КРИПТОНИТ

# О рисках для кибербезопасности
## в связи с созданием квантового компьютера

**Иван Чижов**
Заместитель по науке руководителя
лаборатории криптографии
НПК «Криптонит»,
к.ф.-м.н.

КРИПТОНИТ

# Что такое квантовый компьютер?

Идея принадлежит Ю. И. Манину (1980)

- Квантовая суперпозиция
- Квантовая запутанность
- Квантовый бит, кубит

# Мат. модель квантовых вычислений

КРИПТОНИТ

| | Классические вычисление | Квантовые вычисления |
|---|---|---|
| Единица информации | Бит | Кубит |
| Состояние | 0,1 | $\{(\alpha,\beta)\mid \lvert\alpha\rvert^2+\lvert\beta\rvert^2=1\}$<br>$(1,0)\to\lvert 0\rangle$<br>$(0,1)\to\lvert 1\rangle$<br>$(\alpha,\beta)\to\alpha\lvert 0\rangle+\beta\lvert 1\rangle$ |
| Пример состояния | 0,1 | Есть смешанные состояния<br>$\frac{1}{\sqrt{2}}\lvert 0\rangle+\frac{1}{\sqrt{2}}\lvert 1\rangle$ |
| Измерение состояния | $x\overset{!}{\to}x$ | $\alpha\lvert 0\rangle+\beta\lvert 1\rangle\overset{!}{\to}\begin{cases}\lvert 0\rangle & \text{с вероятностью } \lvert\alpha\rvert^2\\ \lvert 1\rangle & \text{с вероятностью } \lvert\beta\rvert^2\end{cases}$ |

# Задача, которую «хорошо» умеет решать квантовый компьютер

КРИПТОНИТ

$$N = p \cdot q \Rightarrow (p, q)$$

$$15\ 481 \rightarrow (p, q)?$$

# Задача, которую «хорошо» умеет решать квантовый компьютер

КРИПТОНИТ

$$N = p \cdot q \Rightarrow (p, q)$$

$$15\,481 \rightarrow (p, q)?$$

1024 бита (≈ 300 десятичных знаков)
за 8 часов, имея ≈20 млн. физических кубитов

КРИПТОНИТ

# Последствия для криптографии

Криптография с секретным ключом (симметричная криптография): блочные, поточные шифры и хеш-функции

Взлом сводится к решению алгебраического уравнения $f(k)=0$, которое не имеет хорошей структуры

Алгоритм Лова Гровера (1996), квантовый поиск, выигрыш $O(\sqrt{N})$ по сравнению с классическим компьютером $O(N)$.

КРИПТОНИТ

# Последствия для криптографии/2

Криптография с секретным ключом (симметричная криптография)

Блочные шифры: **ГОСТ 34.12-2018 (Магма, Кузнечик), AES**

Хеш-функции: **ГОСТ 34.11-2018 (Стрибог), SHA-***

Просто увеличиваем длину ключа в два раза: **256 → 512**

КРИПТОНИТ

# Последствия для криптографии/3

Криптография с открытым ключом (асимметричная криптография): протоколы распределения ключей и электронная подпись.

Алгоритм Шора (1997), $O(\log^c N)$
по сравнению с классическим компьютером
$O(\exp(c_1 \log^{c_2} N \log^{1-c_2} \log N))$.

# Последствия для криптографии/4

Криптография с открытым ключом (асимметричная криптография)

Распределение ключей (DH, ECDH, согласование ключей VKO ГОСТ 34.11-*), электронная подпись (RSA, ECDSA, ГОСТ 34.10-2018)

Используется в TLS ({http, ftp, smtp, pop,…}s), IPSec (VPN), WireGuard VPN, Outline VPN, SSH (RSA или ECDH ключи) и т. д.

# Последствия для нашей жизни

КРИПТОНИТ

*Пострадает защита коммуникаций в условиях, когда заранее не известен состав «собеседников»:*

- Защита сайтов (https): сертификаты, шифрование данных форм и прочее.
- Электронный нотариат: нет электронной подписи
- Банковские приложения: **online-оплата**, / технология оплаты картой должна быть переработана /
- Виртуальные частные сети: возможно только на PRESHARED-KEY

# Последствия для нашей жизни/2

КРИПТОНИТ

*Коммуникации с заранее известным составом «собеседников» останутся, но будут не так удобны:*

- Телефон (GSM, 3G, 4G, 5G): шифрование с условием предварительного распределения ключей)
- Оплата в метро картами типа «Тройка»
- и т.п.

КРИПТОНИТ

# Что не умеет (пока?) квантовый компьютер

1. Взламывать криптосистемы с секретным ключом
   - Криптография на основе хеш-функций
2. Решать алгебраические квадратные уравнения, не имеющие простой структуры
   - Криптография на основе систем квадратичных полиномов от многих переменных над конечным полем
3. Решать линейные уравнения с ограничением на норму решения
   - Криптография на алгебраических решётках
   - Криптография на кодах, исправляющих ошибки

КРИПТОНИТ

# Что же делать?

В 2016 году Национальный институт стандартов и технологий США (NIST USA) объявил конкурс на создание новых стандартов постквантовой **электронной подписи** и постквантового **механизма инкапсуляции ключа**.

В 2019 году создана рабочая группа «Постквантовые криптографические механизмы» в ТК 26 РФ. Работы ведутся по разработке постквантовой **электронной подписи** и постквантового **механизма инкапсуляции ключа**.

КРИПТОНИТ

# Что есть уже сейчас?


Проект методических рекомендаций
по стандартизации схемы электронной подписи
**«Шиповник»** на кодах, исправляющих ошибки
(2-я стадия рецензирования)


Проект методических рекомендаций
по стандартизации схемы электронной
подписи **«Гиперикум»** на хеш-функциях
(1-я стадия рецензирования)

КРИПТОНИТ

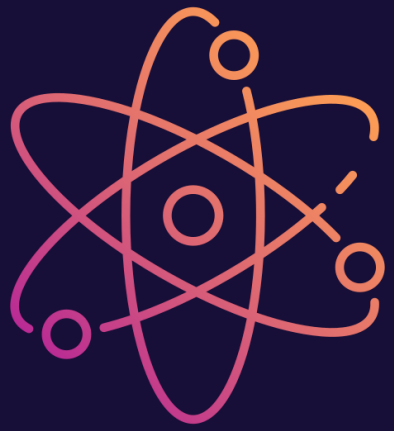
# Что планируется?

1. Проект методических рекомендаций по стандартизации схемы инкапсуляции ключа на основе кодов, исправляющих ошибки.

2. ГОСТы на постквантовые криптографические механизмы.

КРИПТОНИТ

# Не всё так гладко, как хотелось бы…



- Недостаточно исследована стойкость многих постквантовых криптографических механизмов (пример: изогении эллиптических кривых)
- Как правило потребительские характеристики (размер ключа, размер подписи, скорость работы и т.п.) постквантовых механизмов сильно хуже классических
- Требуется доработка прикладных протоколов для использования криптографических механизмов (например, рукопожатие в TLS)
- Сложности реализации (размер подписи в Шиповнике **92Кб**, размер IP-пакета 64 Кб)

КРИПТОНИТ

# Готов ответить на вопросы

**Иван Чижов**
Заместитель по науке руководителя лаборатории криптографии, НПК «Криптонит»,
к.ф.-м.н.

Узнать подробнее
про научные исследования
компании «Криптонит»
в области криптографии:

kryptonite.ru