Создание и стандартизация постквантовых криптографических механизмов

Антон Гуселев и *Александр Бондаренко*

Академия криптографии Российской Федерации

– PKI-Форум Россия 2022 –

Квантовая угроза: пора ли начинать бояться?

- Предложены эффективные методы решения задач, лежащих в основе стойкости схем цифровой подписи и протоколов распределения ключа, с использованием квантового компьютера *(1997 год, П. Шор)*
- Активно развиваются методы построения квантовых компьютеров, подходящих для «практического» применения

$\Rightarrow$ требуется проведение перспективных исследований

Однако нельзя забывать, что

остаются и другие «безопасные» методы обеспечения информационной безопасности, в моделях с квантовыми вычислителями:

- ✓ симметричная криптография $\Rightarrow$ предварительное распределение ключей

  (Для анализа предложены алгоритмы Гровера и Сайона, однако увеличение длины ключа позволит решить проблему)

Квантовая угроза: пора ли начинать бояться?

- Предложены эффективные методы решения задач, лежащих в основе стойкости схем цифровой подписи и протоколов распределения ключа, с использованием квантового компьютера *(1997 год, П. Шор)*
- Активно развиваются методы построения квантовых компьютеров, подходящих для «практического» применения

$\Rightarrow$ требуется проведение перспективных исследований

Однако нельзя забывать, что

остаются и другие «безопасные» методы обеспечения информационной безопасности, в моделях с квантовыми вычислителями:

✓ симметричная криптография $\Rightarrow$ предварительное распределение ключей

(Для анализа предложены алгоритмы Гровера и Сайона, однако увеличение длины ключа позволит решить проблему)

Квантовая угроза: пора ли начинать бояться?

- Предложены эффективные методы решения задач, лежащих в основе стойкости схем цифровой подписи и протоколов распределения ключа, с использованием квантового компьютера *(1997 год, П. Шор)*
- Активно развиваются методы построения квантовых компьютеров, подходящих для «практического» применения

$\Rightarrow$ ⚠ требуется проведение перспективных исследований

Однако нельзя забывать, что

остаются и другие «безопасные» методы обеспечения информационной безопасности, в моделях с квантовыми вычислителями:

✓ симметричная криптография $\Rightarrow$ предварительное распределение ключей
(Для анализа предложены алгоритмы Гровера и Сайона, однако увеличение длины ключа позволит решить проблему)

Что же будет с асимметричной криптографией?

Задача:

создать постквантовый криптографический механизм – механизм, который будет безопасным по отношению к

- методам анализа основе квантового компьютера
- классическим методам анализа

Как создать постквантовый криптографический механизм?

Использовать при обосновании стойкости задачи «неразрешимые» с использованием

- квантового компьютера
- классических методов

Что же будет с асимметричной криптографией?

Задача:

создать постквантовый криптографический механизм – механизм, который будет безопасным по отношению к

- методам анализа основе квантового компьютера
- классическим методам анализа

Как создать постквантовый криптографический механизм?

Использовать при обосновании стойкости задачи «неразрешимые» с использованием

- квантового компьютера
- классических методов

Безопасная асимметрия

Возможно использовать *другие* подходы:

- теория кодирования
- теория многочленов от многих переменных
- теория решеток
- теория изогений эллиптических кривых

Все постквантовое: хорошо забытое «классическое»

В основе (почти) всех постквантовых механизмов лежат идеи, предложенные на заре становления криптографии, однако, уступившие методам на основе дискретного логарифмирования и факторизации

... или «безопасную» симметричную криптографию

- функции хэширования

Безопасная асимметрия

Возможно использовать *другие* подходы:

- теория кодирования ($\sim$ 1978 год)
- теория многочленов от многих переменных ($\sim$ 1988 год)
- теория решеток ($\sim$ 1996 (?) год)
- теория изогений эллиптических кривых ($\sim$ 2014 год)

Все постквантовое: хорошо забытое «классическое»

В основе (почти) всех постквантовых механизмов лежат идеи, предложенные на заре становления криптографии, однако, уступившие методам на основе дискретного логарифмирования и факторизации

... или «безопасную» симметричную криптографию

- функции хэширования

Безопасная асимметрия

Возможно использовать *другие* подходы:

- теория кодирования ($\sim$ 1978 год)
- теория многочленов от многих переменных ($\sim$ 1988 год)
- теория решеток ($\sim$ 1996 (?) год)
- теория изогений эллиптических кривых ($\sim$ 2014 год)

Все постквантовое: хорошо забытое «классическое»

В основе (почти) всех постквантовых механизмов лежат идеи, предложенные на заре становления криптографии, однако, уступившие методам на основе дискретного логарифмирования и факторизации

... или «безопасную» симметричную криптографию

- функции хэширования

Перспективные исследования

- Конкурс NIST PQ

  ноябрь 2017 $\xrightarrow[\text{подано}]{82\text{ заявки}}$ декабрь 2017 $\xrightarrow[\text{1 этап}]{69\text{ заявок}}$ январь 2019 $\xrightarrow[\text{2 этап}]{26\text{ механизмов}}$ июль 2020 $\xrightarrow[\text{3 этап}]{15\text{ механизмов}}$ июль 2022 $\xrightarrow[4\text{ доп. рассмотрение}]{4\text{ стандартизация}}$

- Horizon 2020
- Исследования в Академии криптографии Российской Федерации

Перспективные исследования

- Конкурс NIST PQ

ноябрь 2017 $\xrightarrow[\text{подано}]{82 \text{ заявки}}$ декабрь 2017 $\xrightarrow[1 \text{ этап}]{69 \text{ заявок}}$ январь 2019 $\xrightarrow[2 \text{ этап}]{26 \text{ механизмов}}$ июль 2020 $\xrightarrow[3 \text{ этап}]{15 \text{ механизмов}}$ июль 2022 $\xrightarrow[4 \text{ доп. рассмотрение}]{4 \text{ стандартизация}}$

- Horizon 2020
- Исследования в Академии криптографии Российской Федерации

Стандартизация

- Институт инженеров электротехники и электроники (IEEE)
  - ⋆ P1363.1-2008 *(2008 год, схема шифрования NTRU**)* – *выведен из действия в 2019 году*
- Инженерный Совет Интернета (IETF)
  - ⋆ RFC 8391 *(2018 год, схема цифровой подписи XMSS*)*
  - ⋆ RFC 8554 *(2019 год, схема цифровой подписи LMS*)*
- Международная организация по стандартизации и Международная электротехническая комиссия (ISO/IEC)
  - ⋆ проект ISO/IEC 14888-4 *(схемы цифровой подписи XMSS* и LMS*)*
- Национальный (США) институт стандартов и технологи (NIST)
  - ⋆ планы по стандартизации победителей (третьего этапа) конкурса:
    - *1 механизм инкапсуляции ключа (CRYSTALS-Kyber**)*
    - *3 схемы цифровой подписи (CRYSTALS-Dilithium**, FALCON**, SPHINCS+*)*
- ТК 026 (РГ «Постквантовые криптографические механизмы»)
  - ⋆ проект схемы цифровой подписи «Шиповник»***

*на основе хэш-функций **на основе теории решеток ***на основе теории решеток

Стандартизация

- Институт инженеров электротехники и электроники (IEEE)
  - ⋆ P1363.1-2008 *(2008 год, схема шифрования NTRU**)* – *выведен из действия в 2019 году*
- Инженерный Совет Интернета (IETF)
  - ⋆ RFC 8391 *(2018 год, схема цифровой подписи XMSS*)*
  - ⋆ RFC 8554 *(2019 год, схема цифровой подписи LMS*)*
- Международная организация по стандартизации и Международная электротехническая комиссия (ISO/IEC)
  - ⋆ проект ISO/IEC 14888-4 *(схемы цифровой подписи XMSS* и LMS*)*
- Национальный (США) институт стандартов и технологи (NIST)
  - ⋆ планы по стандартизации победителей (третьего этапа) конкурса:
    *1 механизм инкапсуляции ключа (CRYSTALS-Kyber**)*
    *3 схемы цифровой подписи (CRYSTALS-Dilithium**, FALCON**, SPHINCS+*)*
- ТК 026 (РГ «Постквантовые криптографические механизмы»)
  - ⋆ проект схемы цифровой подписи «Шиповник»***

*на основе хэш-функций **на основе теории решеток ***на основе теории решеток

Стандартизация

- Институт инженеров электротехники и электроники (IEEE)
  - ⋆ P1363.1-2008 *(2008 год, схема шифрования NTRU**)* – *выведен из действия в 2019 году*
- Инженерный Совет Интернета (IETF)
  - ⋆ RFC 8391 *(2018 год, схема цифровой подписи XMSS*)*
  - ⋆ RFC 8554 *(2019 год, схема цифровой подписи LMS*)*
- Международная организация по стандартизации и Международная электротехническая комиссия (ISO/IEC)
  - ⋆ проект ISO/IEC 14888-4 *(схемы цифровой подписи XMSS* и LMS*)*
- Национальный (США) институт стандартов и технологи (NIST)
  - ⋆ планы по стандартизации победителей (третьего этапа) конкурса:
    - *1 механизм инкапсуляции ключа (CRYSTALS-Kyber**)*
    - *3 схемы цифровой подписи (CRYSTALS-Dilithium**, FALCON**, SPHINCS+*)*
- ТК 026 (РГ «Постквантовые криптографические механизмы»)
  - ⋆ проект схемы цифровой подписи «Шиповник»***

*на основе хэш-функций **на основе теории решеток ***на основе теории решеток

Стандартизация

- Институт инженеров электротехники и электроники (IEEE)
  - ⋆ P1363.1-2008 *(2008 год, схема шифрования NTRU**)* – *выведен из действия в 2019 году*
- Инженерный Совет Интернета (IETF)
  - ⋆ RFC 8391 *(2018 год, схема цифровой подписи XMSS*)*
  - ⋆ RFC 8554 *(2019 год, схема цифровой подписи LMS*)*
- Международная организация по стандартизации и Международная электротехническая комиссия (ISO/IEC)
  - ⋆ проект ISO/IEC 14888-4 *(схемы цифровой подписи XMSS* и LMS*)*
- Национальный (США) институт стандартов и технологи (NIST)
  - ⋆ планы по стандартизации победителей (третьего этапа) конкурса:
    *1 механизм инкапсуляции ключа (CRYSTALS-Kyber**)*
    *3 схемы цифровой подписи (CRYSTALS-Dilithium**, FALCON**, SPHINCS+*)*
- ТК 026 (РГ «Постквантовые криптографические механизмы»)
  - ⋆ проект схемы цифровой подписи «Шиповник»***

*на основе хэш-функций **на основе теории решеток ***на основе теории решеток

Стандартизация

- Институт инженеров электротехники и электроники (IEEE)
  - ⋆ P1363.1-2008 *(2008 год, схема шифрования NTRU**)* – *выведен из действия в 2019 году*
- Инженерный Совет Интернета (IETF)
  - ⋆ RFC 8391 *(2018 год, схема цифровой подписи XMSS*)*
  - ⋆ RFC 8554 *(2019 год, схема цифровой подписи LMS*)*
- Международная организация по стандартизации и Международная электротехническая комиссия (ISO/IEC)
  - ⋆ проект ISO/IEC 14888-4 *(схемы цифровой подписи XMSS* и LMS*)*
- Национальный (США) институт стандартов и технологи (NIST)
  - ⋆ планы по стандартизации победителей (третьего этапа) конкурса:
    *1 механизм инкапсуляции ключа (CRYSTALS-Kyber**)*
    *3 схемы цифровой подписи (CRYSTALS-Dilithium**, FALCON**, SPHINCS+*)*
- ТК 026 (РГ «Постквантовые криптографические механизмы»)
  - ⋆ проект схемы цифровой подписи «Шиповник»***

*на основе хэш-функций **на основе теории решеток ***на основе теории решеток

Выводы

1. Ведутся активные исследования по созданию эффективных и безопасных постквантовых криптографических механизмов
2. Однако, окончательного решения о наиболее подходящем синтезном подходе еще не принято
3. Предпринимаются первые попытки стандартизации механизмов, на основе «новых» принципов
4. !!! Создание квантового компьютера не приведет к повсеместной «небезопасности»

Применяемые в настоящее время механизмы в состоянии обеспечить требуемый уровень безопасности

Выводы

1. Ведутся активные исследования по созданию эффективных и безопасных постквантовых криптографических механизмов
2. Однако, окончательного решения о наиболее подходящем синтезном подходе еще не принято
3. Предпринимаются первые попытки стандартизации механизмов, на основе «новых» принципов
4. !!! Создание квантового компьютера не приведет к повсеместной «небезопасности»

Применяемые в настоящее время механизмы в состоянии обеспечить требуемый уровень безопасности