Физико-математические науки

ПОСТКВАНТОВАЯ КРИПТОГРАФИЯ

Балакина О. А.

ФГБОУ ВО «Поволжский государственный университет телекоммуникаций и информатики», e-mail: olesya_balakina@inbox.ru

Научный руководитель: Глущенко А. Г.

Введение

Развитие квантовых вычислений является одним из самых значимых технологических прорывов XXI века. Квантовые компьютеры, основанные на принципах суперпозиции и запутанности, обладают потенциалом решать задачи, недостижимые для классических вычислительных систем. Однако вместе с перспективами, которые открывает квантовая эпоха, человечество сталкивается с новыми угрозами для безопасности информации [2]. Современная криптография, лежащая в основе всех цифровых коммуникаций – от банковских операций до защиты государственных секретов, – строится на предположении о вычислительной сложности определенных математических задач. Если эти задачи могут быть решены эффективно на квантовом компьютере, то привычные алгоритмы шифрования перестают быть надежными.

Именно в этом контексте возникает понятие постквантовой криптографии – области, которая разрабатывает криптографические методы, устойчивые к атакам с использованием квантовых алгоритмов. Постквантовая криптография не отрицает достижения классической криптографии, а, напротив, расширяет их, адаптируя к новой вычислительной парадигме. Это направление стремится обеспечить долгосрочную безопасность цифровых систем в мире, где квантовые компьютеры становятся практической реальностью.

Цель данной статьи – рассмотреть теоретические и прикладные аспекты постквантовой криптографии, описать угрозы, исходящие от квантовых алгоритмов, проанализировать классы криптосистем, которые могут противостоять таким угрозам, и обозначить перспективы развития данного направления в ближайшие десятилетия.

Квантовые вычисления и угроза современной криптографии

Современные криптографические системы опираются на математические задачи, которые чрезвычайно трудны для решения на классических компьютерах. Так, безопасность широко используемых систем с открытым ключом – RSA, Диффи – Хеллмана и алгоритмов на эллиптических кривых – базируется на сложности факторизации больших целых чисел и вычисления дискретного логарифма. Эти задачи считаются практически нерешаемыми, если речь идет о числах длиной в сотни или тысячи бит.

Квантовые компьютеры радикально меняют ситуацию. В 1994 году Питер Шор предложил квантовый алгоритм, способный эффективно решать задачи факторизации и дискретного логарифмирования. Алгоритм Шора демонстрирует экспоненциальное ускорение по сравнению с классическими методами: время его работы растет полиномиально от числа бит в числе, тогда как классические алгоритмы требуют экспоненциальных затрат. Практическое следствие этого заключается в том, что квантовый компьютер с достаточным числом кубитов сможет за считанные минуты взломать RSA-шифр, на взлом которого классическому суперкомпьютеру понадобились бы миллионы лет.

Для понимания масштабов угрозы рассмотрим пример. Современные стандарты безопасности предполагают использование ключей RSA длиной 2048 бит. В классической модели вычислений это обеспечивает безопасность на уровне, превышающем возможности всех известных суперкомпьютеров. Однако квантовый компьютер, реализующий алгоритм Шора, сможет факторизовать такое число за полиномиальное время, что делает подобные системы бессмысленными в постквантовую эпоху [3]. Аналогичные уязвимости имеют алгоритмы Диффи – Хеллмана и его версия на эллиптических кривых (ECDH), широко применяемые для установления защищенных интернет-соединений (например, в протоколах TLS).

Таким образом, появление масштабируемых квантовых вычислительных систем потенциально разрушает основы современной криптографической инфраструктуры, которая обеспечивает конфиденциальность и аутентификацию в Интернете, мобильных сетях и банковских системах.

Квантовые алгоритмы, влияющие на криптографию

Основными источниками угрозы для криптографии являются два квантовых алгоритма – алгоритм Шора и алгоритм Гровера.

Алгоритм Шора

Как уже отмечалось, алгоритм Шора эффективно решает две ключевые задачи: факторизацию целых чисел и вычисление дискретного логарифма. Его применение делает незащищенными системы, основанные на этих задачах, включая RSA, Diffie–Hellman, ElGamal, а также все схемы на эллиптических кривых (ECC). Это означает, что любые данные, зашифрованные с помощью этих алгоритмов, могут быть расшифрованы, если злоумышленник обладает квантовым компьютером достаточной мощности. Более того, угроза носит ретроспективный

характер: данные, перехваченные сегодня, могут быть дешифрованы в будущем, когда квантовые технологии станут зрелыми. Поэтому переход на постквантовые стандарты – вопрос не только текущей, но и долговременной безопасности.

Алгоритм Гровера

В отличие от алгоритма Шора, алгоритм Гровера не нарушает полностью безопасность симметричных криптосистем, таких как AES или хэш-функций SHA. Однако он обеспечивает квадратичное ускорение при поиске ключа методом перебора: если для классического компьютера требуется порядка 2^n операций для перебора ключа длиной n бит, то для квантового компьютера – лишь $2^{n/2}$. Следовательно, уровень защиты симметричных систем фактически уменьшается вдвое. Например, AES-256 при атаке с использованием алгоритма Гровера обеспечивает ту же устойчивость, что и AES-128 при классической атаке. Это означает, что для сохранения эквивалентного уровня безопасности необходимо удвоить длину ключа [3].

Основы постквантовой криптографии

Постквантовая криптография – это область, разрабатывающая криптографические системы, устойчивые к атакам с использованием квантовых алгоритмов. Главное отличие ПКК от квантовой криптографии состоит в том, что постквантовые алгоритмы реализуются на классических вычислительных устройствах, не требуя квантовых каналов связи [1]. Они должны быть совместимы с существующей инфраструктурой, но при этом обеспечивать безопасность даже в условиях появления квантовых компьютеров.

Основная задача исследователей заключается в поиске новых математических проблем, для которых не существует эффективных квантовых алгоритмов. Эти задачи должны удовлетворять следующим критериям:

1. Трудность решения как на классическом, так и на квантовом компьютере;
2. Возможность практической реализации криптографических протоколов;
3. Эффективность по скорости и объему ключей;
4. Доказуемая безопасность на основе известных сложных задач.

На сегодняшний день выделяют несколько основных направлений постквантовой криптографии [1]:

1. Решеточная криптография

Одним из наиболее перспективных направлений является криптография на основе решеток. Она базируется на математических задачах, связанных с поиском кратчайшего вектора в решетке (SVP) и задачей наиближайшего вектора (CVP). Эти задачи остаются сложными как для классических, так и для квантовых компьютеров, что делает их надежной основой для криптосистем нового поколения.

Решеточные схемы обладают рядом преимуществ:

- доказуемая безопасность, основанная на NP-трудных задачах;
- высокая производительность;
- простота реализации на классических процессорах;
- возможность построения не только шифрования, но и цифровых подписей, а также функций хэширования и анонимных идентификаторов.

Классическим примером решеточных схем является криптосистема NTRU, предложенная в 1996 году. Она использует арифметику в кольцах многочленов и обеспечивает высокую скорость шифрования и дешифрования при малом размере ключей. Позже появились более универсальные конструкции – схемы, основанные на LWE (Learning with errors) и ее вариант Ring-LWE, которые легли в основу множества современных постквантовых алгоритмов, включая Kyber и Dilithium [4].

Решеточные схемы особенно привлекательны для стандартизации, поскольку они обладают сбалансированными характеристиками безопасности и эффективности. Именно поэтому в рамках инициативы NIST PQC (Национального института стандартов и технологий США) именно решеточные алгоритмы были выбраны в качестве основных кандидатов для стандартизации постквантовых протоколов.

2. Кодовая криптография

Другим исторически значимым направлением является криптография на основе теории кодирования. Ее основой служит задача декодирования случайных линейных кодов – математически трудная задача, не имеющая известных полиномиальных решений даже при использовании квантовых алгоритмов. Первой практической реализацией стала криптосистема МакЭлиса, предложенная в 1978 году. Она основана на использовании кодов Гоппы и позволяет реализовать стойкое шифрование.

Главным преимуществом кодовых криптосистем является высокая устойчивость к известным видам атак. Недостаток – большие размеры открытых и закрытых ключей (порядка сотен килобайт и более), что затрудняет применение в устройствах с ограниченными ресурсами. Тем не менее, для некоторых задач, таких как защита критически важных данных и квантово-устойчивая передача ключей, эти схемы остаются актуальными.

3. Мультивариантная криптография

Мультивариантные криптосистемы основаны на трудности решения систем многочленов над конечными полями. В общем виде задача заключается в нахождении набора переменных, удовлетворяющих множеству нелинейных уравнений. С математической точки зрения это NP-трудная задача, что делает ее привлекательной основой для построения криптографических схем.

Исторически первым известным примером является система MI (Matsumoto–Imai), предложенная в конце 1980-х годов. Позднее появились улучшенные схемы, такие как HFE (Hidden Field Equations) и ее модификации, включая Rainbow – одну из наиболее известных и исследованных мультивариантных схем цифровой подписи.

Преимуществом мультивариантной криптографии является высокая скорость выполнения операций, особенно на этапе верификации подписи. Однако существенным недостатком долгое время считались большие размеры открытых ключей (часто десятки и сотни килобайт), а также неоднократные компрометации некоторых предложенных схем вследствие алгебраических атак. Несмотря на это, направление остается активно развивающимся, и новые подходы к генерации уравнений позволяют повышать устойчивость систем без значительного увеличения вычислительной нагрузки.

Особый интерес представляют гибридные схемы, в которых мультивариантные подписи комбинируются с решеточными или кодовыми конструкциями. Такой подход позволяет достичь как высокой производительности, так и теоретической стойкости.

4. Криптография на основе изогений эллиптических кривых

Еще одним оригинальным направлением постквантовой криптографии является использование изогений эллиптических кривых. Изогения – это морфизмы между эллиптическими кривыми, сохраняющие их структуру. Безопасность таких систем основана на сложности нахождения изогении между двумя заданными кривыми, что представляет собой математическую задачу, для которой пока не найдено эффективного квантового алгоритма.

Наиболее известной схемой этого типа является SIDH (Supersingular Isogeny Diffie–Hellman), а ее оптимизированная версия – SIKE (Supersingular Isogeny Key Encapsulation) – долгое время считалась одним из самых перспективных кандидатов на стандартизацию. Изогенные криптосистемы привлекательны тем, что обеспечивают чрезвычайно компактные ключи (всего несколько сотен байт), что делает их особенно удобными для применения в мобильных устройствах и встроенных системах.

Однако в 2022 году стало известно, что схема SIKE подвержена атакам, основанным на анализе структуры используемых кривых и вычислении специальных подгрупп. Это показало, что изогенная криптография еще не достигла зрелости, необходимой для массового внедрения, но направление остается важным объектом фундаментальных исследований.

В долгосрочной перспективе изогенные методы могут стать основой для легких и энергоэффективных постквантовых протоколов, особенно если удастся создать универсальные решения с доказуемыми гарантиями безопасности.

5. Криптография на основе хэш-функций

Хэш-ориентированные криптографические схемы считаются одними из самых надежных и проверенных решений постквантового периода. Их безопасность опирается исключительно на свойства криптографических хэш-функций, а именно на устойчивость к коллизиям и предобразам. Поскольку хэширование является базовой операцией, к которой пока не найдено эффективных квантовых алгоритмов (кроме алгоритма Гровера, снижающего безопасность лишь вдвое), хэш-ориентированные схемы обладают высокой устойчивостью к квантовым атакам.

Наиболее известными представителями этого направления являются схемы цифровой подписи: Lamport, Merkle и их современные варианты – XMSS (eXtended Merkle Signature Scheme) и SPHINCS+.

- Lamport Signature – простейшая схема, использующая одноразовые ключи, но требующая большого количества данных;
- Merkle Signature – развивает идею одноразовых подписей, объединяя их в древовидную структуру, что позволяет многократное использование публичного ключа;
- XMSS и SPHINCS+ – современные стандартизированные схемы, обеспечивающие высокую степень защиты и практичность применения.

Главный недостаток хэш-подписей – значительные размеры ключей и относительно медленная генерация подписи. Тем не менее их устойчивость к квантовым атакам делает их незаменимыми в ситуациях, где необходима долговременная сохранность данных, например, при хранении государственных архивов, юридически значимых документов и медицинских записей.

Стандартизация постквантовой криптографии

Понимая надвигающуюся угрозу, международное сообщество активно работает над созданием единых стандартов постквантовой криптографии. Ключевым центром этих инициатив является Национальный институт стандартов и технологий США (NIST), который в 2016 году запустил многоэтапный проект по отбору и оценке постквантовых алгоритмов.

Цель программы NIST PQC – выбрать набор алгоритмов, которые смогут заменить современные схемы RSA и ECC в протоколах TLS, IPsec, SSH и других. Критериями отбора стали:

- математическая устойчивость к известным классическим и квантовым атакам;
- эффективность реализации на различных аппаратных и программных платформах;

• устойчивость к побочным каналам;

• гибкость параметров и совместимость с существующими протоколами.

После нескольких раундов анализа, включающих более 80 предложенных схем, в июле 2022 года NIST объявил первые алгоритмы, выбранные для стандартизации:

• CRYSTALS-Kyber – схема шифрования и обмена ключами, основанная на решеточных задачах LWE;

• CRYSTALS-Dilithium – схема цифровой подписи на основе решеточных конструкций;

• Falcon – более компактная решеточная схема подписи;

• SPHINCS+ – хэш-ориентированная подпись с долгосрочной безопасностью.

Эти алгоритмы демонстрируют оптимальное сочетание производительности и устойчивости, что позволяет постепенно интегрировать их в современные коммуникационные стандарты. В ближайшие годы ожидается появление финальных версий стандартов, после чего начнется глобальный процесс миграции инфраструктуры безопасности [4].

Гибридные подходы и переходный период

Переход от классических к постквантовым системам не может быть мгновенным. Большинство современных сетевых протоколов, включая HTTPS, VPN и почтовые сервисы, тесно связаны с инфраструктурой открытых ключей (PKI), основанной на RSA и ECC. Резкая замена алгоритмов может привести к несовместимости и сбоям в работе систем.

Для решения этой проблемы разработчики используют гибридные криптографические схемы, которые объединяют классические и постквантовые алгоритмы. Например, при установлении защищенного соединения может использоваться комбинация ECDH и Kyber: даже если одна из схем будет скомпрометирована, вторая обеспечит защиту.

Такой подход имеет следующие преимущества:

• плавный переход к новой криптографии без нарушения совместимости;

• возможность постепенного тестирования и оптимизации новых алгоритмов;

• дополнительная устойчивость к непредвиденным атакам на новые схемы.

Параллельно с техническими мерами важную роль играет образование специалистов и обновление нормативной базы. Переход к постквантовым стандартам требует перепроектирования систем сертификации, инфраструктуры ключей и аппаратных модулей безопасности. Все это представляет масштабную задачу для государственных структур, бизнеса и академического сообщества [2].

Практические применения и вызовы внедрения

Несмотря на активные исследования, внедрение постквантовой криптографии в практику сопряжено с рядом сложностей. Основные из них:

1. Размер ключей и сообщений. Некоторые схемы, особенно кодовые и мультивариантные, требуют больших объемов памяти, что затрудняет их использование в IoT-устройствах;

2. Скорость вычислений. Хотя решеточные схемы достаточно быстры, в некоторых случаях они уступают по эффективности классическим алгоритмам, что может замедлить работу серверов;

3. Совместимость протоколов. Новые алгоритмы необходимо адаптировать к существующим стандартам коммуникаций (TLS, SSH, IPsec и т. д.), что требует глубокой переработки инфраструктуры;

4. Безопасность на практике. Реальные реализации подвержены атакам через побочные каналы – измерение времени, потребления энергии и электромагнитных излучений.

Тем не менее ряд компаний уже начал интеграцию постквантовых решений. Google тестировал гибридные алгоритмы в протоколе TLS 1.3; Microsoft и Cloudflare проводят пилотные проекты с Kyber и Dilithium; а правительственные структуры США и ЕС разрабатывают национальные дорожные карты перехода.

Особое внимание уделяется критическим секторам – энергетике, телекоммуникациям и обороне, где долгосрочная сохранность секретных данных имеет первостепенное значение. Даже если квантовые компьютеры массово появятся лишь через 10–15 лет, данные, зашифрованные сегодня, должны оставаться защищенными в будущем.

Перспективы развития постквантовой криптографии

Постквантовая криптография находится на этапе активного становления. На горизонте ближайших десятилетий можно выделить несколько ключевых тенденций ее развития:

1. Интеграция в глобальные стандарты. После окончательной стандартизации NIST и ISO/IEC начнется широкое внедрение PQ-алгоритмов во все уровни сетевых протоколов;

2. Оптимизация и миниатюризация. Активно ведутся работы по сокращению размеров ключей и повышению скорости работы схем, что позволит применять их даже в микроконтроллерах;

3. Комбинированные архитектуры. Гибридные схемы, объединяющие разные математические подходы (решетки + хэши + изогении), будут играть ключевую роль в обеспечении надежности;

4. Развитие формальных доказательств безопасности. Все больше внимания уделяется

строгим математическим доказательствам, связывающим стойкость алгоритмов с фундаментальными задачами теории сложности;

5. Создание национальных стратегий киберустойчивости. Государства разрабатывают программы подготовки инфраструктуры к постквантовой эпохе, включая сертификацию оборудования и обучение специалистов.

Заключение

Постквантовая криптография – это ответ человечества на технологический вызов, который несут квантовые вычисления. В течение десятилетий классические криптографические методы считались незыблемыми, но появление алгоритмов Шора и Гровера продемонстрировало: безопасность, основанная только на вычислительной сложности, не является вечной.

Разработка и внедрение криптографических схем, устойчивых к квантовым атакам, – ключевая задача для государств, корпораций и исследовательских центров [2]. Решеточные, кодовые, хэш-ориентированные и мультивариантные системы представляют собой фундамент, на котором будет построена новая инфраструктура доверия. Уже сегодня стандарты NIST PQC формируют основу для перехода к безопасным коммуникациям в постквантовую эпоху.

Однако технологический прогресс требует не только новых алгоритмов, но и изменения мышления. Необходимо осознать, что защита данных – это процесс, а не состояние. Постквантовая криптография должна стать не разовой заменой старых стандартов, а частью динамичной, постоянно обновляемой системы глобальной безопасности.

В обозримом будущем квантовые компьютеры, вероятно, станут столь же повседневными, как современные серверы. И когда это произойдет, устойчивость цифрового мира будет зависеть от того, насколько успешно сегодня человечество создаст фундамент постквантовой безопасности – надежный, прозрачный и совместимый с принципами открытого интернета.

Список литературы

1. URL: https://ru.wikipedia.org/wiki/Постквантовая_криптография [Электронный ресурс]. (дата обращения: 15.12.2025).

2. Маршев И. С. Постквантовая Криптография // Материалы XVII Международной студенческой научной конференции «Студенческий научный форум – 2025» [Электронный ресурс]. URL: https://files.scienceforum.ru/pdf/2025/6746d1ffaed12.pdf (дата обращения: 15.12.2025).

3. Букашкин С. А., Черепнев М. А. Квантовый компьютер и постквантовая криптография // Программная инженерия. 2021. №4. С. 171-178. [Электронный ресурс]. URL: http://novtex.ru/prin/rus/10.17587/prin.12.171-178.html (дата обращения: 15.12.2025).

4. Федоров С. К. Анализ постквантовых криптографических алгоритмов // Аллея Науки. 2021. №6 (57). [Электронный ресурс]. URL: https://alley-science.ru/domains_data/files/1June2021/ANALIZ%20POSTKVANTOVYH%20KRIPTOGRAFIChESKIH%20ALGORITMOV.pdf (дата обращения: 15.12.2025).