sqrt{\alpha(f)}^{-1}$) операций на классическом (квантовом) компьютере. Применение этого способа позволяет увеличить значение δ для набора параметров Z768-R, что способствует улучшению эксплуатационных характеристик МИК.

При оценке преимущества $\mathcal{A}$ также используется оценка показателя рассеивания γ системы шифрования Σ. Под показателем рассеивания системы шифрования Σ понимается такое $\gamma > 0$, что для всех ключей (pk, sk) и сообщений m выполняется $\max\limits_{c \in C} \Pr[\Sigma.\mathrm{Enc}(pk, m) = c] \leq 2^{-\gamma}$, где C — множество шифртекстов. В теореме 1 представлена впервые полученная формула, определяющая значение γ, для систем шифрования на основе задачи M-LWE.

Теорема 1. *Система асимметричного шифрования на основе задачи M-LWE с параметрами $R = \mathbb{Z}[x]/(x^n + 1)$, где n — степень двойки, k, q, χ_s и χ_e является γ-рассеянной с показателем рассеивания*

$$\gamma = \left(\max_{x \in \mathrm{supp}(\chi_e)} \chi_e(x) \right)^{n \cdot (k+1)}. \tag{6}$$

С использованием этой формулы, установлено, что для всех наборов параметров параметр $\gamma \geq 768 \cdot \log_2(4/3)$, что сокращает поверхность атак П.

Результаты анализа теоретико-сложностной стойкости позволяют выделить три сценария атак на разработанный МИК:

1. Решение лежащей в основе МИК задачи M-LWE;
2. Атаки на псевдослучайную функцию $\mathcal{P}$;
3. Атаки, эксплуатирующие ошибки при декапсуляции.

Оценка сложности решения задачи M-LWE проведена с использованием библиотеки `lattice-estimator` для `Python`. Полученные оценки позволяют заключить, что предложенные наборы параметров соответствуют заявленному уровню практической стойкости к атакам на задачу M-LWE. Результаты анализа известных атак на функцию «Streebog-K» также свидетельствуют в пользу заяв-

ленного уровня практической стойкости. Для оценки сложности атак, эксплуатирующих ошибки при декапсуляции, используется новый способ. Очевидно, что сложность любой такой атаки не меньше сложности вызова хотя бы одной ошибки при декапсуляции. Обосновано, что число запросов на декапсуляцию, доступных злоумышленнику, не превышает 2^{64}. Таким образом, при условии сложности M-LWE для успешной атаки требуется, чтобы $\beta(f) \approx 2^{-64}$. Под зависимостью $\beta(\alpha)$ понимается зависимость значения $\beta(f)$ от значения $\alpha(f)$ при одном и том же f. Эта зависимость получена для набора параметров Z768-R, ее график продемонстрирован на Рис. 4. Для вычисления этой зависимости разработано ПО на языке `Python`. Таким образом, проведение успешной атаки требует выполнения более чем 2^{800} (2^{400}) операций на классическом (квантовом) компьютере. Таким образом, эти атаки не могут быть применены против МИК П. Последнее объясняется тем, что Z768-R обладает наименьшим показателем корректности δ среди всех наборов параметров.

В четвертой главе представлены обзор программной реализации МИК П, результаты сравнения разработанного МИК с МИК Kyber и Saber, а также результаты анализа возможности его интеграции в сетевые протоколы TLS 1.3 и IKEv2. Программная реализация разработана на языке `C`. Проведено ее сравнение с эталонными реализациями Kyber и Saber. Результаты сравнения представлены в Таблице 2. Все размеры даны в байтах, время работы алгоритмов измерено в микросекундах. Все измерения проводились на одном ядре процессора архитектуры ARM64 (Apple M1) с тактовой частотой 3200 МГц. Под уровнем классической (квантовой) стойкости понимается уровень практической стойкости к атакам с применением классического (квантового) компьютера. По результатам сравнения видно, что МИК П превосходит Kyber и Saber по многим эксплуатационным характеристикам, что свидетельствует в пользу

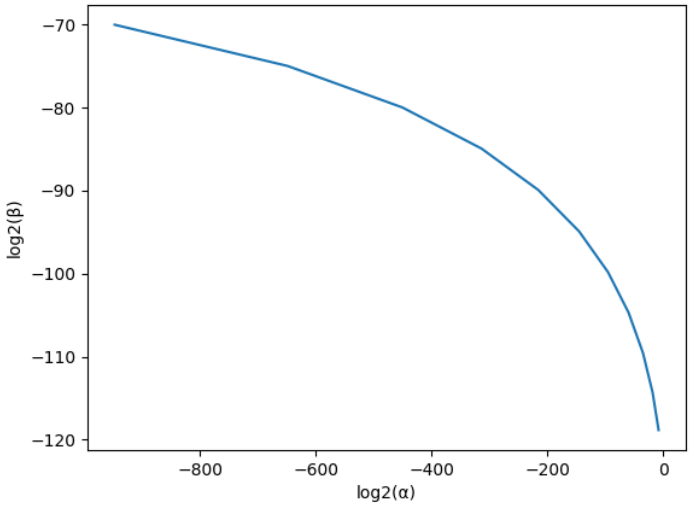

Рис. 4. Зависимость $\beta(\alpha)$ для набора параметров Z768-R

Таблица 2.

Сравнение эксплуатационных характеристик разработанной программной реализации МИК с эталонными реализациями Kyber и Saber

Набор параметров	$\|sk\|$, Б	$\|pk\|$, Б	$\|ct\|$, Б	KeyGen, мкс	Encaps, мкс	Decaps, мкс	Уровень классической стойкости	Уровень квантовой стойкости
Z512	832	672	768	11.5	15.1	14.5	128	64
Kyber512	1632	800	768	21.2	24.5	28.0	128	64
LightSaber	1568	672	736	17.0	21.6	23.3	128	64
Z768-R	1216	992	1280	20.7	21.7	21.3	192	96
Z768-C	1408	1088	1152	23.3	25.3	25.8	192	96
Kyber768	2400	1184	1088	33.1	37.8	42.9	192	96
Saber	2304	992	1088	31.4	37.9	32.3	192	96
Z1024	1856	1440	1568	33.2	38.4	40.7	256	128
Kyber1024	3168	1568	1568	50.8	54.4	61.0	256	128
FireSaber	3040	1312	1472	50.1	50.5	46.7	256	128

практической эффективности предложенных в ходе его разработки решений. Кроме того, согласно результатам проведенных исследований, разработанный МИК может быть интегрирован в протоколы TLS 1.3 и IKEv2 без изменения структур сообщений и расширений, задаваемых их спецификациями.

В заключении перечислены основные полученные в диссертации результаты, которые заключаются в следующем:

1. Проведен аналитический обзор современных постквантовых МИК.
2. Разработан постквантовый МИК Zemlyanika.KEM на основе задачи M-LWE. Впервые в данной конструкции использовано значение модуля q, равное степени двойки, и явное оповещение об ошибке при декапсуляции.
3. Предложена новая оценка влияния атак, эксплуатирующих ошибки при декапсуляции, на теоретико-сложностную стойкость МИК на основе задачи M-LWE.
4. Проведен анализ теоретико-сложностной стойкости Zemlyanika.KEM.
5. Впервые получена формула, определяющая точное значение показателя рассеивания для систем асимметричного шифрования на основе задачи M-LWE.
6. Предложен новый способ анализа вычислительной сложности атак, эксплуатирующих ошибки при декапсуляции, на МИК на основе задачи M-LWE.
7. Предложены наборы параметров для Zemlyanika.KEM, и посчитана соответствующая им практическая стойкость МИК.
8. Разработана программная реализация Zemlyanika.KEM на языке `C`. Проведённое экспериментальное сравнение показало преимущество разработанного МИК над Kyber и Saber по ряду эксплуатационных характеристик.
9. Установлено, что Zemlyanika.KEM может быть интегрирован в протоколы TLS 1.3 и IKEv2 без изменения структур их сообщений и расширений.

Таким образом, все поставленные в работе задачи решены, а цель достигнута. Внедрение результатов настоящей работы в сетевые протоколы установления защищенного соединения будет способствовать повышению информационной безопасности компьютерных сетей при условии действия злоумышленника с доступом к квантовому компьютеру.

ПУБЛИКАЦИИ АВТОРА ПО ТЕМЕ ДИССЕРТАЦИИ

1. Zelenetsky A. S., Klyucharev P. G. Zemlyanika – Module-LWE based KEM with the power-of-two modulus, explicit rejection and revisited decapsulation failures // Journal of Computer Virology and Hacking Techniques. 2025. Vol. 21. DOI: 10.1007/s11416-025-00576-y. (1.5 п.л./1.4 п.л.)
2. Zelenetsky A. S., Klyucharev P. G. Modular arithmetic optimization in Kyber KEM // Journal of Computer Virology and Hacking Techniques. 2024. Vol. 20, no. 4. P. 857–865. DOI: 10.1007/s11416-024-00537-x. (0.6 п.л./0.55 п.л.)
3. Kiktenko E. O., Zelenetsky A. S., Fedorov A. K. Practical quantum multiparty signatures using quantum-key-distribution networks // Physical Review A. 2022. Vol. 105, issue 1. DOI: 10.1103/PhysRevA.105.012408. (1.2 п.л./0.5 п.л.)
4. Зеленецкий А. С., Ключарев П. Г. Алгоритм поиска аффинных аннигиляторов булевой функции // Математика и математическое моделирование. 2021. № 1. С. 13—26. (1 п.л./0.9 п.л.)
5. Зеленецкий А. С., Ключарев П. Г. Булевы функции, имеющие аффинные аннигиляторы // Математика и математическое моделирование. 2020. № 6. С. 1—12. (0.9 п.л./0.8 п.л.)
6. Зеленецкий А. С., Ключарев П. Г. Оптимизация модульной арифметики в механизме инкапсуляции ключа Kyber // ПДМ. Приложение. 2024. № 17. С. 162—166. (0.3 п.л./0.25 п.л.)
7. Зеленецкий А. С. Механизмы инкапсуляции ключа: причины внедрения, особенности и области применения // Безопасные информационные технологии: Сборник трудов Тринадцатой международной научно-технической конференции. Москва : МГТУ им. Н.Э.Баумана, 2024. С. 118—121. (0.25 п.л.)
8. Зеленецкий А. С., Ключарев П. Г. Постквантовые механизмы инкапсуляции ключа на решетках // Безопасные информационные технологии: Сборник трудов Двенадцатой международной научно-технической конференции. Москва : МГТУ им. Н.Э.Баумана, 2023. С. 67—71. (0.3 п.л./0.25 п.л.)
9. Зеленецкий А. С. Исследование булевых функций с аффинными аннигиляторами // Безопасные информационные технологии: Сборник трудов Одиннадцатой международной научно-технической конференции. Москва : МГТУ им. Н.Э.Баумана, 2021. С. 120—123. (0.25 п.л.)
10. Зеленецкий А. С. Изучение булевых функций, имеющих аффинные аннигиляторы // Безопасные информационные технологии: Сборник трудов Десятой международной научно-технической конференции. Москва : МГТУ им. Н.Э.Баумана, 2019. С. 146—149. (0.25 п.л.)