Об одном подходе к внедрению постквантовых криптографических алгоритмов в протокол TLS

Алексеев Евгений Константинович,
к.ф.-м.н., Академия криптографии РФ, ООО «КРИПТО-ПРО», АНО «НТЦ ЦК»

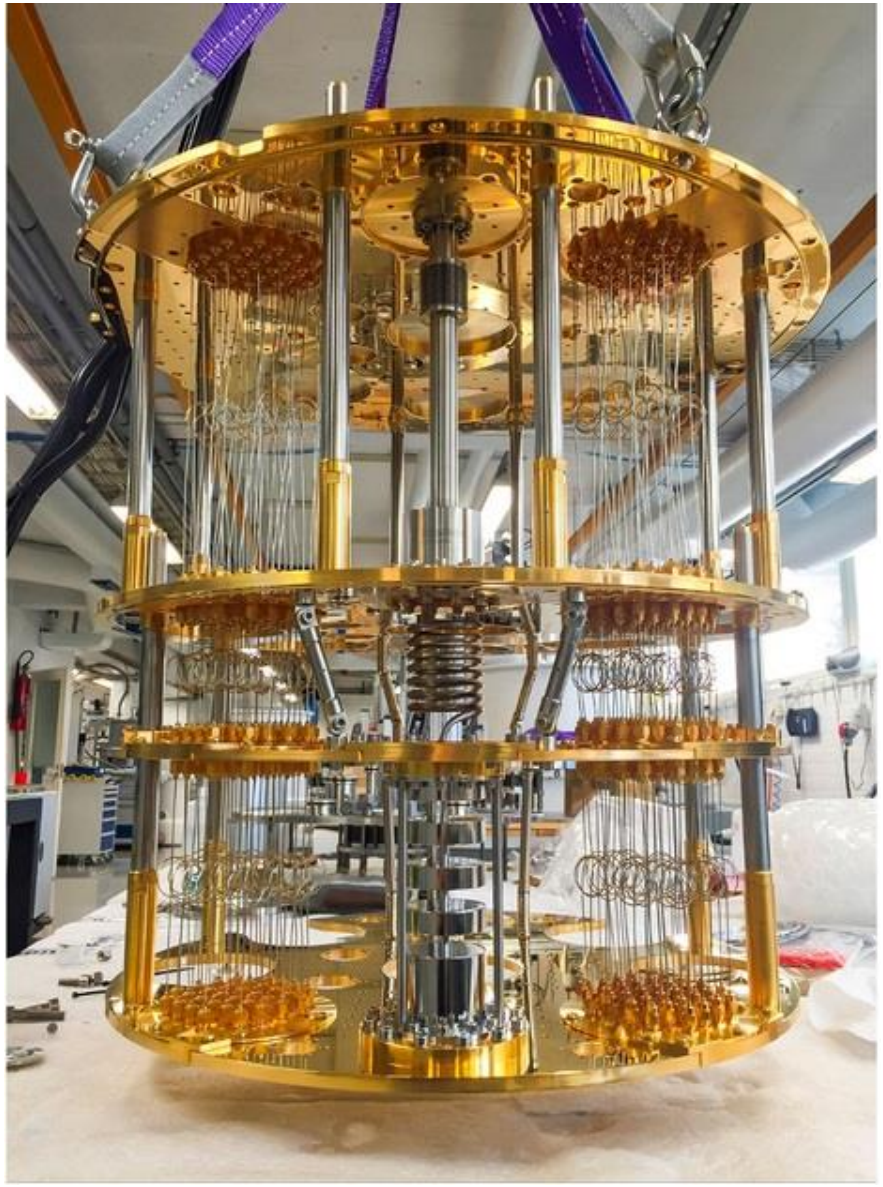
КРИПТОПРО

НТЦ ЦК

PKI-Форум Россия 2024

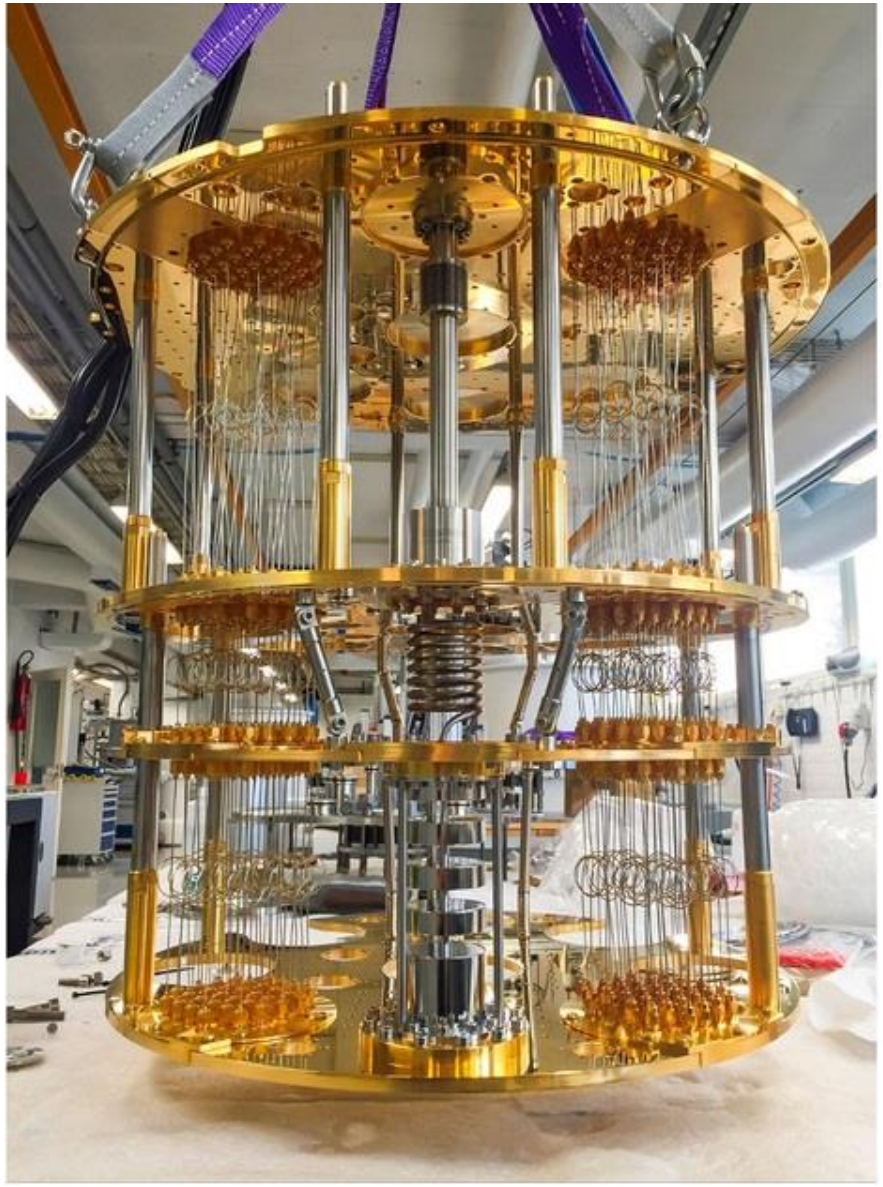
Квантовая угроза

- Квантовый компьютер – в корне отличающийся от классического принцип вычислений
- Алгоритмы Шора позволяют взламывать такие криптосистемы, как RSA, ECDSA и ГОСТ Р 34.10-2012
- Создание достаточно мощного квантового компьютера (CRQC) – все еще открытая инженерно-техническая задача, но мощности растут



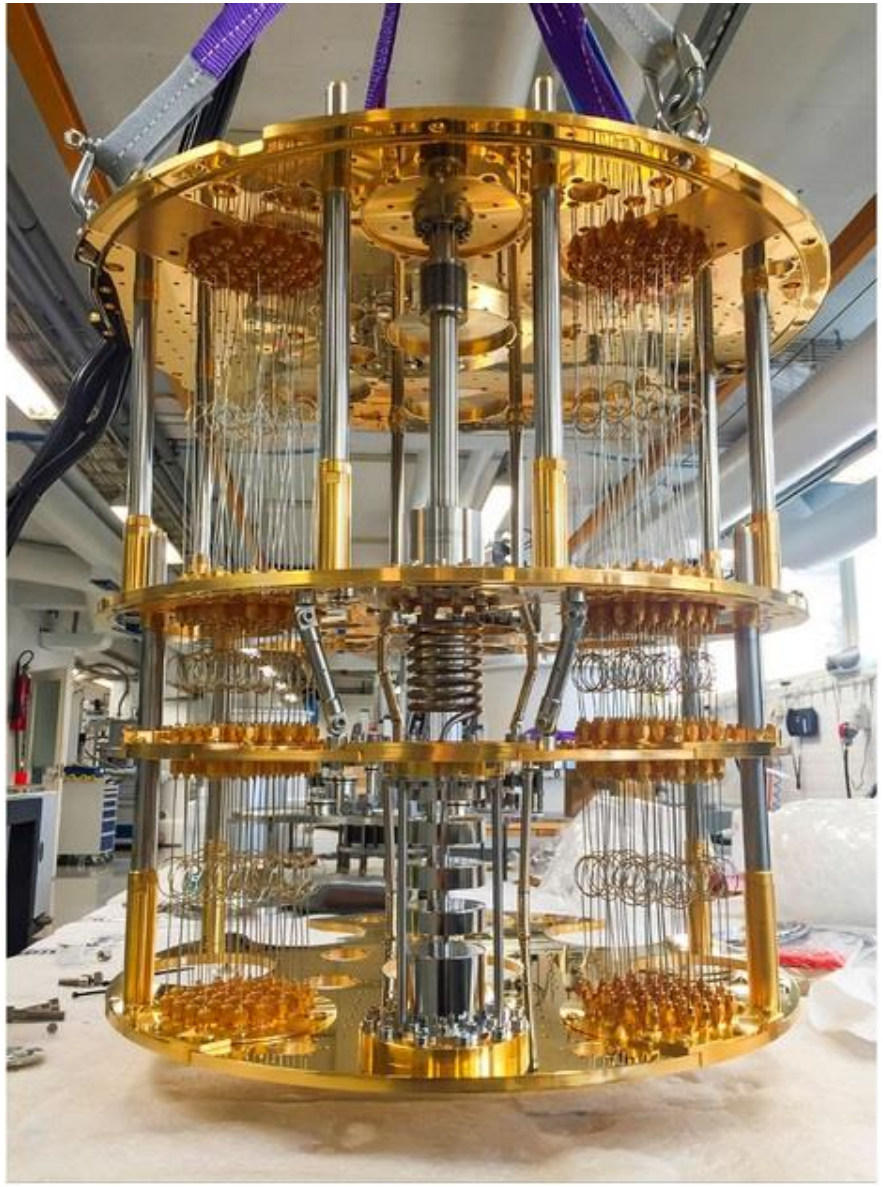
Квантовая угроза

- Атака “Harvest Now, Decrypt Later” – данные собираются сейчас, пока защищены классическими алгоритмами, а дешифруются, когда появится CRQC
- KEM нужно внедрять как можно раньше, т.к. обрабатываемые сейчас данные находятся под угрозой
- Еще одна проблема – переход на новую криптографию всегда происходит долго и мучительно



Алгоритмическая защита – постквантовый TLS

- Зачем разрабатывать постквантовый TLS, если в РФ нет стандартизированных механизмов KEM?
  - Криптографические механизмы не применяются в вакууме, всегда происходит встраивание в какой-то более высокоуровневый протокол
  - Чем раньше заработают постквантовые протоколы, тем больше данных удастся защитить
  - Чтобы не терять времени потом, необходимо разработать режим работы TLS, предполагающий использование постквантовых KEM
  - Разработанный протокол должен предъявлять четкие требования к KEM, чтобы учесть их и обосновать то, что разработанный в будущем KEM им удовлетворяет



Вопросы на пути создания отечественного постквантового TLS

- **Какой KEM встраивать?**
- В какую версию TLS встраивать отечественный KEM?
- Одноразовый или долговременный ключ?
- Как клиенту и серверу согласовывать взаимодействие с помощью KEM?

Постквантовые схемы KEM

- В мире: CRYSTALS-KYBER (решетки) – единственный KEM, победивший в конкурсе NIST
- В России (работы в рамках ТК26):
  - «Кодиеум» (коды, исправляющие ошибки) – идет выбор базового кода (НИР НТЦ ЦК и работы Криптонита в ТК26)
  - KEM на основе решеток (названия еще нет, разработка находится на ранней стадии)

Возможные аналоги Кодиеума	Открытый ключ, байт	Закрытый ключ, байт	Шифртекст/ откр. ключ, байт	Генерация ключа, мкс	Инкапсуляция (шифрование)/ вычисление общего ключа, мкс	Декапсуляция (расшифрование) / вычисление общего ключа, мкс
CRYSTALS-KYBER	800	1632	768	7	9	6
Classic McEliece	**261120**	6492	128	**9454**	10	2010
ECDH	64	32	64	72	72	72

- Вывод: в РФ близок к готовности лишь Кодиеум, но открытый ключ занимает сотни килобайтов, а время генерации ключа в сотни раз превышает существующие аналоги

Вопросы на пути создания отечественного постквантового TLS

- Какой KEM встраивать?
  - «Кодиеум» – есть недостатки, но существенно ближе к стандартизации, чем KEM на решетках
- **В какую версию TLS встраивать отечественный KEM?**
- Одноразовый или долговременный ключ?
- Как клиенту и серверу согласовывать взаимодействие с помощью KEM?

Международный опыт внедрения KEM в TLS

- TLS 1.2:
  - IETF целенаправленно не проводит работы по внедрению постквантов в TLS 1.2 и вообще какие-либо работы по развитию TLS 1.2, чтобы стимулировать переход к использованию TLS 1.3

    Критика (статья «Notes on Post-Quantum Cryptography for TLS 1.2»):

    1. Переходить на новый протокол тяжелее, чем на новые алгоритмы
    2. В некоторых ситуациях есть потребность уметь читать трафик, зная лишь долговременный закрытый ключ сервера (в TLS 1.2 так можно, в TLS 1.3 – нет)
  - Есть возможность передать большой ключ – **сообщение ServerCertificate**
- TLS 1.3:
  - В IETF нет оформившегося решения, лишь драфты («Hybrid key exchange in TLS 1.3»)
  - Эфемерные ключи передаются в ограниченных по размеру сообщениях приветствия

Вывод: встраиваем Кодиеум в TLS 1.2, т.к. без изменения состава сообщений TLS 1.3 открытые ключи Кодиеума передать невозможно

Вопросы на пути создания отечественного постквантового TLS

- Какой KEM встраивать?
  - «Кодиеум» – есть недостатки, но существенно ближе к стандартизации, чем KEM на решетках
- В какую версию TLS встраивать отечественный KEM?
  - TLS 1.2 – уже сейчас, по сути, использует KEM, и есть возможность передать ключ большого размера
- **Одноразовый или долговременный ключ?**
- Как клиенту и серверу согласовывать взаимодействие с помощью KEM?

Долговременный или эфемерный ключ?

- Долговременный:
  - Постквантовые KEM не позволяют создать подписанный запрос на сертификат
  - Доклад «Об одной проблеме при выдаче сертификатов открытых ключей постквантовых алгоритмов инкапсуляции ключа» на PKI-форуме 2023:
    - Для KEM на решетках есть лишь одна схема создания «подписи» под запросом на сертификат
    - Для KEM на теории кодирования таких схем не известно (пока)
  - НИР «Квант-2», проводимый АНО «НТЦ ЦК»: есть надежда на создание механизма доказательства знания закрытого ключа для кодового KEM (*первого в мире!*), но данный механизм слишком мало исследован, чтобы применять его прямо сейчас
- Эфемерный:
  - Для Кодиеума время генерации ключевой пары в сотни раз дольше, чем то, что работает сейчас (эллиптика)

Вывод: «кратковременный» ключ – и не долговременный, и не эфемерный, с существенно ограниченным сроком жизни (десятки часов)

Вопросы на пути создания отечественного постквантового TLS

- Какой KEM встраивать?
  - «Кодиеум» – есть недостатки, но существенно ближе к стандартизации, чем KEM на решетках
- В какую версию TLS встраивать отечественный KEM?
  - TLS 1.2 – уже сейчас, по сути, использует KEM и есть возможность передать ключ большого размера
- Одноразовый или долговременный ключ?
  - «Кратковременный» – ключ без сертификата, который используется несколько раз, но с малым сроком действия (десятки часов)
- **Как клиенту и серверу согласовывать взаимодействие с помощью KEM?**

Как согласовывать новый порядок работы?

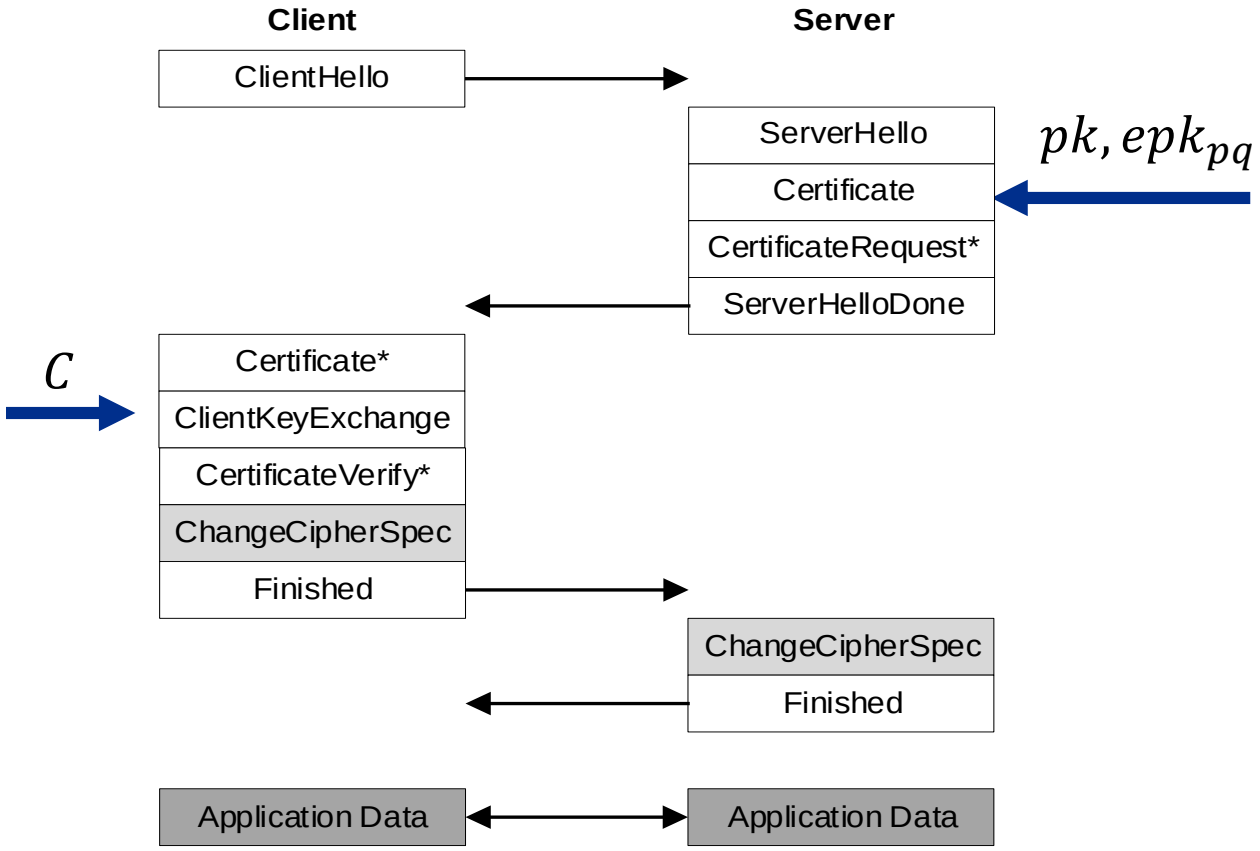
- Как сейчас:
  - В TLS 1.2 выбор состоит лишь в том, с помощью какой кривой вырабатывать ключ шифрования разделяемого секрета
  - Кривая для защиты секрета определяется сертификатом сервера
  - Считается, что клиент, указывая номер криптонабора в сообщении приветствия, сообщает серверу, что он поддерживает все стандартизированные в РФ кривые
- Потенциальные решения:
  - Клиент указывает в сообщении приветствия новую «кривую», обозначая, что он умеет работать с KEM – *не реализуемо при встраивании в Windows!*
  - Клиент два раза указывает в ClientHello существующий отечественный криптонабор – *слишком тяжело в реализации в ряде случаев и чересчур экзотично!*
  - Клиент указывает новый криптонабор – *не сможем зарегистрировать в IANA (развитие TLS 1.2 прекращено)*!

Вывод: новый криптонабор, указываемый в первом сообщении протокола

Вопросы на пути создания отечественного постквантового TLS

- Какой KEM встраивать?
  - «Кодиеум» – есть недостатки, но существенно ближе к стандартизации, чем KEM на решетках
- В какую версию TLS встраивать отечественный KEM?
  - TLS 1.2 – уже сейчас, по сути, использует KEM и есть возможность передать ключ большого размера
- Одноразовый или долговременный ключ?
  - «Кратковременный» – ключ без сертификата, который используется несколько раз, но с малым сроком действия (десятки часов)
- Как клиенту и серверу согласовывать взаимодействие с помощью KEM?
  - Через указание новых криптонаборов в первом сообщении протокола – придется работать без зарегистрированных IANA номеров, но так уже работали довольно долго раньше

Текущая структура протокола



Ключ Сервера:
$sk, cert[pk]$ – ключ классической подписи

Certificate:

1. $(esk_{pq}, epk_{pq}) \leftarrow KGen()$
2. $\sigma \leftarrow Sign(sk, epk_{pq} \parallel CH \parallel SH)$
3. $ecert_{pq} \leftarrow epk_{pq} \parallel \sigma$
4. $cert\_list \leftarrow ecert_{pq}[epk_{pq}] \parallel cert \parallel \cdots$

ClientKeyExchange:

1. $Verify(pk, epk_{pq}, \sigma)$
2. $C, PS \leftarrow Encaps(epk_{pq})$

Предстоящие работы

- Определение характера разрабатываемого документа – впервые разрабатываем протокол, который базируется на механизме, которого, строго говоря, еще нет
- Полноценный криптографический анализ протокола и формирование требований к механизму KEM
- Прохождение экспертизы ТК26

Спасибо за внимание!

КРИПТОПРО