ГЛАВА 1
Постановка задачи на разработку постквантовых алгебраических алгоритмов ЭЦП с малыми размерами и высокой стойкостью

Квантовые компьютеры представляют серьезную угрозу для современных криптографических алгоритмов с открытым ключом. В частности, широко используемые схемы ЭЦП на базе RSA и эллиптических кривых уязвимы перед квантовым алгоритмом Шора, способным эффективно решать задачи факторизации и дискретного логарифмирования (Hidden Discrete Logarithm Problem, HDLP). Появление релевантного или практически значимого квантового компьютера приведет к взлому таких подписей за полиномиальное время, что поставит под угрозу целостность и конфиденциальность защищаемых цифровых документов [1]–[10], [18]–[23], [25], [30]–[34], [36]–[39], [41]–[44], [47]–[49], [52]–[56], [89]–[92], [94]–[97]. В связи с этим активное развитие получили постквантовые криптографические алгоритмы электронной подписи, устойчивые к квантовым атакам злоумышленников с применением квантового компьютера. Здесь особое внимание уделяется постквантовым схемам ЭЦП, безопасность которых основана на решении вычислительно сложных задач для квантовых компьютеров и классических суперЭВМ фон Неймана с высокой и сверхвысокой производительностью.

В 2016 году Национальный институт стандартов и технологий США инициировал программу стандартизации постквантовой криптографии [166], [168] и в 2024-м утвердил первые стандарты постквантовых алгоритмов цифровой подписи и инкапсуляции ключей. Были стандартизованы первые три схемы постквантовой ЭЦП: FIPS 204 (на основе алгоритма CRYSTALS-Dilithium), FIPS 205 (на основе SPHINCS+) и FIPS 206 (на основе FALCON) [98], [165]. Также были стандартизованы хеш-ориентированные схемы ЭЦП с сохранением состояния (XMSS и LMS) и многоуровневая многомерная квадратическая схема Rainbow [112].

В настоящее время за рубежом широкое распространение получают следующие схемы постквантовых ЭЦП.

- *Решеточные схемы постквантовой электронной подписи.* Их безопасность основана на задачах теории решеток, в том числе на сложности проблемы обучения с ошибками (LWE) или нахождении короткого вектора в решетке. Таковы, например, схемы CRYSTALS-Dilithium и FALCON [98], [165]. Они характеризуются высокой производительностью и относительно компактными ключами по сравнению с другими PQ-системами, однако длина подписи может быть значительной.
- *Хеш-основанные схемы постквантовой электронной подписи.* Различают схемы с сохранением состояния (stateful) и схемы без сохранения состояния (stateless). Первые (например, XMSS и LMS) используют дерево Меркла для обеспечения возможности многократной подписи и требуют ведения состояния (счетчика использованных ключевых пар) [134]. Вторые, например SPHINCS+, устраняют необходимость отслеживать состояние ценой увеличения размера подписи. Хеш-алгоритмы считаются криптографически консервативными в том смысле, что их надежность сводится к стойкости используемого хеша, однако генерируемые подписи весьма объемны [125], а скорость подписи и проверки сравнительно низкая.
- *Многомерные квадратические схемы постквантовой электронной подписи.* Их безопасность базируется на сложности решения систем многочленов над конечными полями (задача Multivariate Quadratic, MQ). Здесь большее распространение получила схема Rainbow, предлагавшая короткие подписи и высокую скорость их формирования и использования. Однако схема Rainbow была успешно взломана в 2022 году, что существенно замедлило ее развитие и распространение на практике [107].
- *Схемы постквантовой электронной подписи на основе корректирующих кодов.* Это, например, схема Wave или схема Picnic/SDitH. Однако они характеризуются значительными размерами подписи и высокой вычислительной трудоемкостью. В результате они рассматриваются для довольно узких сценариев применения на практике.

В главе 1 представлены результаты сравнительного анализа известных постквантовых алгоритмов ЭЦП, показаны ограничения существующих схем ЭЦП и обоснована необходимость разработки нового подхода. Обоснована разработка метода построения новой постквантовой ЭЦП на основе некоммутативных ассоциативных алгебр с повышенным уровнем информационной безопасности.

1.1. Оценка достаточности международных постквантовых алгоритмов ЭЦП

1.1.1. Постквантовый алгоритм CRYSTALS-Dilithium (FIPS 204 — ML-DSA)

CRYSTALS-Dilithium — это решеточная схема электронной подписи, основанная на задаче модульного обучения с ошибками (Module-LWE). Алгоритм был отобран NIST в качестве основного стандарта постквантовой подписи, он опубликован как федеральный стандарт FIPS 204 под названием *Module-Lattice-Based Digital Signature Algorithm* (ML-DSA) [165]. Dilithium унаследовал достоинства решеточных схем, а именно высокую скорость операций и относительно небольшие требования к памяти. Генерация ключей, подпись и проверка могут быть эффективно реализованы с использованием векторно-матричных операций, хорошо оптимизируемых на современных процессорах. Например, на профилях ML-DSA-44/65/87, соответствующих категориям NIST 2/3/5, для ориентира при ML-DSA-44 публичный ключ ≈ 1,3 Кбайт и подпись ≈ 2,4 Кбайт. Это значительно больше, чем у традиционных ECDSA, но приемлемо для многих приложений. Ключевым преимуществом Dilithium является баланс безопасности и производительности, алгоритм признан вполне пригодным для широкого применения — он относительно прост в реализации и не требует нестандартных операций, таких как арифметика чисел с плавающей запятой [124]. Кроме того, при правильной реализации схема устойчива к известным криптоаналитическим атакам на решетки и атакам по побочным каналам [119].

В то же время Dilithium присущ ряд ограничений. Во-первых, подписи и ключи довольно большие по сравнению с классическими алгоритмами ЭЦП. Во-вторых, безопасность Dilithium опирается на решение вычислительно сложной задачи, которая хотя и считается трудноразрешимой, но не так уж хорошо изучена.

1.1.2. Постквантовый алгоритм FALCON (FIPS 206 — FN-DSA)

FALCON — еще одна решеточная схема, основанная на другой задаче из теории решеток, а именно на сложности нахождения короткого решеточного вектора (задача семейства NTRU). Алгоритм FALCON обеспечивает более компактные подписи и ключи, чем Dilithium: так, для сравнимого

уровня безопасности публичный ключ составляет порядка 0,9 Кбайт, а подпись — приблизительно 0,66 Кбайт [126]. Такая эффективность достигнута благодаря использованию теоретико-числовых преобразований и усовершенствованных алгоритмов дискретной выборки из целочисленных распределений шума. FALCON был финалистом конкурса NIST и планируется к стандартизации как FIPS 206 под именем *FFT NTRU-based DSA* (FN-DSA) [98]. Преимущество FALCON — минимальный размер подписи среди всех основных PQC-схем, что делает его привлекательным для применения в системах с жесткими ограничениями на пропускную способность или объем хранимых данных.

Однако у FALCON имеются серьезные инженерные сложности. Алгоритм требует реализации точной выборки из многомерного гауссова распределения на решетке, для чего используется плавающая арифметика. Быстрая реализация FALCON опирается на аппаратные операции с плавающей запятой, которые трудно обеспечить при реализации с постоянным временем исполнения. Как отмечают специалисты, быстрая версия FALCON уязвима для атак по временным побочным каналам, а безопасная реализация с эмуляцией вычислений примерно в 20 раз медленнее [111]. На текущий момент заявленных показателей производительности FALCON сложно достичь на практике без потери безопасности. Это ограничивает применение алгоритма в сценариях, требующих высокой скорости этапа формирования подписи. Еще одной особенностью является более сложная структура секретного ключа и процесса генерации ключа, что увеличивает риск ошибок при реализации. В совокупности, несмотря на математическую элегантность и компактность, FALCON считается менее подходящим для массового внедрения, чем Dilithium, из-за трудности безопасной реализации [111].

1.1.3. Постквантовый алгоритм SPHINCS+ (FIPS 205 — SLH-DSA)

SPHINCS+ является представителем семейства хеш-подписей без сохранения состояния. Это значит, что для каждой подписи не требуется хранить или обновлять состояние (счетчик использования ключа), в отличие от XMSS/LMS. SPHINCS+ основывается исключительно на безопасности криптографических хеш-функций, то есть его стойкость обусловлена стойкостью используемого хеша (SHA-256, SHAKE256 и т. д.) и не зависит от нестандартных математических предположений.

Данная схема была также отобрана NIST и стандартизована как FIPS 205 под названием *Stateless Hash-Based DSA* (SLH-DSA) [106]. Главным достоинством SPHINCS+ является высокая степень обоснованности стойкости. На сегодняшний день криптоаналитически хеш-функции изучены лучше, чем математические основы решеточных и других современных постквантовых схем, поэтому степень апробации и криптоаналитической изученности SPHINCS+ довольно высока. Отмечается, что даже на минимальном рекомендованном уровне безопасности SPHINCS+ обеспечивает большую криптостойкость, чем многие другие схемы при максимальных параметрах.

Однако, несмотря на значительную криптостойкость, алгоритм обладает довольно низкой эффективностью. Он характеризуется крайне большими размерами подписи и существенной временной задержкой. В зависимости от выбора параметров подпись SPHINCS+ может составлять приблизительно 8...17 Кбайт для уровня 128 битов безопасности [125], а при повышенных требованиях безопасности размер возрастает вплоть до десятков килобайтов [125]. Верификация и особенно генерация подписи требуют выполнения множества хеш-вычислений, что делает алгоритм на порядки медленнее решеточных аналогов. Например, добавление SPHINCS+-сертификата к TLS-соединению увеличивает объем передаваемых данных почти на 40 Кбайт и вносит значительный дополнительный расход времени. Такие характеристики фактически исключают применение SPHINCS+ в устройствах с ограниченными ресурсами и делают затруднительным масштабирование под нагрузкой. В целом же SPHINCS+ целесообразно использовать как резервную схему на случай, если в будущем будут скомпрометированы более эффективные решения [106].

1.1.4. Постквантовые алгоритмы XMSS и LMS

XMSS (Extended Merkle Signature Scheme) и LMS (Leighton-Micali Signatures) — два схожих алгоритма электронной подписи, основанных на древовидных хеш-структурах с однократными подписями. Они относятся к *хеш-основанным схемам ЭЦП с сохранением состояния*, то есть каждая ключевая пара может выработать ограниченное число подписей, и для безопасности необходимо отслеживать состояние — уже использованный порядковый номер подписи. И XMSS, и LMS были стандартизованы раньше других PQC-схем: их спецификации опубликованы в IETF (RFC 8391

для XMSS, RFC 8554 для LMS) и одобрены NIST в специальной публикации SP 800-208 [112]. Фактически XMSS и LMS стали первыми в мире стандартизованными постквантовыми подписями [148]. Эти алгоритмы основываются на комбинировании однократных подписей (например, схемы Винтерница или Лампорта — Диффи) с деревьями Меркла для расширения до многократных подписей. Безопасность XMSS/LMS сводится к стойкости используемой хеш-функции, что делает их криптографически простыми, а их криптостойкость — предсказуемой. Кроме того, они позволяют достичь относительно небольшого размера подписи, так за счет многоуровневых деревьев Меркла можно подписывать очень большое количество сообщений, сохраняя длину одной подписи порядка нескольких килобайтов или меньше. Например, возможна конфигурация LMS с четырехуровневым деревом и высотой поддерева 20, дающая подписи приблизительно 1,1 Кбайт [167].

Тем не менее широко применять XMSS и LMS мешают существенные недостатки, прежде всего необходимость вести состояние приватного ключа. Если один и тот же одноразовый ключ будет использован дважды, криптостойкость схемы рушится — атакующий сможет восстановить закрытый ключ из двух разных подписей одного индекса. Потому реализация таких схем требует безошибочного учета каждой выданной подписи и применения надежных механизмов хранения и синхронизации счетчика. В некоторых приложениях наподобие распределенных систем, резервного копирования ключей и т. д. это сложно гарантировать. NIST прямо отмечает, что хеш-основанные схемы ЭЦП с сохранением состояния не подходят для общего использования из-за сложностей управления состоянием. Они годятся лишь для узкоспециализированных случаев, когда приватный ключ хранится и применяется строго централизованно и контролируемо (например, для прошивки устройств, обновляемой в режиме офлайн) [134]. Другой недостаток — ограниченное число подписей от одного ключа. Теоретически можно задать очень большое число, например 2^{60}, но оно конечно и по его исчерпании ключ должен быть заменен. Кроме того, если требуется значительно увеличить допустимое число подписей на один ключ, приходится увеличивать высоту дерева, что пропорционально увеличивает размер подписи в виде хеш-цепочки на пути дерева. Наконец, производительность формирования подписи тоже снижается при росте дерева, если нет возможности хранить большие промежуточные таблицы. XMSS и LMS хотя и являются криптографически надежными и дают относительно компактные подписи, но весьма неудобны и рискованны

в эксплуатации. Их можно рассматривать только как временное решение для противодействия квантовой угрозе, но не как долгосрочную замену универсальным цифровым подписям.

1.1.5. Постквантовый алгоритм Rainbow

Rainbow — многоуровневая схема на основе многочленов, долгое время считавшаяся перспективной постквантовой подписью. Идея Rainbow заключалась в использовании нескольких слоев уравнений квадратической системы для создания сложной скрытой структуры, позволяющей быстро подписывать и проверять сообщения. Алгоритм предлагал чрезвычайно компактные подписи и высокую скорость, что делало его привлекательным кандидатом для стандартизации в международных организациях (к примеру, рассматривался проект стандарта ISO/IEC 14888-4). Однако в 2022 году независимые исследователи обнаружили эффективный метод взлома Rainbow, им удалось решить систему уравнений для параметров предложенного стандарта за считаные дни на обычном компьютере [107]. Этот взлом фактически исключил Rainbow из числа претендентов на стандартизацию. Показательно, что атака стала возможна уже на стадии черновика стандарта, до его широкого внедрения, что подчеркнуло значение всесторонней криптоаналитической оценки. После провала Rainbow интерес к многомерным схемам несколько снизился, хотя в исследованиях продолжают рассматриваться иные варианты MQ-систем. Тем не менее на текущий момент не существует надежной стандартизованной мультиполиномиальной схемы ЭЦП. Опыт Rainbow указывает на возможную нестойкость этого класса задач или, по крайней мере, на необходимость значительно увеличивать параметры для восстановления безопасности, что нивелирует изначальные преимущества.

1.2. Достоинства и недостатки известных международных алгоритмов постквантовой ЭЦП

Ранее были описаны шесть основных постквантовых алгоритмов электронной подписи, дошедших до стадии стандартизации. Сравнивая их, можно сделать общий вывод: ни одна из постквантовых схем не обладает всеми качествами, присущими классическим ЭЦП (RSA/ECDSA). Так, одни алгоритмы дают приемлемую скорость, но требуют сильно увеличить

длину ключей и подписей (Dilithium), другие обеспечивают компактность подписи ценой усложнения реализации (Falcon), третьи просты в криптоанализе, но непрактичны из-за больших размеров (SPHINCS+), а хеш-основанные схемы ЭЦП с сохранением состояния и вовсе нельзя применять без строгого управления ключевой инфраструктурой. Исследователи отмечают, что ни одна из новых схем не сравнится по совокупности параметров с классическими эллиптическими подписями [164] — везде приходится жертвовать либо производительностью, либо удобством, либо доказанной криптостойкостью. В табл. 1.1 суммированы ключевые параметры рассмотренных алгоритмов для категории безопасности NIST 5 ($\approx 2^{256}$ в классической модели).

Таблица 1.1. Сравнение постквантовых алгоритмов ЭЦП для категории NIST 5

Алгоритм	Класс	Публичный ключ, байт	Подпись, байт	Примечание
ML-DSA-87 (FIPS 204; CRYSTALS-Dilithium-5)	Решетки	≈ 2592	≈ 4595	Простая реализация, без плавающей арифметики
FN-DSA-1024 (проект FIPS 206; FALCON-1024)	Решетки	≈ 1793	≈ 1280–1330	Очень компактная подпись, сложная корректная реализация
SLH-DSA-256 (FIPS 205; SPHINCS+-256 s/f)	Хеш-основанные (stateless)	64	≈ 35 000–50 000	Высокая криптоустойчивость, очень крупные подписи
XMSS (NIST SP 800-208, Cat 5)	Хеш-основанные (stateful)	≈ 32–64	≈ 2000–10 000	Требует учета состояния, размеры зависят от высоты дерева
LMS (NIST SP 800-208, Cat 5)	Хеш-основанные (stateful)	≈ 32–64	≈ 1000–4000	Требует учета состояния, возможны более компактные подписи при подходящих профилях

Здесь приведены ориентировочные оценки по открытым источникам [110], [175], однако реальные показатели могут зависеть от реализации. Из таблицы видно, что решеточные схемы (ML-DSA, FN-DSA) позволяют получить

более компактные подписи и ключи, чем хеш-основанные подходы (SLH-DSA, XMSS/LMS). При этом решеточные схемы (ML-DSA, FN-DSA) по сравнению с классическими алгоритмами ЭЦП (ECDSA/EdDSA) крупнее и сложнее в реализации.

1.3. Оценка достаточности отечественных постквантовых алгоритмов ЭЦП

В России разработкой постквантовых алгоритмов ЭЦП занимаются научные школы под руководством Технического комитета по стандартизации «Криптографическая защита информации» (ТК 26). Рассмотрим основные подходы к созданию постквантовых алгоритмов ЭЦП.

1.3.1. Постквантовый алгоритм «Шиповник»

«Шиповник» — отечественный алгоритм электронной подписи, устойчивый к атакам с использованием квантового компьютера [11]. Он разработан экспертами компании «Криптонит» совместно со специалистами из «QApp» в рамках рабочей группы «ТК 26» [93]. Схема «Шиповник» основана на протоколе идентификации Штерна (теоретико-кодовый протокол с нулевым разглашением), преобразованном в подпись методом Фиата — Шамира [122]. Стойкость редуцируется к задаче декодирования случайного линейного кода, которая является NP-полной (результат Берлекэмпа — Мак-Элиса — ван Тилборга, 1978) [105]. За счет этого для «Шиповника» известны лишь атаки экспоненциальной сложности, по данным авторов схемы, заявлены целевые уровни безопасности в классической модели порядка 2^{256} операций, в квантовой модели — порядка 2^{170} [181], что недостижимо на современных и перспективных компьютерах. Алгоритм реализован на языке C и открыт в репозитории GitHub, оптимизации позволили достичь времени генерации ключевой пары около 3 мс, подписи сообщения — приблизительно 0,85 с, проверки — приблизительно 11 мс на стандартном CPU [174]. В целом же «Шиповник» предлагает высокую криптостойкость при довольно компактных ключах и приемлемой производительности, хотя скорость формирования подписи заметно ниже, чем у многих зарубежных аналогов.

1.3.2. Постквантовый алгоритм «Крыжовник»

«Крыжовник» — это схема постквантовой цифровой подписи на основе алгебраических решеток. Конструктивно она является адаптированной вариацией алгоритма CRYSTALS-Dilithium. Схема построена по парадигме Фиата — Шамира, а безопасность опирается на предположительную трудность задач на модульных решетках (Module-SIS, в смежных постановках Module-LWE) [26]. Для разных уровней безопасности предложены варианты параметров «Крыжовничек», «Крыжовник», «Крыжовнище», различающиеся размерами ключей и подписей и скоростью работы [29], [27]. По данным прототипов, размеры сопоставимы с Dilithium, при этом этап формирования подписи требует больших вычислительных затрат из-за особенностей реализации [28]. Исходный код «Крыжовника» также выложен в открытый доступ на GitHub [142]. «Крыжовник» перенимает идеологию и преимущества решеточных схем, но, как и Dilithium, требует существенных вычислений при подписи. Его преимуществом перед «Шиповником» является более высокая скорость формирования подписи, однако размер публичного ключа у решеточных схем несколько больше, а доказуемая NP-полнота основной задачи в применяемых параметризациях до сих пор не гарантирована [168].

1.3.3. Другие постквантовые алгоритмы электронной подписи

Помимо «Шиповника» и «Крыжовника», в России известны и другие постквантовые схемы ЭЦП. Например, «Гиперикум» — схема электронной подписи без сохранения состояния на основе хеш-функций, конструктивно следующая подходу семейства SPHINCS+ с использованием отечественного стандарта хеширования «Стрибог» (ГОСТ Р 34.11-2012) в качестве базового примитива [178]. Криптографическая стойкость «Гиперикума» сводится к стойкости применяемой хеш-функции и не опирается на числовые и алгебраические предположения о сложности. Типичные размеры ключей составляют порядка 64 байт для открытого и 128 байт — для секретного ключа, размер подписи зависит от выбранного профиля и для уровня безопасности, сопоставимого с категорией 5 по классификации NIST PQC ($\approx 2^{256}$ в классической модели), находится примерно в диапазоне 17–50 Кбайт, а при меньших уровнях — ниже. Такая конструкция рассматривается как консервативный резервный вариант, конструктивно близкий к международному SPHINCS+.

Отметим, что, несмотря на доступность открытых спецификаций и экспериментальных реализаций, перечисленные отечественные постквантовые алгоритмы ЭЦП остаются предметом исследований и обсуждений, так как официально утвержденных государственных стандартов по этим схемам еще нет и сроки стандартизации не определены.

1.4. Предпосылки создания нового метода построения постквантовых ЭЦП на основе КНАА с двумя скрытыми группами

Несмотря на появление новых стандартов постквантовых ЭЦП, их ограничения и недостатки остаются существенными [57], [58], [60], [63], [65], [67], [69], [72], [74], [85], [169], [170], [177]. Дополнительную неопределенность создают ограниченная история криптоаналитических исследований используемых математических задач и прецеденты успешных атак в смежных классах. Отечественные же разработки находятся на стадии сертификации. Следовательно, ни одно из существующих направлений на сегодняшний день не дает универсального и апробированного решения без серьезных компромиссов по размеру, скорости, простоте внедрения и доказательной надежности.

Это мотивирует на поиск альтернативных путей разрешения задачи построения постквантового алгоритма ЭЦП с повышенным уровнем безопасности. Помимо задач, на решетках активно изучаются проблемы декодирования случайных линейных кодов и ранговых кодов, многомерные квадратические системы, изогенные конструкции, задачи изоморфизма многочленов и тензорных разложений, а также подходы на некоммутативных группах и полугруппах.

Здесь особый интерес представляют конструкции на некоммутативных ассоциативных алгебрах. Многие квантовые алгоритмы эффективно решают задачи в коммутативных структурах, но это не распространяется напрямую на некоммутативные структуры, в частности некоммутативные кольца, групповые и матричные алгебры. Далее приведен обзор исследований по использованию конечных некоммутативных ассоциативных алгебр и родственных структур в постквантовых криптоалгоритмах.