Постквантовая криптография. Задачи, перспективы, стандартизация

Доклад

Шишкин Василий Алексеевич (ТК 26, НПК Криптонит),
Чижов Иван Владимирович (ТК 26, МГУ, НПК Криптонит)

03 марта 2022 г.

Технический комитет 26

- Функции закреплены приказом Федерального агентства по техническому регулированию и метрологии от 09 июня 2017 года № 1319 «Об организации деятельности технического комитета по стандартизации „Криптографическая защита информации“»
- Занимается вопросами стандартизации объектов, относящихся к методам криптографической защиты информации (шифрование, аутентификация, имитозащита, электронная подпись и т.п.)
- Постоянно действующий национальный рабочий орган в подкомитете 27 «Information security, cybersecurity and privacy protection» (Безопасность информации, кибербезопасность и защита персональных данных) СТК 1 ИСО/МЭК «Информационные технологии» и в техническом комитете ИСО/ТК 307 «Blockchain and electronic distributed ledger technologies» (Технологии цепной записи данных и распределенных реестров)

Технический комитет 26. Подкомитет 2. Рабочая группа 2.5

- Название рабочей подгруппы — «Постквантовые криптографические механизмы».
- Занимается вопросами стандартизации объектов, относящихся к постквантовым методам криптографической защиты информации (шифрование, аутентификация, имитозащита, электронная подпись и т.п.)

Что такое постквантовая криптография

Определение

Постквантовый криптографический механизм — криптографический механизм, который является стойким как в классической модели противника, так и в квантовой модели противника. Квантовая модель предполагает, что противник имеет доступ к квантовому вычислителю и способен на нём запускать эффективные (полиномиальные) алгоритмы.

Что такое постквантовая криптография

- Криптография с секретным ключом (симметричная криптография): блочные, поточные шифры, криптографические хеш-функции.
  - Обычно защищают данные.
  - Задача криптоанализа сводится к поиску корней некоторого алгебраического уравнения $f(k) = 0$ над конечным полем.
  - Обычно $f(\cdot)$ не имеет простой структуры.
- Криптография с открытым ключом: схемы инкапсуляции ключа, схемы электронной подписи.
  - Решают задачи: обмен или выработка ключей шифрования, аутентификация сторон, доказательство авторства документа или сообщения
  - Задача криптоанализа обычно сводится к решению какой-либо вычислительно сложной математической задачи.
  - Стойкость большинства механизмов, используемых на практике, сводится к сложности следующих задач: целочисленная факторизация, дискретное логарифмирование в конечной мультипликативной группе.

Что такое постквантовая криптография

- Криптография с секретным ключом (симметричная криптография): блочные, поточные шифры, криптографические хеш-функции.
  - В квантовой модели сложность поиска решения уравнения, не имеющего простой структуры, понизится до $O\left(\sqrt{N}\right)$, где $O(N)$ — сложность решения этого уравнения в классической модели (алгоритм Лова Гровера, 1996 год).
  - Порядок сложности взлома криптографического механизма упадёт в 2 раза.
  - Решение: увеличение длины ключа в два раза, например, с 256 битов до 512.
  - Задачи синтеза постквантовых криптографических механизмов с секретным ключом не стоит.

Что такое постквантовая криптография

- Криптография с открытым ключом: схемы инкапсуляции ключа, схемы электронной подписи.
  - В квантовой модели задачи целочисленной факторизации и дискретного логарифмирования имеют эффективное решение (алгоритм Питера Шора, 1997 год).
  - В классической модели стойкость — 2^{128}, в квантовой — 128.
  - Снижение принципиально, так как отсутствует экспоненциальный разрыв между вычислительной сложностью алгоритмов легального абонента и злоумышленника. Решить проблему увеличением ключа нельзя.
  - Задача — разработать схемы электронной подписи и обмена ключами, стойкие как в квантовой, так и в классической модели.

Как готовится криптография к квантовой угрозе

- В 2016 году Национальный институт стандартов и технологий США (NIST USA) объявил конкурс на создание новых стандартов постквантовой электронной подписи и постквантового механизма инкапсуляции ключа.
- В 2019 году создана рабочая группа «Постквантовые криптографические механизмы» в ТК 26. Работы ведутся по разработке постквантовой электронной подписи и постквантового механизма инкапсуляции ключа.

Направления постквантовой криптографии

- Криптографические механизмы на основе криптографических хеш-функций
- Криптографические механизмы на основе систем квадратичных полиномов от многих переменных над конечным полем
- Криптографические механизмы на основе алгебраических решёток
- Криптографические механизмы на основе кодов, исправляющих ошибки
- Криптографические механизмы на основе изогений эллиптических кривых
- Другие.

Криптографические механизмы на основе криптографических хеш-функций

- Строятся на основе некоторой криптографической хеш-функции (схема Меркля–Лемпорта).
- Только схемы электронной подписи.
- Две проблемы
  - Схемы, для которых доказана стойкость в предположениях наличия стойкой криптографической хеш-функции, требуют сохранения состояния. Невозможно использовать во многих приложениях. Ориентированы на системы хранения, в том числе, построенные на основе технологии блокчейн.
  - Для универсальных схем отсутствует обоснование стойкости.

Криптографические механизмы на основе систем квадратичных полиномов от многих переменных над конечным полем

- Стойкость основана на сложности решения системы однородных алгебраических уравнений

$$\{f_i(x_1, \ldots, x_n) = 0,\ i = 1, 2, \ldots, m\ ,$$

здесь $f_i(x_1, \ldots, x_n)$ — многочлен с коэффициентами из конечного поля $GF(q)$.

- Как схемы электронной подписи, так и схемы обмена ключами.
- Проблемы: в последнее время построены алгебраические атаки на схемы, которые, в том числе, предлагались для стандартизации.
- Перспективное направление, так как можно построить «хорошие» схемы подписи. Однако нужно развивать техники анализа таких схем, для уточнения уровня стойкости.

Криптографические механизмы на основе алгебраических решёток

- Старое направление в криптографии с открытым ключом, изучается более 50 лет.
- Стойкость основана на сложности некоторых задач из теории алгебраических решёток: поиск относительно коротких векторов решёток, задача обучения с ошибкой (например, с округлением), задача поиска короткого целочисленного решения однородного линейного уравнения и т.п.
- Как схемы электронной подписи, так и схемы обмена ключами.
- Классические схемы стойкие, но имеют «непрактичные» параметры (скорость работы, длина ключей и т.п.).
- Современные схемы строятся на решётках с дополнительными алгебраическими свойствами. Насколько эти модификации стойкие?
- Уязвимы к атакам с использованием побочных каналов получения информации.

Криптографические механизмы на основе кодов, исправляющих ошибки

- Старое направление в криптографии с открытым ключом, изучается более 50 лет.
- Стойкость основана на сложности задач декодирования линейного кода, исправляющего ошибки.
- Как схемы электронной подписи, так и схемы обмена ключами.
- Классические схемы стойкие, но имеют «непрактичные» параметры (длина ключей).
- Многие современные схемы уязвимы к атакам с использованием побочных каналов получения информации.
- Крайне сложно построить схемы электронной подписи.

Криптографические механизмы на основе изогений эллиптических кривых

- Новое направление в криптографии с открытым ключом, появилось в 2010 году.
- Стойкость основана на сложности задачи построения изогении между эллиптическими кривыми (1999 год).
- Пока только схемы выработки ключей (аналог протокола Диффи–Хеллмана). Обладают достаточно малой длиной ключей, но высокой вычислительной сложностью.
- Появляются новые атаки, так как схема новая и пока недостаточно изученная.
- Пока нет подхода к построению схемы электронной подписи.
- Отсутствуют результаты в области доказуемой стойкости таких схем.

Задачи в области постквантовой криптографии

- Разработка стойких постквантовых схем электронной подписи с небольшой длиной ключа и размером подписи.
- Развитие аппарата оценки стойкости постквантовых криптографических механизмов против атак по побочным каналам.
- Разработка постквантовых криптографических механизмов, устойчивых к атакам по побочным каналам.
- Развитие аппарата доказуемой стойкости для постквантовых криптографических механизмов.
- Интеграция в существующие приложения и сетевые протоколы.

Спасибо за внимание!

Вопросы, пожалуйста.