АНАЛИЗ ПОДХОДОВ К ПОСТРОЕНИЮ КРИПТОГРАФИЧЕСКИХ СХЕМ, УСТОЙЧИВЫХ К КВАНТОВЫМ АТАКАМ

Крупенич Е. Г., Лукьянов А. А.
Кафедра программного обеспечения информационных технологий, Факультет компьютерных систем и сетей,
Центр информатизации и инновационных разработок,
Белорусский государственный университет информатики и радиоэлектороники
Минск, Республика Беларусь
E-mail: {e.krupenich, a.lukianov}@bsuir.by

Статья даёт обзор современных подходов к построению постквантовых криптографических схем: решётчатых, кодовых, многочленных, хеш-основанных конструкций и изогений. Рассмотрены основные математические предпосылки, оценены устойчивость к классическим и квантовым атакам, сопоставлены производительность и практические ограничения. Приведены рекомендации по применимости в различных классах систем и указаны ключевые источники для углублённого изучения.

Введение

Появление масштабируемых квантовых вычислений ставит под сомнение безопасность классических асимметричных схем на основе факторизации и дискретного логарифма. В ответ разработаны несколько семей постквантовых примитивов, различающихся по математической предпосылке, эффективности и области применения. Цель статьи – систематизировать эти подходы, сопоставить их по ключевым критериям (стойкость, размеры, производительность, масштабируемость) и сформулировать практические рекомендации для поэтапной миграции протоколов и систем.

I. Обзор моделей

Решётчатые (Lattice-based). Опираются на SVP/CVP и LWE/Ring-LWE; дают широкий набор примитивов: KEM, подписи, шифрование, гомоморфия. Сильная теоретическая база и гибкость параметризации; основные ограничения – чувствительность к выбору параметров и увеличенные размеры ключей/шифротекстов в ряде реализаций.

Кодовые криптосхемы(Code-based). Основаны на сложности декодирования линейных кодов (классика – McEliece). Отличаются высокой скоростью шифрования/дешифрования и устойчивой практикой, но страдают очень большими открытыми ключами и менее гибкой параметризацией.

Многочленные и структурированные алгебраические конструкции (Ring/Module-LWE, NTRU-класс). Используют кольцевую структуру для уменьшения размеров и ускорения арифметики; позволяют компактные реализации для встроенных устройств. Риск – появление структурных слабостей при небрежной параметризации.

Хеш-основанные подписи. Lamport, Merkle, XMSS, LMS, SPHINCS+ полагаются на стойкость хеш-функций; дают простую и формально выверяемую модель безопасности. Минусы – управление состоянием (stateful решения) или увеличенная длина подписей (stateless схемы).

Isogeny-schemes. Схемы на основе изогений эллиптических кривых над сложными полями (пример SIKE) обеспечивают крайне компактные ключи, но операции относительно медленны, доказательная база и практическая зрелость ограничены; подходят в сценариях с критическим ограничением размера ключа.

II. Сравнение моделей

Для практического сравнения постквантовых схем использованы следующие критерии: (i) математические предпосылки и наличие доказательной базы; (ii) размеры ключей и подписи; (iii) производительность и затраты ресурсов; (iv) масштабируемость и архитектурные ограничения. Эти критерии позволяют соотнести безопасность с ресурсными требованиями и выбрать подходящие классы схем для конкретных приложений. Сводная оценка по указанным критериям приведена в Таблице 1.

III. Применимость в реальных системах

- Сетевые протоколы (TLS, VPN): предпочтение – решётчатые KEM и NTRU-подобные; внедрять гибридно для совместимости.
- Встроенные/IoT-устройства: приоритет – кольцевые/многочленные реализации (Module-LWE, NTRU) с оптимизацией памяти и CPU.
- Долговременная архивация и юридические подписи: предпочтение – хеш-основанные схемы; обеспечить процедуру управления состоянием.
- Серверная инфраструктура и HSM: кодовые схемы и оптимизированные решётчатые реализации; предусмотреть хранение и распределение крупных ключей.
- Миграция и эксплуатация: поэтапная интеграция, гибридные ключи, тестирование реализаций и мониторинг стандартов (NIST и др.).

IV. Вывод

Сравнительный анализ показывает, что универсального «лучшего» подхода не существует. Выбор зависит от требований: если важна гибкость и широкий набор примитивов – решётчатые схемы; при необходимости очень быстрых операций шифрования – кодовые; для долгосрочной гарантийной подписи – хеш-основанные; для компактных ключей при допускаемой медлительности – isogeny-методы. При практической миграции важно проводить системную оценку: анализ угроз, оценку ресурсов, тестирование реализации и план постепенного развёртывания. На переходном этапе стоит использовать гибридные схемы (классические + постквантовые) и опираться на параметры, рекомендованные профильными стандартами и профессиональными сообществами.

V. Список литературы

1. Москвин, В. С., Богатырёв, В. А. Постквантовые алгоритмы электронной цифровой подписи и их применение в распределённом реестре / В. С. Москвин, В. А. Богатырёв // H&ES Research. – 2022. – Vol. 14, № 4. – P. 47–53.
2. Лежинский, М. В., Мокряков, А. В. Алгоритмы шифрования, устойчивые к взлому в условиях квантового превосходства / М. В. Лежинский, А. В. Мокряков // Сборник научных трудов кафедры прикладной математики и программирования по результатам работы постоянного семинара «Теория систем». – 2021. – С. 141–147.
3. Шемякина, М. А. Анализ применения квантовых технологий в криптографии / М. А. Шемякина // International Journal of the Humanities and Natural Sciences. – 2019. – № 5-4. – С. 59–62.
4. National Institute of Standards and Technology. Status Report on the First Round of the NIST Post-Quantum Cryptography Standardization Process / Alagic J. et al. // NISTIR – 8240. – Gaithersburg, MD: NIST, 2019. – 27 pp.
5. Bos, J., Ducas, L., Kiltz, E., Lepoint, T., Lyubashevsky, V., Presern, T., Schwabe, P., Seiler, G., Stehlé, D. CRYSTALS-Kyber: a CCA-secure module-LWE based KEM / J. Bos et al. // Proc. PQCrypto 2020. – 2020. – P. 1–23.
6. Ducas, L., Kiltz, E., Lepoint, T., Lyubashevsky, V., Neves, S., Seiler, G., Stehlé, D. CRYSTALS-Dilithium: a lattice-based digital signature scheme / L. Ducas, E. Kiltz, T. Lepoint etal.// Proc. Eurocrypt/PQCrypto 2020 – 2020. – P. 24–45.
7. Bernstein, D. J., Hülsing, A., Käsper, E., Lange, T., Schwabe, P. SPHINCS+: stateless hash-based signatures / D.J.Bernstein, A. Hülsing, E. Käsper etal.// Proc. PQCrypto 2020 / IACR ePrint Archive – 2020. – P. 1–31.

Таблица 1 – Сравнение моделей

Класс	Предпосылка безопасности	Размеры ключей /подписей	Производительность и ресурсы	Масштабируемость и ограничения
Решётчатые	LWE/Ring-LWE, SVP/CVP; богатая доказательная база	открытые ключи: 1–5 КБ; подписи: 1–3 КБ	хорошая при оптимизациях; подходит для аппаратного ускорения	требует памяти/пропускной способности для больших параметров; легко масштабируются на серверы
Кодовые	декодирование линейных кодов; устойчивая практика	открытые ключи: 100 КБ–1 МБ; подписи/-шифротексты: десятки–несколько сотен байт	очень быстрые шифрование/-дешифрование; генерация ключей дороже	хранение и передача больших ключей; предпочтительны серверные инфраструктуры
Кольца /многочлены	Ring/Module-LWE, NTRU-класс; риск структурных атак	открытые ключи: 1–2 КБ; подписи: 1–2 КБ	высокая эффективность при полиномиальной арифметике; низкая латентность	хороши для встраиваемых/IoT при оптимизации; требуют аккуратной параметризации
Хеш-основанные	безопасность сводится к стойкости хеш-функций; простая модель анализа	ключи: 32–64 байта; подписи: 10–40 КБ, stateless ближе к верхней границе	производительность зависит от конструкции; stateful обычно дешевле	подходят для архивирования и контролируемых сред; управление состоянием критично
Isogeny	сложность вычисления изогений; ограниченная доказательная база	открытые ключи: 200–400 байт; подписи/обмены: 100–300 байт	относительно медленные операции; высокие вычислительные накладные расходы	ограниченная практическая зрелость; пригодны при жёстких ограничениях по размеру ключей