Об одной проблеме при выдаче сертификатов открытых ключей постквантовых алгоритмов инкапсуляции ключа

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

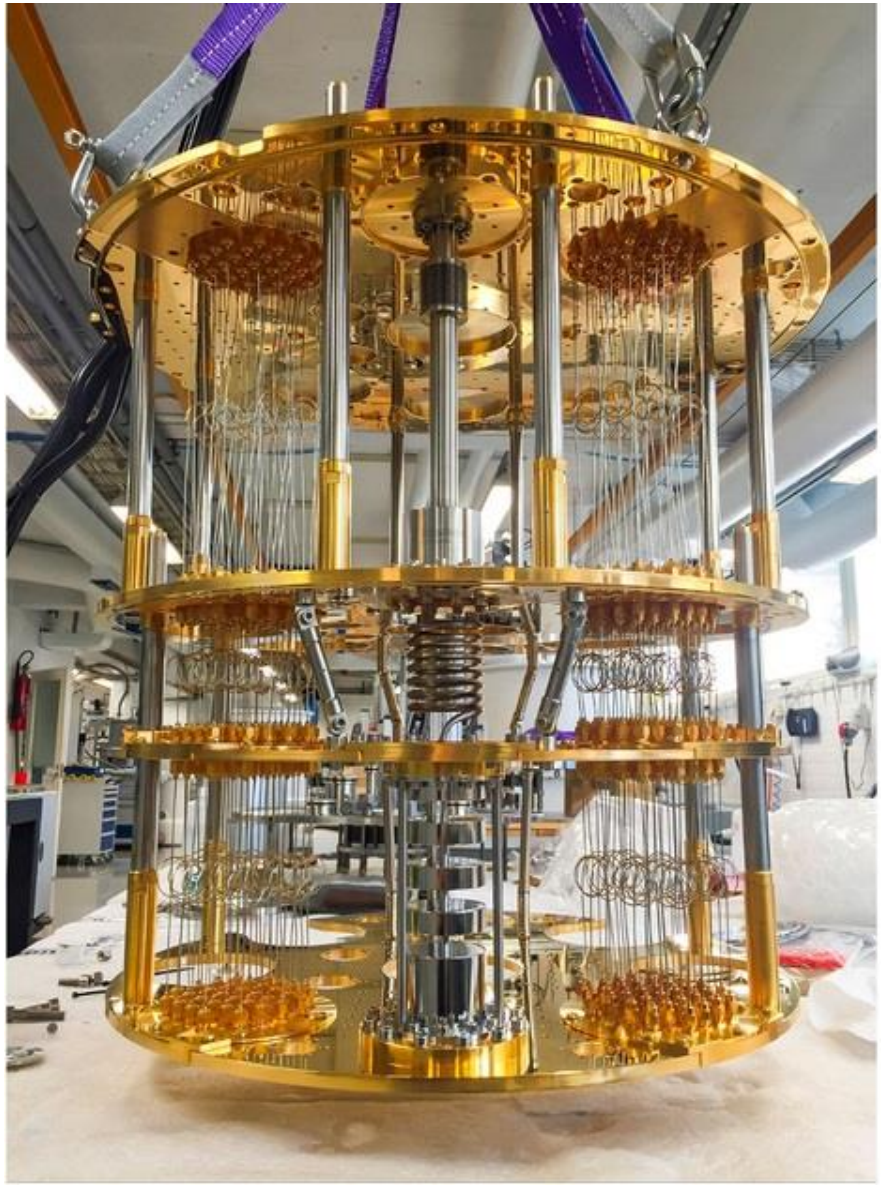
Зинюк Борис Федорович,
Академии криптографии РФ

КРИПТОПРО

PKI-Форум Россия 2023

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 – все еще открытая инженерно-техническая задача, но мощности растут:
- Опасность:
  - трафик можно собирать сейчас, а расшифровать потом
  - сложность перехода на новую криптографию в промышленных масштабах



КРИПТОПРО

Подходы к защите

- Квантовое распределение ключей
  - Стойкость основана на физических принципах
  - Требует наличия достаточно сложной аппаратуры
  - Требует предварительного распределения симметричного ключа
- Постквантовые алгоритмы
  - Стойкость основана на математических задачах, для которых не известно эффективных алгоритмов решения ни на классическом, ни на квантовом компьютере
  - Могут быть реализованы программно
  - Заметно менее эффективны (и по времени вычислений, и по размерам параметров), чем классические криптоалгоритмы

Постквантовые алгоритмы

- Два основных класса алгоритмов:
  - электронная подпись
  - алгоритм шифрования ключа (KEM – Key Encapsulation Mechanism)
- Состояние исследований в мире и в РФ
  - Открытый конкурс NIST в США: 2017-2023 год, 4 победителя (и 5 альтернативных схем):
    - 1 KEM: CRYSTALS-KYBER (решетки)
    - 3 схемы подписи: CRYSTALS-Dilithium (решетки), FALCON (решетки), SPHINCS+ (хэши)
  - Рабочая группа в ТК26: функционирует с 2021 года, в разработке следующие механизмы:
    - 2 KEM: на основе кодов и решеток
    - 3 схемы подписи: Гиперикум (хэши), Крыжовник (решетки), Шиповник (коды)

Выдача сертификатов для KEM

- Протокол выдачи сертификата:
  - Клиент генерирует ключевую пару и подписывает запрос на сертификат
- Зачем подписывать запрос на сертификат?
  - Доказательство владения закрытым ключом (Proof-of-Possession, PoP)
  - Если нет PoP, возможны атаки на прикладные протоколы: UKS-атака на протокол STS-MAC [MQV95]
  - Подробнее: «On the usefulness of proof-of-possession», 2003 [ANL03]
- Выдача сертификата для существующих KEM
  - Выработка ключа по схеме Диффи-Хеллмана и дальше симметричное шифрование
  - Ключевая пара – скаляр d и соответствующая кратная точка $Q = d \cdot P$ (как и для подписи!)
  - PoP для таких KEM – подпись запроса на сертификат с помощью ключа d

Проблема постквантового KEM

Конкурс NIST. KEM

Решетки

- CRYSTALS-Kyber
- Saber
- Frodo

Коды

- Classic McEliece
- BIKE
- HQC

Конкурс NIST. Signature

Решетки

- CRYSTALS-Dilithium
- Falcon

Хэш-функции

- Sphincs+

КРИПТОПРО

Проблема постквантового КЕМ

Конкурс NIST. KEM

Решетки

- CRYSTALS-Kyber
- Saber
- Frodo

Коды

- Classic McEliece
- BIKE
- HQC

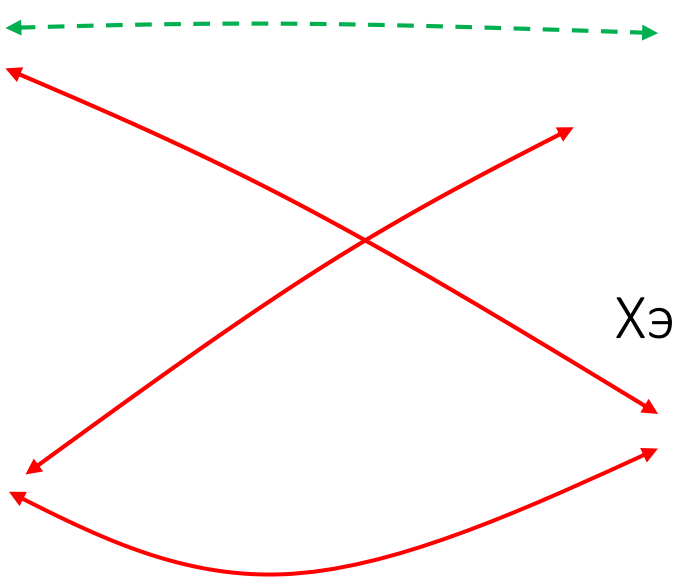
Конкурс NIST. Signature

Решетки

- CRYSTALS-Dilithium
- Falcon

Хэш-функции

- Sphincs+



Ключи схем несовместимы по формату

Ключи схем потенциально (!) совместимы

КРИПТОПРО

Возможные подходы

- Оффлайн-запрос на сертификат (схема запрос-ответ):
  - Использование ключа KEM для подписи запроса
  - Зашифрованный сертификат
  - Генерация ключа с доказательством (Verifiable Generation)
- Онлайн-запрос на сертификат (протокол с 3+ пересылками)
  - Доказательство с помощью расшифрования: протоколы из [CMP05]

Подпись на ключе KEM

Конкурс NIST. KEM

Решетки

- CRYSTALS-Kyber

Конкурс NIST. Signature

Решетки

- CRYSTALS-Dilithium

Параметры: q, n, k, l – натуральные числа, χ – распределение над R_q

$R_q = \mathbb{Z}_q[x]/(x^n+1)$ – кольцо многочленов

Закрытый ключ: $(s, e) \in R_q^k \times R_q^l$ – два вектора многочленов (многочлены выбраны в соответствии с χ)

Открытый ключ: $(A, b = A \cdot s + e) \in R_q^{k \times l} \times R_q^l$ – матрица и вектор многочленов

КРИПТОПРО

Подпись на ключе KEM

Конкурс NIST. KEM

Решетки

- CRYSTALS-Kyber

Конкурс NIST. Signature

Решетки

- CRYSTALS-Dilithium

НО:

- используются различные параметры q, n, k, l и χ для одного уровня стойкости;
- в схеме подписи Dilithium дополнительно используются механизмы сжатия открытого ключа.

КРИПТОПРО

Подпись на ключе KEM

Открытые направления исследований:

- построение постквантовых схемы подписи и схемы KEM с одинаковым алгоритмом генерации ключевой пары;
- исследование безопасности одновременного использования одной ключевой пары для подписи и для KEM.

Зашифрованный сертификат

- Основная идея: без знания закрытого ключа клиент не расшифрует сертификат
- Способ упоминается в RFC 4210 [CMP05]
- Эксплуатационные недостатки:
  - УЦ не должен публиковать сертификат, пока не будет уверен, что он расшифрован (без второго сообщения от клиента, это невозможно)
- Криптографические недостатки – кросс-протокольные атаки:
  - нарушитель взял открытый ключ из прикладной системы, где аутентификация осуществляется путем предъявления результата расшифрования
  - после выдачи УЦ зашифрованного сертификата нарушитель получает его через штатный функционал прикладной системы

Расширенный интерфейс KEM

- Стандартный интерфейс схемы KEM:
  - KEM.KeyGen() → (pk,sk)
  - KEM.Encaps(pk) → (c,K)
  - KEM.Decaps(sk,c) → K или ⊥
- Новый подход предложен в 2022 году в работе «Proof-of-Possession for KEM Certificates using Verifiable Generation» [GHLOSZ22]
- Расширение интерфейса KEM:
  - Вместо KeyGen() теперь KGP(attr) → (pk,sk,π),

    где π – док-во владения sk «с привязкой» к строке атрибутов attr
- Может рассматриваться, как частный случай совместимых схем подписи и KEM, но с одним запросом на подпись, причем в момент генерации ключа

КРИПТОПРО

Выводы

- Оффлайн-запрос на сертификат (схема запрос-ответ):
  - Использование ключа KEM для подписи запроса
    - Необходимо разработать безопасно совместимые схемы KEM и подписи
  - Зашифрованный сертификат
    - Проблемы эксплуатационного и криптографического характера
  - Генерация ключа с доказательством (Verifiable Generation)
    - Новый подход, необходимо учесть при разработке KEM
- Онлайн-запрос на сертификат (протокол с 3+ пересылками)
  - Доказательство с помощью расшифрования: протоколы из [CMP05]
    - Существенное усложнение процедуры выпуска сертификата

КРИПТОПРО

Спасибо за внимание!

КРИПТОПРО

Ссылки

[MQV95] Menezes A.J., Qu M., Vanstone S.A. «Some new key agreement protocols providing implicit authentication». Workshop on Selected Areas in Cryptography (SAC'95), pp. 22--32, 1995.

[ANL03] Asokan N., Niemi V., Laitinen P. «On the usefulness of proof-of-possession». 2nd Annual PKI Research Workshop – Pre-Proceedings, 2003.

[CMP05] RFC 4210 «Internet X.509 Public Key Infrastructure Certificate Management Protocol (CMP)». Adams C., Farrell S., Kause T., Mononen T. 2005.

[GHLOSZ22] Guneysu T., Hodges P., Land G., Ounsworth M., Stebila D., Zaverucha G. «**Proof-of-possession for KEM certificates using verifiable generation**», Cryptology ePrint Archive, Paper 2022/703.

Случай постквантового KEM

Конкурс NIST. KEM

Решетки

- CRYSTALS-Kyber
- Saber
- Frodo

Коды

- Classic McEliece
- BIKE
- HQC

Какие схемы подписи могут использоваться для подписания запросов на сертификат?

Финалисты конкурса

Альтернативные схемы

КРИПТОПРО