PQ/T-гибридные схемы цифровой подписи как этап миграции к постквантовой криптографии

Руслан Качмазов
Старший инженер по информационной безопасности, Яндекс Облако
Студент НИУ ВШЭ

rukachmaz@yandex-team.ru

О чем поговорим

1. Актуальность
2. Что хотим получить
3. Систематизация элементов дизайна
4. Анализ безопасности

Актуальность

Реальна ли угроза?

Сроки появления CRQC — **не определены**.

Риск — **велик**.

Существующие решения

Harvest Now, Decrypt Later — один из главных двигателей развития PQC, потому что ретроспективные атаки наиболее опасны.

Для митигации массово внедряются **PQ/T механизмы обмена ключами (KEX)**.

Где уже сейчас применяются PQ/T-гибридные KEX

- Cloudflare
- Google Chrome
- OpenSSH
- Apple iMessage
- Signal
- И многие другие

Что под капотом?

Чаще всего **X25519MLKEM768** — комбинация **X25519 ECDH** и **ML-KEM-768.**

Ранее были PQ/T-гибриды на базе оригинального **CRYSTALS-Kyber**, но сейчас они перестали быть актуальными.

Ряд внедряемых гибридных KEX уже отражен в IANA.

Решения для гибридных KEX есть.
Пора подумать про подпись.

Что хотим получить

Мотивация

Для использования PQ/T-гибридных схем ЦП

Управление рисками

Если мы допускаем появление CRQC в ближайшие десятилетия, то миграция необходима уже сейчас.

Но нужен промежуточный этап, так как прямая миграция рискованна.

Обратная совместимость

Для обеспечения функциональности и безопасности всех систем, включая устаревшие, необходимо учесть требования обратной совместимости.

Гибридные схемы дают такую возможность.

Терминология

- **Многоалгоритмическая схема** — криптографическая схема, которая включает более одного компонентного алгоритма, причем эти компонентные алгоритмы имеют одинаковое криптографическое назначение как друг с другом, так и со всей многоалгоритмической схемой.

- **Постквантовая/традиционная (PQ/T) гибридная схема ЦП** — многоалгоритмическая схема цифровой подписи, состоящая из двух или более компонентных алгоритмов цифровой подписи, где по крайней мере один из них является постквантовым алгоритмом, а по крайней мере один – традиционным.

RFC с терминологией: https://datatracker.ietf.org/doc/html/rfc9794

Важные свойства гибридных схем ЦП

- **Гибридная аутентификация** — свойство, согласно которому аутентификация обеспечивается PQ/T-гибридной схемой до тех пор, пока хотя бы один компонентный алгоритм, предназначенный для обеспечения данного свойства, остается стойким.

- **Гибридная неподделываемость** — свойство, согласно которому допущение безопасности для PQ/T гибридной схемы сохраняется, пока хотя бы один из компонентных алгоритмов сохраняет это допущение. Частный случай гибридной аутентификации.

- **Композиционность доказательств** — свойство, при котором компонентные алгоритмы объединяются так, что можно доказать редукцию безопасности гибридной схемы к безопасности компонентных алгоритмов.

Систематизация элементов дизайна

1. Ось A: тип комбинируемых алгоритмов
2. Ось B: степень атомарности представления
3. Ось C: способ комбинирования на уровне примитива
4. Ось D: политика принятия
5. Ось E: уровень неразделимости
6. Ось F: расположение артефактов
7. Ось G: способ внедрения в PKI

1. Ось A: тип комбинируемых алгоритмов
2. Ось B: степень атомарности представления
3. Ось C: способ комбинирования на уровне примитива
4. Ось D: политика принятия
5. Ось E: уровень неразделимости
6. Ось F: расположение артефактов
7. Ось G: способ внедрения в PKI

Тип комбинируемых алгоритмов

Ось A

1. PQ/T

Рассматриваемый вариант — в гибридной схеме как минимум один постквантовый алгоритм, и как минимум один — традиционный.

Например:

- ГОСТ 34.10 + Гиперикум
- ML-DSA + ECDSA

2. PQ/PQ

В гибридной схеме как минимум два постквантовых алгоритма, как правило, основанных на разных математических задачах.

Например:

- Гиперикум + Шиповник
- ML-DSA + SLH-DSA

1. Ось A: тип комбинируемых алгоритмов
2. Ось B: степень атомарности представления
3. Ось C: способ комбинирования на уровне примитива
4. Ось D: политика принятия
5. Ось E: уровень неразделимости
6. Ось F: расположение артефактов
7. Ось G: способ внедрения в PKI

Степень атомарности представления

Ось B

1. Композитный

Гибридная схема представляется как единый логический объект или алгоритм подписи.

2. Частично-композитный

Внешнее оформление в виде обертки или контейнера, но компонентные подписи внутри остаются различимыми.

3. Некомпозитный

Гибридность выражается через несколько самостоятельных аутентификационных объектов.

1. Ось A: тип комбинируемых алгоритмов
2. Ось B: степень атомарности представления
3. Ось C: способ комбинирования на уровне примитива
4. Ось D: политика принятия
5. Ось E: уровень неразделимости
6. Ось F: расположение артефактов
7. Ось G: способ внедрения в PKI

Способ комбинирования на уровне примитива

Ось C

1. Параллельное

Наиболее простой комбайнер, где каждая компонента работает независимо, а гибридная подпись — объединение подписей компонент, например, конкатенация.

2. Вложенное (nested)

Последовательная подпись одной компоненты другой, например, $\sigma = Sign_2(m, Sign_1(m))$

3. Связанное

Компонентные алгоритмы остаются различимыми, но у них есть связующая сущность, например, общий prehash.

4. Интегрированное (fused)

Подпись формируется как единое целое на криптографическом уровне, без явного выделения компонент.

1. Ось A: тип комбинируемых алгоритмов
2. Ось B: степень атомарности представления
3. Ось C: способ комбинирования на уровне примитива
4. Ось D: политика принятия
5. Ось E: уровень неразделимости
6. Ось F: расположение артефактов
7. Ось G: способ внедрения в PKI

Политика принятия

Ось D

1. Конъюнктивная (AND)

Подпись валидна тогда, когда валидны все компонентные подписи.

Более безопасный вариант.

2. Дизъюнктивная (OR)

Подпись валидна тогда, когда валидна хотя бы одна компонентная подпись.

Подходит для обратной совместимости.

1. Ось A: тип комбинируемых алгоритмов
2. Ось B: степень атомарности представления
3. Ось C: способ комбинирования на уровне примитива
4. Ось D: политика принятия
5. Ось E: уровень неразделимости
6. Ось F: расположение артефактов
7. Ось G: способ внедрения в PKI

Уровень неразделимости

Ось E

1. Отсутствие неразделимости

Компонентные подписи можно незаметно разделить.

2. Слабая неразделимость (WNS)

Компонентные подписи можно разделить, но это оставит артефакты. Верификация в таком случае может пройти.

3. Сильная неразделимость (SNS)

Подпись не пройдет верификацию при отделении хотя бы одной из компонент. Не зависит от внешних артефактов.

4. Одновременная верификация (SNS+SV)

Усиление SNS. Честный проверяющий не может завершить проверку гибридной подписи, не зная статуса проверки всех компонент.

1. Ось A: тип комбинируемых алгоритмов
2. Ось B: степень атомарности представления
3. Ось C: способ комбинирования на уровне примитива
4. Ось D: политика принятия
5. Ось E: уровень неразделимости
6. Ось F: расположение артефактов
7. Ось G: способ внедрения в PKI

Расположение артефактов

Ось F

1. Артефакт в подписи

Алгоритмический уровень. Признак гибридизации встроен в саму подпись. Наименее зависит от внешней инфраструктуры; естественно согласуется с SNS, а в сильном случае и с SV.

2. Артефакт в сертификате или цепочке

Протокольный уровень. Признак гибридизации задается сертификатом или цепочкой сертификатов, а не самой подписью. Безопасность сильнее зависит от PKI и правил проверки.

3. Артефакт в согласовании

Протокольный уровень. Признак гибридизации фиксируется при согласовании алгоритмов или параметров, например как в TLS. Безопасность зависит от контекста протокола и корректности его обработки.

4. Артефакт в сообщении

Уровень политики. Признак гибридизации содержится в самом сообщении. Требует анализа содержимого и может создавать риск циклической зависимости.

1. Ось A: тип комбинируемых алгоритмов
2. Ось B: степень атомарности представления
3. Ось C: способ комбинирования на уровне примитива
4. Ось D: политика принятия
5. Ось E: уровень неразделимости
6. Ось F: расположение артефактов
7. Ось G: способ внедрения в PKI

Способ внедрения в PKI

Ось G

1. Гибридный сертификат или цепочка

Один объект PKI содержит все компоненты.
Наиболее атомарный формат, но требует обновления OID, ASN.1, парсеров и ПО.

2. Параллельные цепочки

Использование двух параллельных цепочек сертификатов. Мягкий путь миграции, потенциально сохраняющий обратную совместимость и не требующий значительных изменений.

3. Смешанная цепочка

В рамках одной цепочки сертификатов есть постквантовые, традиционные и/или гибридные.
Наиболее реалистичный вариант постепенной миграции.
Возможна поддержка обратной совместимости.

Возможные противоречия

Сильная неразделимость
и обратная совместимость

Гибридная
неподделываемость
и обратная совместимость

Композитное
представление и обратная
совместимость

Композиционность
доказательств
и интегрированное
комбинирование

Параллельное
комбинирование
и сильная неразделимость

Мягкая PKI-миграция
и композитное
представление

Анализ безопасности

1. Модель атакующего
2. EUF-CMA в контексте PQ/T-гибридных ЦП
3. Формулировка критериев безопасности

XyZ-модель атакующего

Полезно понимать, на каких этапах атакующий обладает доступом к CRQC
и как он взаимодействует с оракулом.

Источник: https://eprint.iacr.org/2017/460.pdf

Параметры модели

X

Тип атакующего в период доступа к оракулу подписи.

- **Q** — квантовый
- **C** — классический

y

Тип доступа к оракулу подписи.

- **q** — квантовый доступ, включая запросы в суперпозиции
- **c** — классические запросы

Z

Тип атакующего после завершения доступа к оракулу подписи.

- **Q** — становится или остается квантовым
- **C** — остается классическим

Интерпретируемые модели атакующего

CcC

Классический атакующий с классическим доступом к оракулу.

CcQ

Атакующий является классическим во время доступа к оракулу и взаимодействует с ним также в классическом виде, но в будущем он имеет CRQC.

QcQ

Квантовый атакующий как во время доступа к оракулу, так и после, но интерфейс взаимодействия его с оракулом — классический.

QqQ

Полностью квантовый атакующий.

Иерархия как цепочка импликаций

$$QqQ \Rightarrow QcQ \Rightarrow CcQ \Rightarrow CcC$$

Доказательство: https://eprint.iacr.org/2017/460.pdf, стр. 8

1. Модель атакующего
2. EUF-CMA в контексте PQ/T-гибридных ЦП
3. Формулировка критериев безопасности

EUF-CMA базово

Экзистенциальная неподделываемость (EUF) при атаке с адаптивным выбором сообщений (CMA)

1. Генерация пары ключей $(sk,\ pk) \leftarrow KeyGen(1^n)$.

2. $A(1^n,\ pk)$ — вероятностному полиномиальному противнику передаются параметр безопасности 1^n и открытый ключ pk .

3. Инициализация множества сообщений, уже подписанных по запросу противника A: $M' = \emptyset$.

4. При запросе A на подпись сообщения $m \in M$, оракул вычисляет $Sign(sk,\ m)$ и возвращает σ^* противнику, после чего добавляет m в M'.

5. Противник A выдает пару $(m^*,\ \sigma^*)$, после чего проверяются два условия:

   a. $Verify(pk,\ \sigma^*,\ m^*) = 1$ — подпись σ^* на сообщении m^* прошла верификацию.

   b. $m^* \notin M'$ — сообщение m^* ранее не подавалось на подпись.

Основные атаки на PQ/T-гибридные схемы ЦП

Stripping attack

Атака разделения, при которой атакующий, получив гибридную подпись, удаляет одну из ее компонентов и пытается использовать оставшуюся часть отдельно. Целью может быть обход требования гибридной проверки или перевод гибридной подписи в контекст проверки только одной компоненты.

Component algorithm forgery

Атака, при которой компонент гибридной подписи принимается как самостоятельная подпись соответствующего алгоритма, хотя отдельно этот алгоритм для данного сообщения не вызывался. Если такой алгоритм используется отдельно в другой системе, то это может приводить к EUF-CMA-подделке для компонентного алгоритма в этом внешнем контексте.

Особенности EUF-CMA для PQ/T-гибридов

Допустим прямое расширение EUF-CMA на PQ/T-гибриды

При формальном определении EUF-CMA для гибридных схем так же, как и для традиционных, мы охватываем только стойкость гибридного объекта относительно гибридного верификатора.

В отличие от обычных схем, для гибридов дополнительно существенны риски подделки на уровне компонентных алгоритмов, межалгоритмического использования отделенных компонентов подписи, повторного использования ключей и степень неразделимости конструкции.

Практический смысл EUF-CMA для гибридов зависит от уровня неразделимости и возможности переиспользования ключей.

Защита от component algorithm forgery

Два основных варианта:

- Запрет на переиспользование ключей
- Обеспечение как минимум сильной неразделимости (SNS)

1. Модель атакующего
2. EUF-CMA в контексте PQ/T-гибридных ЦП
3. Формулировка критериев безопасности

Формулировка критериев безопасности

В случае PQ/T-гибридных схем ЦП безопасность корректнее формулировать как комплексное утверждение, включающее в себя:

- Модель атакующего
- Модель стойкости
- Условия, исключающие stripping-атаки и межалгоритмические эффекты.

Дальнейшее направление исследований

Для большей практической пользы следует рассмотреть сценарии и механизмы внедрения PQ/T-гибридных схем ЦП в PKI, учитывая их особенности.

Ваши вопросы

Руслан Качмазов
Старший инженер по информационной безопасности, Яндекс Облако
Студент НИУ ВШЭ

rukachmaz@yandex-team.ru