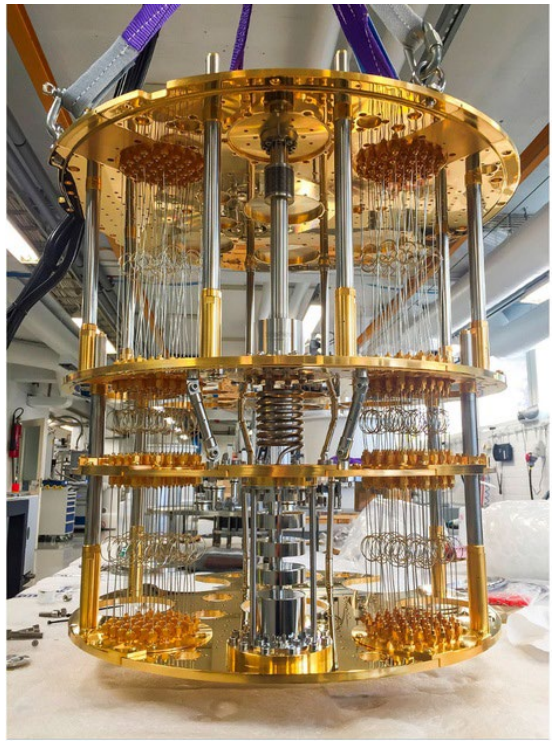
Массовая постквантовая криптография: задачи и перспективы

Смышляев Станислав Витальевич, д.ф.-м.н.
заместитель генерального директора КриптоПро

КРИПТОПРО

Постквантовая криптография: зачем и когда?

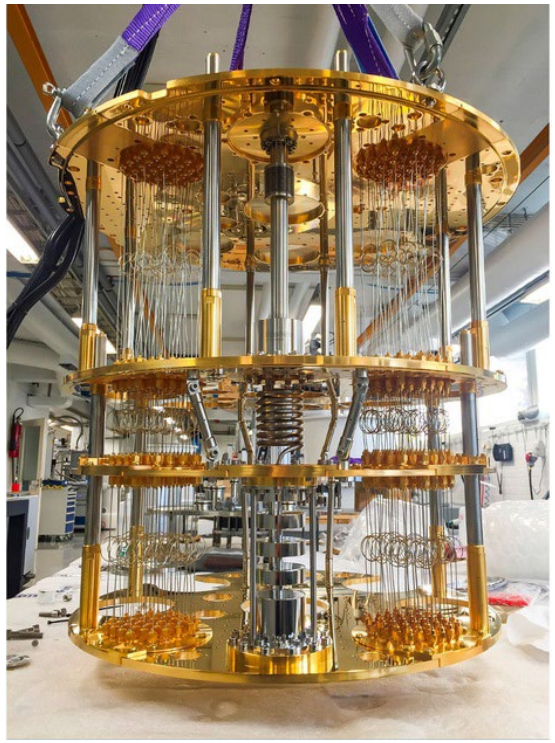
- «Квантовая угроза»: угроза создания [когда-то в будущем] криптографически значимого квантового компьютера (CRQC).
- Угроза: дешифрование в будущем защищаемых сейчас данных.



- Симметричные алгоритмы: снижение битовой стойкости вдвое.
- Электронная подпись, выработка общего ключа на основе задач факторизации и дискретного логарифмирования: экспоненциальное снижение битовой стойкости.
- Три подхода к противодействию:
  - Симметричная криптография.
  - Квантовое распределение ключей.
  - Постквантовые (квантово-устойчивые) криптографические механизмы.

Постквантовая криптография: зачем и когда?

- «Квантовая угроза»: угроза создания [когда-то в будущем] криптографически значимого квантового компьютера (CRQC).
- Угроза: дешифрование в будущем защищаемых сейчас данных.



- Симметричные алгоритмы: снижение битовой стойкости вдвое.
- Электронная подпись, выработка общего ключа на основе задач факторизации и дискретного логарифмирования: экспоненциальное снижение битовой стойкости.
- Три подхода к противодействию:
  - Симметричная криптография.
  - Квантовое распределение ключей.
  - Постквантовые (квантово-устойчивые) криптографические механизмы.
- Для массовой криптографии подход только один.

Постквантовые механизмы: схемы инкапсуляции ключа (KEM)

	NIST	ТК 26 (в разработке)
Решетки	Kyber	Отсутствует
Коды	McEliece	Кодиеум

Значения параметров (128 бит стойкости) в килобайтах (КВ):

	Открытый ключ	Закрытый ключ	Шифртекст, полученный при инкапсуляции ключа (256 бит)
Kyber	0.8	1.6	0.7
McEliece	260	6.5	0.1

Постквантовые механизмы: схемы подписи

	NIST	ТК 26 (в разработке)
Решетки	Dilithium	Крыжовник
Коды	отсутствует	Шиповник
Хэши	SPHINCS+ (без сохр. состояния) XMSS-MT (с сохр. состояния)	Гиперикум (без сохр. состояния)

Значения параметров (128 бит стойкости) в килобайтах (КВ):

	Открытый ключ	Закрытый ключ	Подпись
Dilithium	1.3	2.5	0.7
SPHINCS+	0.03	0.06	7.8
XMSS-MT (2^{60} подписей)	0.03	0.03	27
Шиповник	0.1	0.3	1000

Проблема смены базовых алгоритмов в массовой криптографии

Ожидание

- Синтез и анализ базового алгоритма
- Стандартизация базового алгоритма
- Разработка/модернизация СКЗИ
- Распространение новых СКЗИ

Проблема смены базовых алгоритмов в массовой криптографии

Ожидание

- Синтез и анализ базового алгоритма
- Стандартизация базового алгоритма
- Разработка/модернизация СКЗИ
- Распространение новых СКЗИ

Реальность

- Синтез и анализ базового алгоритма
- Стандартизация базового алгоритма
- Синтез и анализ сопутствующих алгоритмов
- Стандартизация сопутствующих алгоритмов
- [Спецификация в IETF: драфты/RFC]
- Разработка и исследования порядка применения в протоколах
- Стандартизация порядка применения в протоколах
- [Спецификация в IETF: идентификаторы IANA]
- Разработка/модернизация СКЗИ
- Тематические исследования и получение заключения Регулятора
- Встраивание в информационные системы
- Оценка влияния ИС на СКЗИ
- Распространение новых СКЗИ

КРИПТОПРО

Смена алгоритмов средств массовой криптографии: примеры

- Переход с ГОСТ Р 34.10-2001 на ГОСТ Р 34.10-2012
  - 2014 г. (январь): «О порядке перехода к использованию новых стандартов и ЭЦП и функции хэширования», от 31.01.2014 г: «Использование схемы подписи ГОСТ Р 34.10-2001 для формирования подписи **после 31 декабря 2018 года** не допускается».
  - 2016 г. (март):
    - Стандартизация сопутствующих алгоритмов.
    - Разработаны и сертифицированы СКЗИ с поддержкой ГОСТ Р 34.10-2012.
    - Запрет работы по ГОСТ Р 34.10-2001 **после 31 декабря 2018 года**:
      - в документации;
      - техническая блокировка работы СКЗИ.
  - 2018 г. (октябрь): перенос сроков на год (на **31 декабря 2019 года**).
  - 2020 г. (январь): переход на массовое использование ГОСТ Р 34.10-2012.

Внедрение постквантовых механизмов: дополнительные сложности

- Размеры сертификатов, открытых ключей и значений подписи.
- Вместо схем выработки общего ключа – KEM.
- Более сложный в реализации математический аппарат (пример: выбор параметров в соответствии с распределениями):
  - Увеличение сложности разработки СКЗИ.
  - Увеличение сложности исследований.
  - Увеличение сложности экспертизы.
- Необходимость глубокой переработки (с риском усложнения) процедур при выдаче сертификата.
  - Разработчики массовых СКЗИ ответственны за удобство установки/настройки/начала использования и нацелены на него – но не всемогущи.
- Необходимость в обозримом будущем использовать гибридные (композитные) схемы: два ключа/механизма в каждом протоколе и реализации.

Композитные подписи и КЕМ

- Гибридное встраивание механизмов – использование в протоколах и классических, и постквантовых механизмов.
- «or»-схема объединения механизмов: выбор механизма стороной обработки.
- «and»-схема объединения механизмов (композитные схемы): отдельный новый алгоритм соответствующего класса.
  - Ключ композитной схемы: конкатенация ключей двух схем.
  - На уровне приложения обрабатывается как один ключ.

	Плюсы	Минусы
«and» -схема	• Стойкая, если **хотя бы один** из базовых механизмов стойкий. • Новый механизм, но стандартный интерфейс.	• Проблемы с обратной совместимостью в ряде протоколов.
«or»-схема	• В ряде случаев проще обеспечить обратную совместимость.	• Стойкая, если **выбранный для использования** механизм стойкий. • Необходимо реализовать выбор механизма.

Если внедрять в ближайшее время, то как?

- Переход к усилению защиты за счет постквантовых механизмов **в дополнение** к основанным на эллиптических кривых по принципу «and» (схема стойкая, если хотя бы один из двух механизмов стойкий) с целью **защититься от дешифрования в будущем защищаемых сейчас данных**.
- Сохранение соответствия Требованиям независимо от свойств постквантовых механизмов (их внедрение не должно понижать стойкость).
- Сохранение обратной совместимости с существующими реализациями.
- ЭП дистрибутивов, прошивок: дополнительно подписывать с помощью постквантовых механизмов заблаговременно.
- ЭП документов:
  - сохранение юридической значимости документов (в частности, соответствие Приказу 795 и другим нормативным документам);
  - в будущем: переподписание документов.

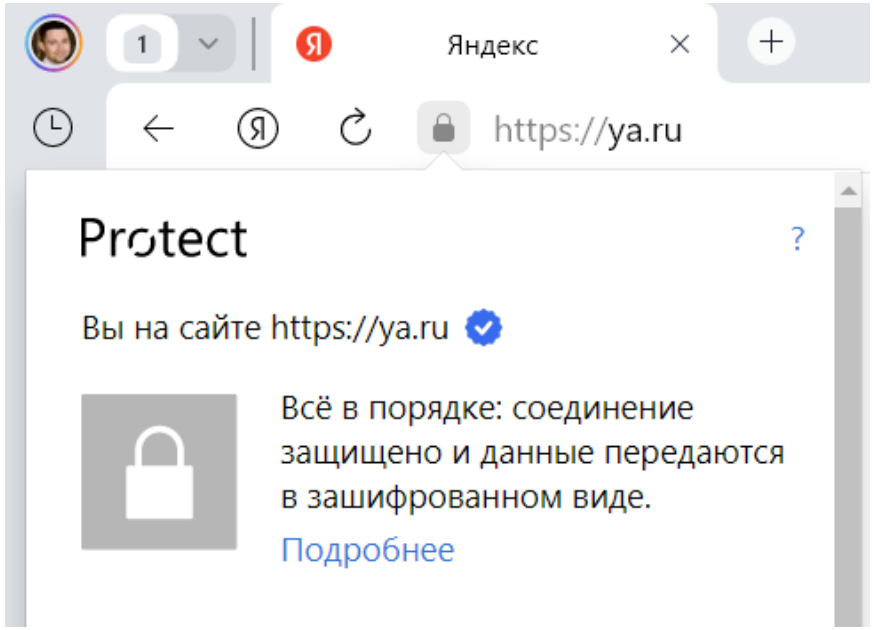
Композитные KEM: пример (ГОСТ 34.10-2018/Мак-Элиса), CMS/TLS 1.2

- Секретный ключ композитной схемы: конкатенация секретного ключа VKO (Р 50.1.113-2016) и секретного ключа криптосистемы Мак-Элиса.
- Открытый ключ композитной схемы: конкатенация открытого ключа VKO (Р 50.1.113-2016) и открытого ключа криптосистемы Мак-Элиса.

- Порядок применения KEM требуется аккуратно разрабатывать. «Наивный» пример (не учитывающий требования по безопасности) формирования симметричного ключа для CMS/TLS 1.2:
  - Выработать ключ R алгоритма VKO (Р 50.1.113-2016);
  - Вызвать VKO для R и ключа из сертификата (получить симметричный ключ K1).
  - Вызвать алгоритм инкапсуляции KEM Мак-Элиса на открытом ключе из сертификата (получить симметричный ключ K2 и шифртекст C);
  - Вычислить итоговый ключ K = H (K1 | K2);
  - Приемной стороне передать конкатенацию эфемерной точки R и шифртекст C.

Внедрение постквантовых механизмов в протокол TLS

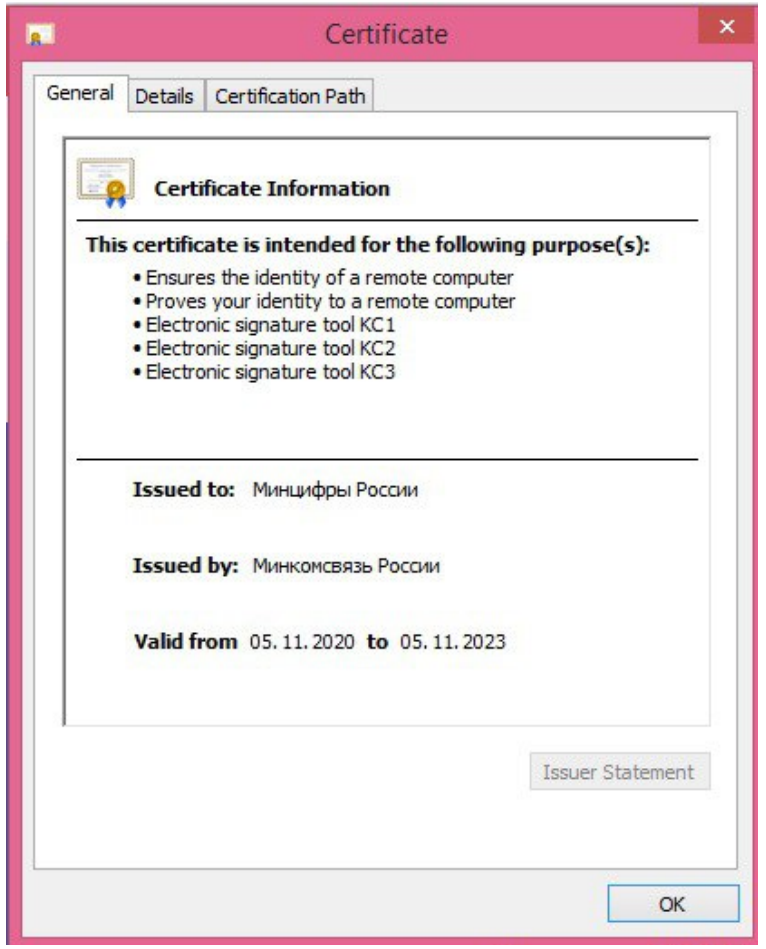
- Композитный KEM (на кодах и кривых) можно встроить в отечественный TLS 1.2 (с доработкой Рекомендаций), при этом:
  - разработать порядок подписи сертификата ключа KEM;
  - убедиться в отсутствии проблем при реализации на существующих ОС (из-за несоответствия компонент ОС RFC).



- Нет возможности без изменения протокола встроить композитный KEM (на кодах и кривых) в TLS 1.3 (ограничения на размер сообщений).
  - Путь решения: добавление дополнительных раундов взаимодействия (с потерей совместимости).
- Композитную подпись (на хэшах и кривых) можно встроить в TLS 1.2 и 1.3. Однако для задачи защиты от дешифрования в будущем защищаемых сейчас данных это не требуется.

Внедрение постквантовых механизмов в CMS

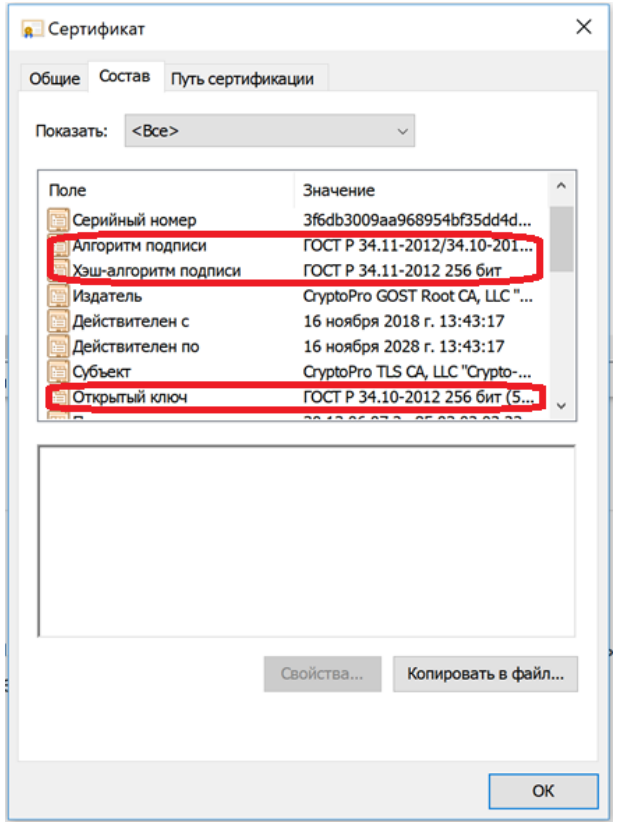
- CMS Signed Data: отдельных проблем не видно (с доработкой Рекомендаций).
  - Необходимо встроить в сертификаты.



- CMS Enveloped Data: отдельных проблем не видно (с доработкой Рекомендаций).
  - Необходимо встроить в сертификаты
  - Необходимо, как и для TLS 1.2, сделать композитный KEM для транспорта ключа шифрования данных (см. draft-ietf-lamps-cms-kyber).

Внедрение постквантовых механизмов в PKI

- Два ключа («классический» и «композитный»).
- Сертификат для «композитных» ключей для решения задачи защиты от дешифрования в будущем защищаемых сейчас данных:
  - Открытый ключ – конкатенация «классического» и «постквантового».
  - Подпись сертификата на «классическом».
- Запрос на сертификат для «композитных» ключей:
  - Офлайн-запрос на сертификат (запрос-ответ):
    - Либо сертификат в зашифрованном виде.
    - Либо протокол создания ключевой пары с доказательством знания ключа).
  - Онлайн-запрос на сертификат:
    - Интерактивный протокол доказательства с помощью расшифрования (с разработкой новых API СКЗИ, ограничением способов выпуска сертификата).



Массовая постквантовая криптография: план действий

- Работать, не дожидаясь стандартизации базовых механизмов в ТК 26.
  - Механизмы: синтез, анализ.
  - Сопутствующие алгоритмы и процедуры: синтез, анализ.
  - Протоколы: выбор решений по доработке протоколов.
  - Документы: перечень требуемых стандартов/рекомендаций и НПА (форматы сертификатов, электронных документов и т.п.).
  - Макетирование и испытания: проверка функциональных свойств.
  - Реализации: доработка СКЗИ (пока в экспериментальном режиме).
  - Методики: исследования СКЗИ, встраивание в ИС, оценка влияния.
- Учитывать зарубежный опыт и подходы (например, draft-ietf-pquip-pqc-engineers).
- Реалистичная цель: в течение 5 лет после стандартизации механизмов перейти в средствах массовой криптографии на поддержку гибридных схем.
  - ТК 26, НТЦ ЦК, разработчики СКЗИ и лаборатории
  - Поиск и обсуждение решений на секциях CTCrypt и РусКрипто.

Спасибо за внимание!