ТЕХНОЛОГИЧЕСКАЯ КОНФЕРЕНЦИЯ

РУТОКЕН DAY

ТЕХНОЛОГИИ ДОВЕРИЯ

КОМПАНИЯ АКТИВ

Постквантовая криптография: подходы, стандарты и перспективы

Сергей Панасенко

Директор по научной работе,
Компания «Актив»

Квантовые вычисления

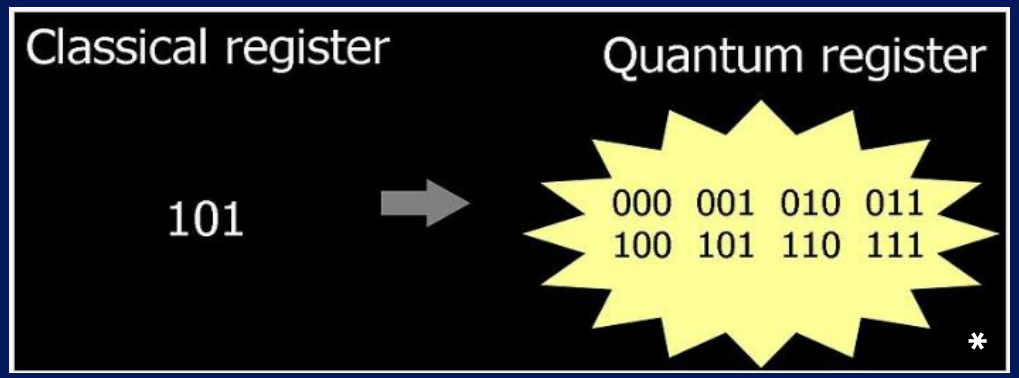
Вычисления, производимые с помощью квантового компьютера: он использует явления квантовой механики для обработки данных.

Единицей измерения данных в квантовом компьютере является кубит (q-bit – quantum bit), который находится в суперпозиции возможных значений.

Текущее состояние кубита обозначается следующим образом:

$$|\psi\rangle = a|0\rangle + b|1\rangle$$

Кубиты могут быть связаны в квантовый регистр из n кубитов, который также находится в суперпозиции всех возможных состояний:



* Рисунок: Википедия

Квантовые вычисления

«Выигрыш в квантовых алгоритмах достигается за счёт того, что при применении одной квантовой операции большое число коэффициентов суперпозиции квантовых состояний, которые в виртуальной форме содержат классическую информацию, преобразуется одновременно». *

* Источник: Википедия

Немного о терминологии

Квантовый криптоанализ	Совокупность методов анализа криптографических алгоритмов с применением квантовых вычислений
Постквантовая криптография	Совокупность криптографических алгоритмов, устойчивых к квантовому криптоанализу
Квантовое превосходство	Радикальное (суперполиномиальное) ускорение вычислений квантовым алгоритмом по сравнению с классическим
Квантовое преимущество	Существенное ускорение вычислений квантовым алгоритмом по сравнению с классическим

Основные результаты квантового криптоанализа

	Симметричные криптоалгоритмы		Асимметричные криптоалгоритмы		
Классы алгоритмов	Симметричное шифрование	Хеширование	Асимметричное шифрование	Электронная подпись	Вычисление общего ключа
Квантовый криптоанализ	Алгоритм Гровера и его варианты		Алгоритм Шора и его варианты		
Результат криптоанализа	Уменьшение битовой стойкости в два раза		Полное вскрытие		
Метод защиты	Увеличение размеров основных параметров алгоритма		Отсутствует, необходим переход на постквантовые алгоритмы		

Традиционные асимметричные криптоалгоритмы становятся подверженными полному вскрытию в случае появления квантового компьютера с достаточными ресурсами

Ограничения квантовых вычислений

#1

Квантовая декогеренция — нарушение состояния и связей между кубитами квантовой системы с течением времени

#2

Зашумление квантовых вычислений — наличие определенного процента ошибок в вычислениях на всех стадиях работы квантовой системы (обусловленных вероятностной природой квантовых вычислений)

#3

Необходимость максимальной защиты квантовых компьютеров от внешних воздействий

Скептическое мнение
о квантовых вычислениях

Вместо реальных криптозадач происходит отвлечение на «негодный» объект (квантовый компьютер) и построение фантастически умозрительных конструкций; исходя из текущей траектории развития, готовность квантового компьютера для взлома текущих отечественных стандартов электронной подписи будет не ранее, чем через 600-1200 лет. *

* Баранов А. П. Информационная безопасность, ожидания и действительность.
// XXIX научно-практическая конференция «Комплексная защита информации» — Санкт-Петербург, 2024.

Скептическое мнение
о квантовых вычислениях

Практическое осуществление квантового компьютера основано на манипулировании на микроскопическом уровне и с грандиозной точностью многоэлементной физической системой с непрерывными степенями свободы.

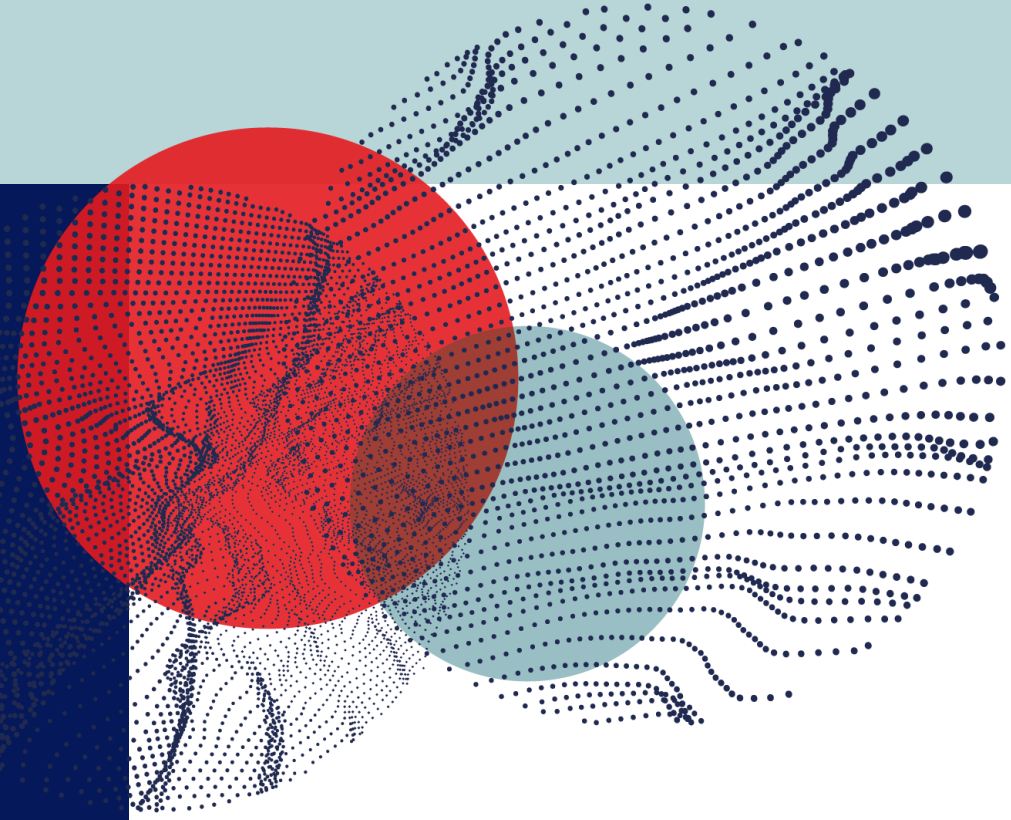
Очевидно, что для достаточно большой системы, квантовой или классической, эта задача становится невыполнимой, именно поэтому такие системы переходят из ведения микроскопической физики в область статистической физики.

Представляется ли система из $N = 10^3 \div 10^5$ квантовых спинов, необходимая, чтобы превзойти классический компьютер в решении ограниченного числа специальных задач, достаточно большой в этом смысле? Сможем ли мы когда-либо научиться контролировать 10^{300} (по меньшей мере) амплитуд, определяющих квантовое состояние такой системы? Мой ответ — «нет, никогда»*

* Дьяконов М. И. Будет ли у нас когда-нибудь квантовый компьютер? // В защиту науки. Бюллетень № 21 — Комиссия РАН по борьбе с лженаукой и фальсификацией научных исследований – М.: ПРОБЕЛ-2000, 2018 – с. 90-99.

Постквантовые криптоалгоритмы

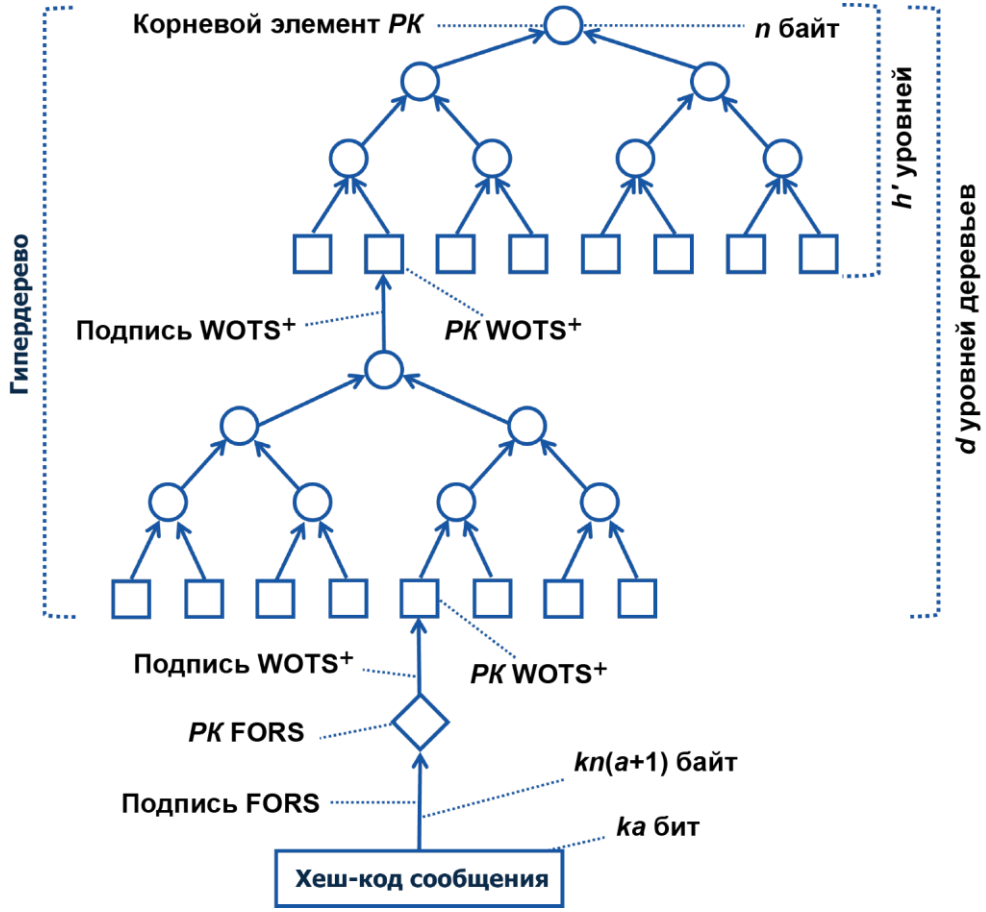
Постквантовые криптоалгоритмы должны быть основаны на задачах, сложных для решения как с помощью традиционных, так и квантовых вычислений. Это поможет им противостоять методам и классического, и квантового криптоанализа.



Основные структуры, на которых базируются известные подходы к разработке постквантовых криптоалгоритмов:

- хеш-функции;
- линейные коды;
- алгебраические решетки;
- многомерные квадратичные системы;
- изогении эллиптических кривых.

Пример структуры алгоритма на основе хеш-функций

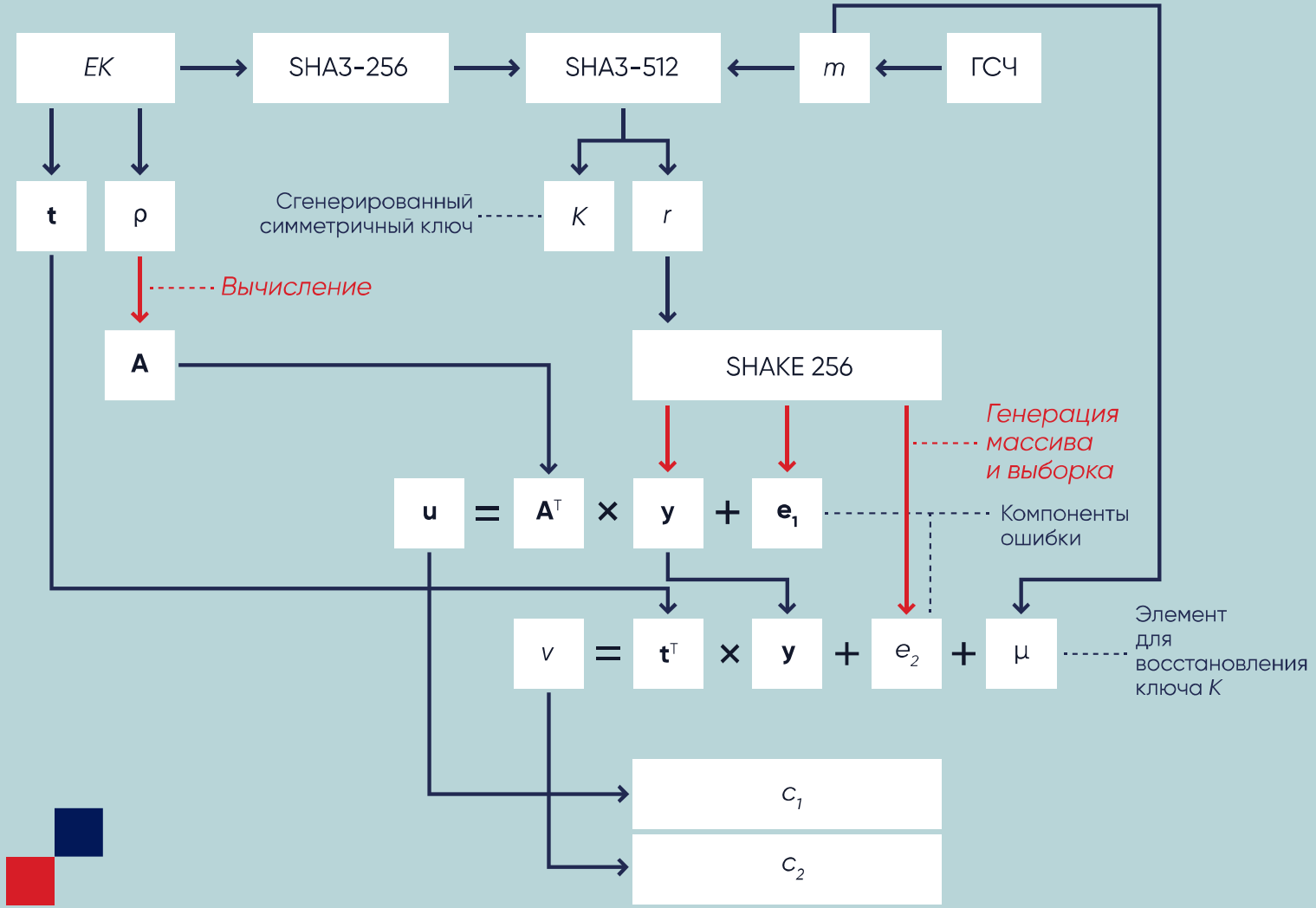


SLH-DSA: Stateless Hash-Based Digital Signature Standard.

Компоненты:

- FORS (Forest of Random Subsets) – ЭП с ограниченным количеством применений;
- WOTS+ (Winternitz One Time Signature) – одноразовая ЭП;
- XMSS (Extended Merkle Signature Scheme) – одноразовая ЭП, структурированная в виде гипердерева (HT – Hypertree);
- хеш-функции SHA-2 и SHAKE.

Пример структуры алгоритма на основе алгебраических решеток

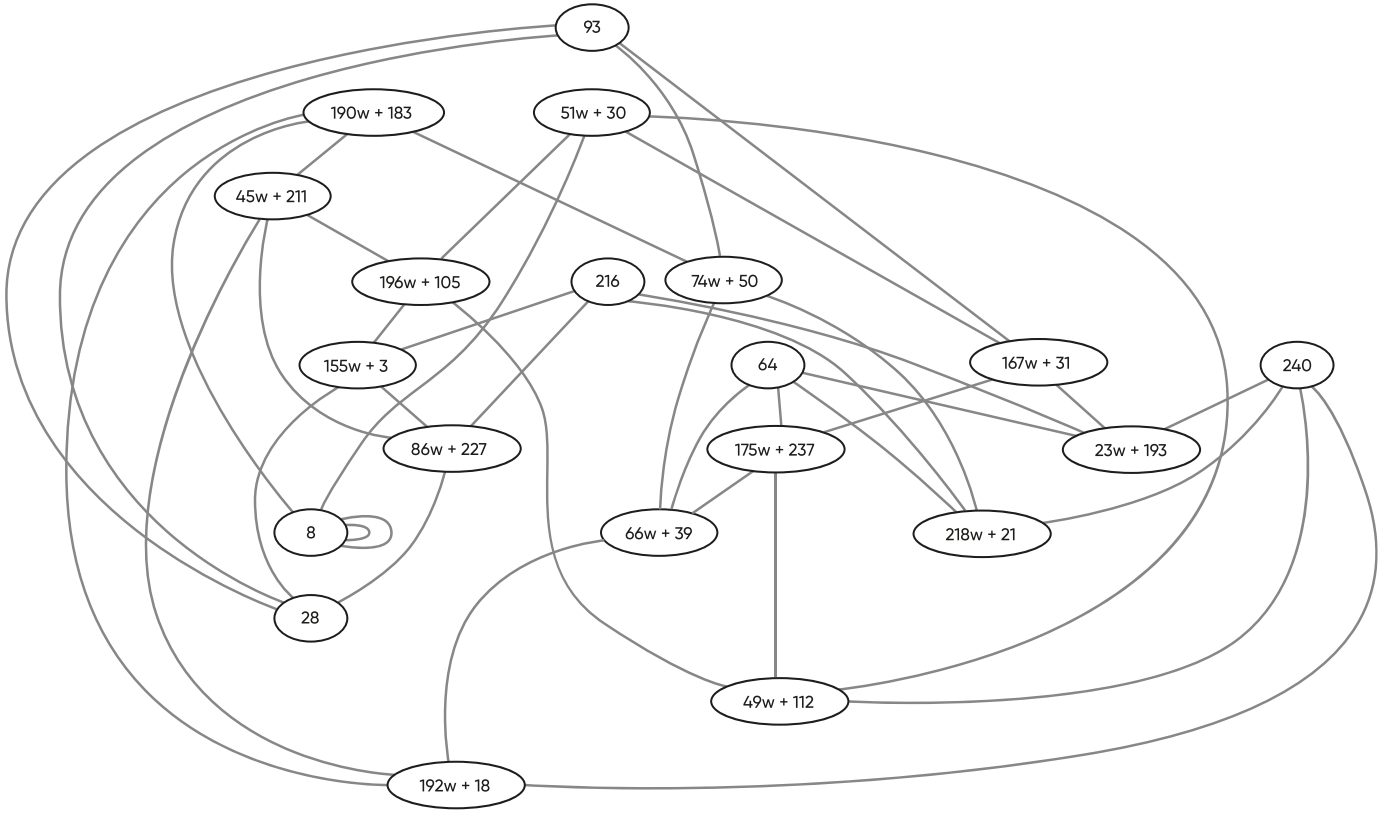


ML-KEM: Module-Lattice-Based Key-Encapsulation Mechanism.

В шифртекст вносится ошибка, которая впоследствии устраняется с помощью компонентов ключа декапсуляции.

Альтернативный вариант: округление вместо вноса ошибки.

Алгоритмы на основе изогений эллиптических кривых



Базируются
на вычислительной
сложности задачи поиска
пути в графе изогений.

* Рисунок из статьи Тараскин О. Постквантовая реинкарнация алгоритма Диффи-Хеллмана: вероятное будущее (изогении). https://habr.com/ru/companies/aktiv-company/articles/332494/ — Блог Компании «Актив» — 17.07.2017.

Пример структуры алгоритма на основе линейных кодов

Криптосистема Мак-Элиса. *

Компоненты секретного ключа (*G*, *S*, *P*):

- *G* – порождающая матрица линейного кода;
- *S* – случайная невырожденная бинарная матрица;
- *P* – случайная матрица перестановки.

Открытый ключ ($\hat{G}$):

$$\hat{G} = SGP$$

Криптосистема основана на сложности разложения открытого ключа $\hat{G}$ на его матрицы-сомножители.

$$S = \begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \end{pmatrix} \quad **$$

$$G = \begin{pmatrix} 0 & 1 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 1 & 0 \end{pmatrix}$$

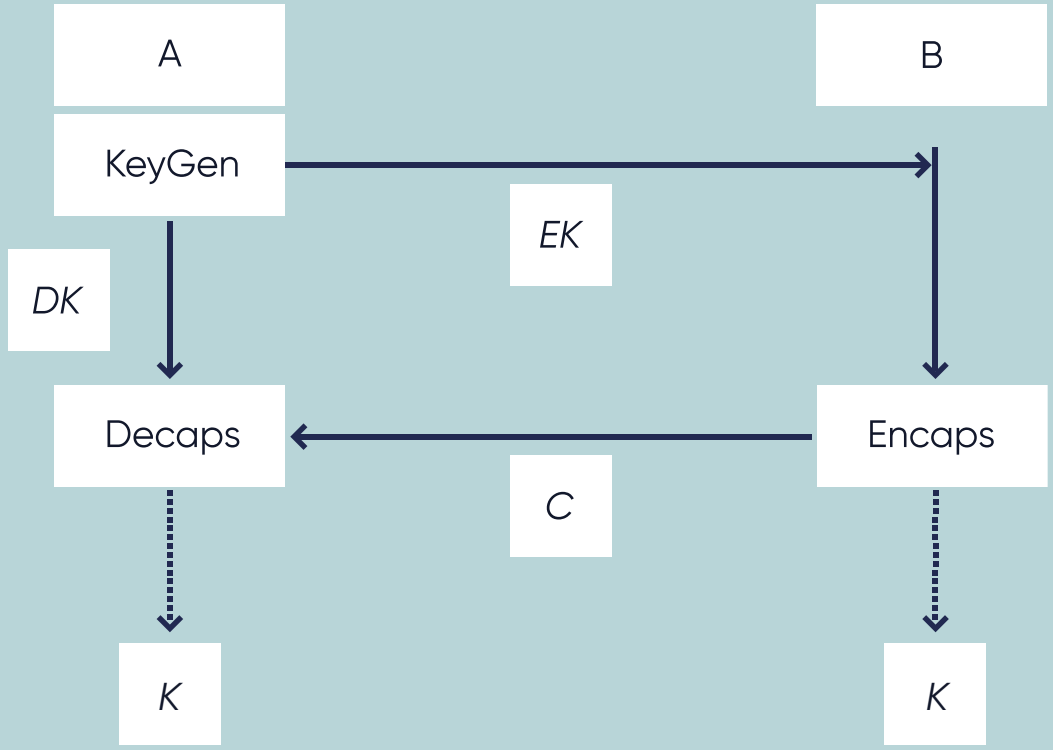
$$P = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

$$\hat{G} = SGP = \begin{pmatrix} 1 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 1 \end{pmatrix}$$

* McEliece R. J. A Public-Key Cryptosystem Based On Algebraic Coding Theory. https://ipnpr.jpl.nasa.gov/progress_report2/42-44/44N.PDF — January and February 1978.

** Пример из Википедии.

Смена парадигмы: инкапсуляция вместо вычисления общего ключа



Алгоритмы инкапсуляции ключей (KEM – Key Encapsulation Mechanism) содержат следующие процедуры:

- KeyGen – генерация долговременной асимметричной ключевой пары для последующей инкапсуляции/ декапсуляции ключей;
- Encaps – генерация и инкапсуляция симметричного ключа;
- Decaps – декапсуляция (извлечение) симметричного ключа.

Т.е. симметричный ключ не вычисляется обеими сторонами, а создается одной из них и в защищенном виде передается другой.

Стандартизация постквантовых криптоалгоритмов в России

В России разработано несколько постквантовых криптоалгоритмов, наиболее известные из них:

Алгоритм	Назначение	Основа	Компания-разработчик
«Шиповник»	ЭП	Линейные коды	НПК «Криптонит»
«Гиперикум»	ЭП	Хеш-функции	«КуАпп» (QApp)
«Крыжовник»	ЭП	Алгебраические решетки	БФУ им. И. Канта
«Кодиеум»	КЕМ	Линейные коды	НПК «Криптонит»

Есть и другие («Иггдрасиль», «Облепиха», «Земляника»…).

Технический комитет по стандартизации ТК 26 («Криптографическая защита информации») проводит анализ ряда алгоритмов с целью их стандартизации.

Стандартизация постквантовых криптоалгоритмов в США

С 2016 г. проводится конкурс NIST по выбору алгоритмов ЭП и KEM для стандартизации. *

Важнейшим промежуточным результатом конкурса стало принятие трех стандартов США на постквантовые криптоалгоритмы:

#1 KEM: FIPS 203. Module-Lattice-Based Key-Encapsulation Mechanism Standard (ML-KEM). https://doi.org/10.6028/NIST.FIPS.203.

#2 ЭП (основной): FIPS 204. Module-Lattice-Based Digital Signature Standard (ML-DSA). https://doi.org/10.6028/NIST.FIPS.204.

#3 ЭП (резервный): FIPS 205. Stateless Hash-Based Digital Signature Standard (SLH-DSA). https://doi.org/10.6028/NIST.FIPS.205.

Кроме того, постквантовые алгоритмы на основе хеш-функций с сохранением состояния XMSS и LMS (Leighton-Micali Signature) и их варианты (XMSS^{MT} – Multi-tree XMSS и HSS – Hierarchical Signature Scheme) стандартизованы в NIST SP 800-208 в 2020 г.

Принято решение о стандартизации еще двух алгоритмов: FALCON (ЭП) и HQC (KEM).

* Post-Quantum Cryptography. https://csrc.nist.gov/pqc-standardization.

Основные недостатки постквантовых криптоалгоритмов

Высокая

вычислительная ресурсоемкость. Например, количество циклов, требуемых для выполнения процедур ЭП, в сравнении с алгоритмом EdDSA-25519: *

- для алгоритма ML-DSA-44 — в среднем, больше на 1 порядок;
- для алгоритма SLH-DSA-SHAKE-128f — в среднем, больше на 2 порядка;
- для алгоритма SLH-DSA-SHAKE-128s — в среднем, больше на 3 порядка.

Большие

размеры ключей и/или ЭП или шифртекста. Например:

- размер секретного ключа алгоритма ML-DSA — от 2560 до 4896 байт;
- размер открытого ключа алгоритма ML-DSA — от 1312 до 2592 байт;
- размер ЭП алгоритма SLH-DSA — от 7856 до 49856 байт.

Сложные

преобразования увеличивают риск некорректной реализации.

* Согласно замерам производительности, выполняемым в рамках проекта eBACS: ECRYPT Benchmarking of Cryptographic Systems. https://bench.cr.yp.to.

Пути реагирования на угрозу

#1 Переход на постквантовую криптографию (PQC) сейчас

#2 Модернизация систем, включая переход на PQC, впоследствии

#3 Только усиление традиционных протоколов шифрования

*Baumgärtner L. et al. When – and how – to prepare for post-quantum cryptography. //https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/when-and-how-to-prepare-for-post-quantum-cryptography#/ – McKinsey Digital – May 4, 2022.

Варианты перехода на постквантовую криптографию

#1 Замена классических криптоалгоритмов на постквантовые.

#2 Одновременное последовательное использование традиционных и постквантовых криптоалгоритмов.

Второй из подходов («гибридный») считается более соответствующим текущим реалиям: *

- сохраняется соответствие текущим криптографическим стандартам;
- сохраняет соответствие средств криптографической защиты информации требованиям Регулятора (при условии корректного встраивания постквантовых криптоалгоритмов).

В США также рекомендован гибридный подход. **

* Смышляев С. В. Массовая постквантовая криптография: задачи и перспективы. XXVI научно-практическая конференция «РусКрипто'2024» – Солнечногорск, 19-22.03.2024 – КриптоПро.

** NIST IR 8547 ipd. Transition to Post-Quantum Cryptography Standards. Initial Public Draft. https://doi.org/10.6028/NIST.IR.8547.ipd – National Institute of Standards and Technology – November 2024.

Заключение

#1

Квантовые алгоритмы при их выполнении на квантовом компьютере могут обеспечить квантовое превосходство или преимущество при решении ряда задач, в том числе, криптоаналитических.
В частности, традиционные асимметричные криптоалгоритмы могут быть полностью вскрыты квантовым компьютером с достаточными ресурсами.

#2

Существует ряд сложных математических задач, в отношении которых не достигается квантовое превосходство или преимущество. На основе данных задач базируются постквантовые асимметричные криптоалгоритмы. Некоторые постквантовые алгоритмы стандартизованы в США или проходят стандартизацию в России.

#3

Несмотря на существующее скептическое мнение о квантовой угрозе, многие эксперты считают высоким риск появления квантового компьютера с достаточными ресурсами в течение ближайших 5-10 лет.
Рекомендуется уже сейчас начать осуществление перехода на постквантовые криптоалгоритмы.
Оптимальным вариантом видится их гибридная реализация последовательно с традиционными.

КОМПАНИЯ АКТИВ

РУТОКЕН DAY

Контактная информация

Сергей Панасенко

Директор по научной работе,
Компания «Актив»

panasenko@guardant.ru
info@rutoken.ru

www.rutoken.ru
www.aktiv-company.ru

+7 495 925-77-90
+7 916 356-53-13