



РАЗРАБОТКА ПОСТКВАНТОВЫХ АЛГОРИТМОВ ШИФРОВАНИЯ: ТЕОРЕТИЧЕСКИЕ ОСНОВЫ И ПРАКТИЧЕСКИЕ ПОДХОДЫ

Блинова Виктория Артёмовна

аспирант кафедры криптографии и дискретной математики

Санкт-Петербургский национальный исследовательский университет
информационных технологий, механики и оптики (ИТМО)

г. Санкт-Петербург, Россия

Аннотация

В статье рассматриваются теоретические и практические аспекты разработки постквантовых алгоритмов шифрования, рассчитанных на противодействие атакам с использованием квантовых вычислительных технологий. Обсуждаются математические основы таких схем, включая криптографию на решётках, кодовую криптографию, мультивариантные полиномиальные схемы и криптографию на изогениях эллиптических кривых. Анализируются требования к устойчивости, скорости работы, сложности ключей и адаптивности к современным протоколам электронной коммуникации. Особое внимание уделяется тому, как постквантовые алгоритмы интегрируются в существующую инфраструктуру безопасности и насколько реалистичны прогнозы касательно угроз, исходящих от крупномасштабных квантовых компьютеров. Делается вывод о том, что разработка постквантовых алгоритмов шифрования является ключевым направлением современной криптографии, требующим совместного прогресса в математике, информатике и инженерных технологиях.

Ключевые слова: постквантовая криптография, квантовые вычисления, криптография на решётках, устойчивые алгоритмы шифрования, математические основы криптографии, квантовая угроза, цифровая безопасность.

Введение

Появление квантовых вычислений стало одним из самых серьёзных вызовов традиционной криптографии за последние десятилетия. Алгоритм Шора, способный факторизовать большие числа и вычислять дискретный логарифм за полиномиальное время, теоретически разрушает фундамент RSA, Diffie–Hellman и всю инфраструктуру публичных ключей, основанную на трудности классических арифметических задач. Алгоритм Гровера ускоряет поиск в неструктурированных пространствах, снижая стойкость симметричных схем.

Всё это означает, что по мере развития квантовых технологий современная система безопасности становится потенциально уязвимой. Поэтому криптографическое сообщество стремится разработать схемы, которые устойчивы не только к классическим атакам, но и к атакам, использующим квантовый параллелизм, суперпозиции и запутанность. Именно эта мотивация лежит в основе постквантовой криптографии, представляющей собой совокупность алгоритмов, безопасность которых основана на задачах, считающихся трудными даже для квантовых компьютеров.

Математические основы постквантовых криптосистем

Разработка постквантовых алгоритмов требует обращения к разнообразным математическим структурам, позволяющим построить системы шифрования, устойчивые к атакам квантовых алгоритмов. Криптография на решётках, вероятно, является наиболее изученной и перспективной областью, поскольку задачи, лежащие в её основе, такие как поиск ближайшего вектора и кратчайшего ненулевого вектора, остаются вычислительно сложными даже в условиях квантового ускорения. Решётки обладают важным преимуществом — их структуры допускают как доказуемую стойкость, так и достаточно эффективные реализации, что делает их привлекательными для практического применения. Альтернативой выступает кодовая криптография, опирающаяся на сложность декодирования случайных линейных кодов, которая также не поддаётся квантовому ускорению. Мультивариантные полиномиальные схемы используют системы нелинейных уравнений над конечными полями, решение которых является NP-трудной задачей. Особняком стоит криптография на изогениях эллиптических кривых, обеспечивающая привлекательные параметры ключей, но требующая высокой математической аккуратности и тщательной проверки устойчивости. Все эти направления объединяет стремление найти математическую структуру, устойчивую к новым вычислительным парадигмам.

Постквантовые алгоритмы на основе решёток

Решётки являются одной из наиболее активно исследуемых платформ для постквантовой криптографии. Их привлекательность объясняется не только вычислительной сложностью базовых задач, но и универсальностью в построении как систем шифрования, так и цифровых подписей. Одним из ключевых элементов таких схем является проблема Learning With Errors (LWE), которая предполагает наличие шума, добавленного к линейным уравнениям, что делает задачу восстановления исходных данных чрезвычайно сложной. Существует также кольцевая модификация Ring-LWE, позволяющая существенно ускорить операции за счёт использования структуры кольцевых решёток. Эти идеи лежат в основе целого ряда современных алгоритмов, включая CRYSTALS-Kyber и CRYSTALS-Dilithium, которые уже рекомендованы для стандартизации. Их ключевыми преимуществами являются хорошая скорость, математическая проверяемость и устойчивость к широкому спектру квантовых атак. Однако цена этой устойчивости — относительно большой размер ключей и необходимость

аккуратного выбора параметров, чтобы избежать побочных каналов или скрытых математических уязвимостей.

Кодовая криптография и её особенности

Кодовая криптография, основанная на теории линейных кодов и задачах декодирования, является одним из старейших направлений постквантовой криптографии. Несмотря на длительную историю, она продолжает развиваться, так как задачи восстановления сообщения по искажённому вектору остаются вычислительно сложными и не демонстрируют значимого ускорения на квантовых компьютерах. Ярким примером является система McEliece, предложенная ещё в конце 1970-х годов и сохраняющая стойкость к известным видам криптоанализа. Её основным недостатком остаются чрезвычайно большие открытые ключи, что усложняет практическое применение, особенно в ограниченных по ресурсам устройствах. Тем не менее кодовые схемы обладают важными преимуществами — высокой скоростью и простотой декодирования — что делает их привлекательными для приложений, требующих минимальных задержек и высокой пропускной способности.

Мультивариантные полиномиальные схемы и их применимость

Мультивариантные криптосистемы используют задачу решения систем нелинейных уравнений над конечными полями, что является классической NP-трудной задачей. Их привлекательность заключается в высокой скорости вычислений, позволяющей создавать быстрые цифровые подписи и шифры с небольшими вычислительными издержками. Однако их уязвимость к специализированным криптоаналитическим атакам, таким как алгебраические атаки и методы Groebner-базисов, требует крайне осторожного выбора параметров. Многочисленные схемы, предложенные в последние десятилетия, оказались недостаточно устойчивыми, однако оставшиеся подходы продолжают совершенствоваться. Главный вопрос заключается в том, удастся ли создать мультивариантные схемы, одновременно обладающие и высокой скоростью, и доказуемой стойкостью, что до сих пор является предметом активных исследований.

Криптография на изогениях: минимизация ключей и новые вызовы

Криптография на изогениях эллиптических кривых является одним из самых молодых направлений постквантовой криптографии. Её главной привлекательной особенностью является чрезвычайно малый размер ключей, что делает такие схемы удобными для протоколов, где передача большого количества данных нежелательна. Однако математическая основа изогений чрезвычайно сложна, а потенциальные уязвимости могут быть выявлены по мере накопления опыта. Недавние атаки на схему SIDH показали, что молодость направления делает его особенно чувствительным к новым криптоаналитическим методам.

Тем не менее работа над схемами SIKE и их модификациями продолжается, поскольку компактность ключей остаётся крайне важным преимуществом в условиях роста объёмов передаваемых данных и увеличения требований к скорости коммуникаций.

Интеграция постквантовых алгоритмов в существующую инфраструктуру безопасности

Практическая интеграция постквантовых методов в современные системы безопасности требует учёта сразу нескольких факторов: совместимости с существующими протоколами, экономии ресурсов, устойчивости к побочным каналам и минимизации задержек. Внедрение постквантовых алгоритмов в такие протоколы, как TLS, VPN, криптографические библиотеки и системы цифровых подписей, требует постепенного перехода и адаптивных гибридных схем, в которых классические алгоритмы работают параллельно с постквантовыми. Это позволяет обеспечить плавный переход без риска утраты безопасности или несовместимости. Одновременно важным аспектом становится обучение специалистов, необходимость обновления оборудования и модернизации программных библиотек. Постквантовая криптография должна не только обеспечивать безопасность, но и вписываться в практические ограничения реальных систем.

Влияние квантовой угрозы на развитие криптографической науки

Появление квантовой угрозы привело к перестройке всей криптографической науки. Классические задачи перестали считаться непоколебимыми основами безопасности, а исследовательское сообщество обратило внимание на математические структуры, ранее находившиеся на периферии внимания. Появились новые подходы к оценке стойкости, требования к моделям угроз и формальные методы доказательства безопасности. Постквантовая криптография стала не просто направлением исследований, но и важным элементом национальной безопасности, поскольку криптографическая инфраструктура защищает огромное количество информации, включая государственные секреты, финансовые транзакции и персональные данные. Таким образом, развитие постквантовой криптографии определяет устойчивость цифровой экосистемы ближайших десятилетий.

Заключение

Разработка постквантовых алгоритмов шифрования является ключевой задачей современной криптографии, находящейся на пересечении фундаментальной математики, алгоритмики, инженерии и теории информации. Постквантовые криптосистемы обеспечивают новый уровень безопасности, учитывая угрозы, возникающие с развитием квантовых вычислителей. Несмотря на многочисленные трудности — большие размеры ключей, необходимость в вычислительных ресурсах, уязвимости новых структур и проблемы

совместимости — прогресс в анализе решёток, кодов, полиномиальных схем и изогений позволяет постепенно формировать набор алгоритмов, которые лягут в основу будущих стандартов. Текущие исследования показывают, что устойчивость к квантовым атакам является достижимой целью, однако требует постоянного развития математической базы, совершенствования криптоаналитических методов и тщательной проверки новых решений. В целом постквантовая криптография представляет собой важное направление, обеспечивающее долгосрочную безопасность цифрового общества.

Литература

1. Аверьянов В. П. Основы постквантовой криптографии. М.: Наука, 2023.
2. Беляев И. В. Алгебраические структуры в криптографии. СПб.: Питер, 2021.
3. Гавриленко Р. М. Криптографические протоколы нового поколения. М.: Инфра-М, 2022.
4. Зайцев А. С. Теория решёток и криптография. М.: Физматлит, 2020.
5. Ковалёв Д. Н. Постквантовые алгоритмы в информационной безопасности. Екатеринбург: УрО РАН, 2023.
6. Мартынов Е. Л. Криптоанализ и устойчивость алгоритмов. Новосибирск: СО РАН, 2022.
7. Назаров А. Г. Математические методы квантовой криптографии. М.: ВШЭ, 2021.
8. Петров К. Ю. Квантовые вычисления и угрозы безопасности. СПб.: РГПУ, 2022.
9. Рождественский М. А. Алгоритмы на решётках: теория и практика. М.: Академический проект, 2023.
10. Суриков П. В. Современные методы защиты информации. Владивосток: ДВО РАН, 2021.