«Сейфуллин оқулары-18(2): «XXI ғасыр ғылымы – трансформация дәуірі» Халықаралық ғылыми-практикалық конференция материалдары = Материалы международной научно-практической конференции «Сейфуллинские чтения – 18(2): «Наука XXI века - эпоха трансформации» - 2022.- Т.I, Ч.III. - С.84-87.

ОСНОВНЫЕ ПОДХОДЫ ПОСТКВАНТОВОЙ КРИПТОГРАФИИ

Кубигенова А.Т., докторант 2 курса
Исмаилова А.А., ассоц. профессор, доктор PhD

Казахский агротехнический университет им. С. Сейфуллина, г. Нур-Султан

Постквантовая криптография (иногда называемая квантово-устойчивый, квантово-безопасный или квантово-устойчивый) относится к криптографическим алгоритмам (обычно алгоритмам с открытым ключом) которые считаются защищенными от атак квантового компьютера. Проблема с распространенными в настоящее время алгоритмами заключается в том, что их безопасность основана на одной из трех сложных математических проблем:

1. проблема целочисленной факторизации,
2. проблема дискретного логарифма
3. дискретный логарифм эллиптической кривой.

Все эти проблемы легко решаются на достаточно мощном квантовом компьютере, использующем алгоритм Шора. Несмотря на то, что текущим, широко известным экспериментальным квантовым компьютерам не хватает вычислительной мощности для взлома любого реального криптографического алгоритма, многие криптографы разрабатывают новые алгоритмы, чтобы подготовиться к тому времени, когда квантовые вычисления станут угрозой.

В отличие от угрозы, которую квантовые вычисления представляют для текущих алгоритмов с открытым ключом, наиболее современные симметричные криптографические алгоритмы и хэш-функции считаются относительно защищены от атак квантовых компьютеров. Хотя квантовый алгоритм Гровера действительно ускоряет атаки на симметричные шифры, удвоение размера ключа может эффективно блокировать эти атаки.

В настоящее время исследования постквантовой криптографии в основном сосредоточены на шести различных подходах:

- теория решеток;
- многомерные квадратичные системы;
- электронные подписи на хэш-функциях;
- алгебраическая теория кодирования;
- изогении эллиптических кривых;

- теория кос.

Рассмотрим кратко преимущества и недостатки каждого подхода, приведем примеры конкретных реализаций [1].

Криптография на решётках. Данный раздел криптографии начал активно развиваться с 1990-х годов и включает в себя большое количество сложно вычислимых задач, некоторые из которых считаются NP-полными. Большинство схем просты в понимании, обеспечивают хорошее быстродействие и обладают свойством распараллеливания вычислений. Помимо шифрования и подписи, на решётках могут быть построены другие интересные приложения (полностью гомоморфное шифрование, шифрование и подпись с использованием атрибута. Некоторые системы из этого раздела обладают сложностью в наихудшем случае, а не в среднем, как большинство криптосистем. К минусам можно отнести отсутствие точного метода оценки сложности алгоритмов на решетках к существующим видам атак. Наиболее известной схемой является криптосистема NTRU (Nth-degree TRUncated polynomial ring) , предложенная в 1998 году.

Криптография, основанная на многомерных квадратичных системах. Стойкость этого раздела криптографии основывается на сложности решения системы многомерных квадратичных многочленов над конечным полем. Данная задача считается NP-полной. Системы из этого раздела обладают хорошей скоростью и небольшими требованиями к вычислительным ресурсам, однако, длины открытых ключей довольно большие. Наиболее известным примером является криптосистема HFE (Hidden Fields Equations), основанная на скрытых уравнениях поля и предложенная Ж. Патариным (J.Patarin) в 1996 году.

Криптография, основанная на хэш-функциях. В данный раздел входят электронные подписи, построенные с помощью хэш-функций, в силу чего обеспечивается их стойкость к квантовому вычислительному устройству. С помощью этого подхода можно выработать лишь ограниченное количество подписей на одном ключе. Также, к недостаткам системы относится тот факт, что подписанту необходимо записывать точное количество уже подписанных сообщений. Ошибка в этой записи приведёт к уязвимостям системы. Классическим примером является подпись Р. Меркла (R. Merkle), предложенная в 1979 году.

Криптография на кодах, исправляющих ошибки (алгебраическая теория кодирования). К плюсам такого рода систем можно отнести скорость вычислений. К минусам - слишком большую длину ключей. На алгебраической теории кодирования базируются криптосистемы McEliece и Niederreiter. McEliece была предложенная Р. Мак-Элисом (R. Mac-Eliece) в 1978 году. Niederreiter была разработана Х. Нидеррайтером (H. Niederreiter) в 1986 году.

Изогении суперсингулярной эллиптической кривой. Наиболее популярный протокол SIDH (Supersingular isogeny Diffie–Hellman, SIDH) позволяет произвести обмен ключами по незащищенному каналу связи. Этот факт и является его отличительной особенностью, гарантирующей

совершенную секретность. С учётом сжатия SIDH имеет наименьшую длину ключа из всех постквантовых протоколов обмена ключами. Однако полноценной криптосистемы на изогениях пока реализовано не было.

Криптосистемы, основанные на группах кос. Основы теории кос были введены в 20-х годах 19 века немецким математиком Э. Артином (E. Artin). Криптографические примитивы, основанные на группах кос, могут решать большой спектр задач ИБ (обеспечение целостности, подлинности, безотказности, конфиденциальности передаваемой информации, осуществление протоколов обмена ключами, шифрования и ЭП). Также они обладают свойством быстрой генерации ключей, но время шифрования или подписания документа оставляет желать лучшего. В качестве примера, можно привести схему ЭП WalnutDSA.

Обобщение вышеупомянутых подходов приведено в Таблице 1.

Таблица 1 - Сравнение постквантовых подходов

	Вид	Обоснование сложности	Скорость	Преимущества	Недостатки
Теория решеток	Шифрование ЭП Хэш-функции Обмен ключами Полностью гомоморфное шифрование Протоколы «забывчивой передачи» Протоколы с использованием атрибута Шифрование, основанное на идентификации	Нахождение «хорошего» базиса решетки Решение задач теории решеток в особых решетках	Хорошо реализуется на специальном ПО	Обоснование сложности в наихудшем случае Множество сфер применения	Повышенная длина ключей Отсутствие точного метода оценки сложности

Продолжение таблицы 1

Многомерные квадратичные системы	Шифрование ЭП Обмен ключами	Решение систем многомерных квадратичных уравнений	Хорошо реализуется на аппаратных средствах	Быстрота Малая длина ключей даже в сравнении с ЭК	Несостоятельность обоснования безопасности Большое количество систем было взломано Повышенная длина открытого ключа
ЭП на хэш-функциях	ЭП	Сопротивление коллизиям	Зависит от используемой хэш-функции	Сравнительная быстрота	Возможность реализации только протоколов ЭП Ограниченное количество подписей на одном ключе Безопасность зависит от выбираемой хэш- функции Большая длина подписи
Алгебраическая теория кодирования	Шифрование ЭП Хэш-функции Обмен ключами	Декодирование полных линейных кодов	Хорошо реализуется на аппаратных средствах	Хорошая скорость вычислений	Слишком большая длина ключей Большие требования к памяти устройства Большое количество систем было взломано

Изогении эллиптических кривых	Обмен ключами	Задача нахождения изогенных отображений между двумя суперсингуля рны ми ЭК	Хорошо реализуется на специальном ПО	Совершенно прямая секретность Наименьшая длина ключа	Отсутствие полноценной криптосистем ы
Теория кос	Шифрование ЭП Обмен ключами	Решение проблемы поиска сопряжений	Хорошо реализуется на аппаратных средствах	Решают большой спектр задач Быстрая генерация ключей	Медленные процессы генерации и проверки ЭП

Как и в классических криптографических алгоритмах и схемах ЭП, трудность взлома которых основывается на сложности вычисления какой-либо «трудной» односторонней математической задачи функции, в постквантовой криптографии стойкость основывается также на сложности вычисления некоторой трудно решаемой задачи.

Вышеуказанные системы, а точнее, некоторые их частные задачи, считаются стойкими как к классическим компьютерам, там и к квантовым в силу того, что на данный момент не было предложено эффективных полиномиальных квантовых алгоритмов решения этих задач, то есть криптоаналитики пока не нашли способа модификации алгоритма Шора [2] для этих систем.

Список использованной литературы

1 Комарова А.В., Коробейников А.Г. Анализ основных существующих постквантовых подходов и схем электронной подписи [Текст] / Вопросы кибербезопасности - 2019. - № 3(31). - С. 58-68.

2 Chen L., Jordan S., Liu Y.K., Moody D., Peralta R., Perlner R., Smith-tone D. Report on Post-Quantum Cryptography, NISTIR 8105 [Text] / National Institute of Standards and Technology, Gaithersburg, Maryland, April – 2016. – P. 10. https://doi.org/10.6028/NIST.IR.8105.