Страх и ненависть в постквантовой криптографии

Что мы слышим о «квантовой угрозе»?

- Неотвратима
- Катастрофична
- Непрогнозируема

- Требуется разработка и внедрение постквантовых механизмов

Карл Брюллов. Последний день Помпеи

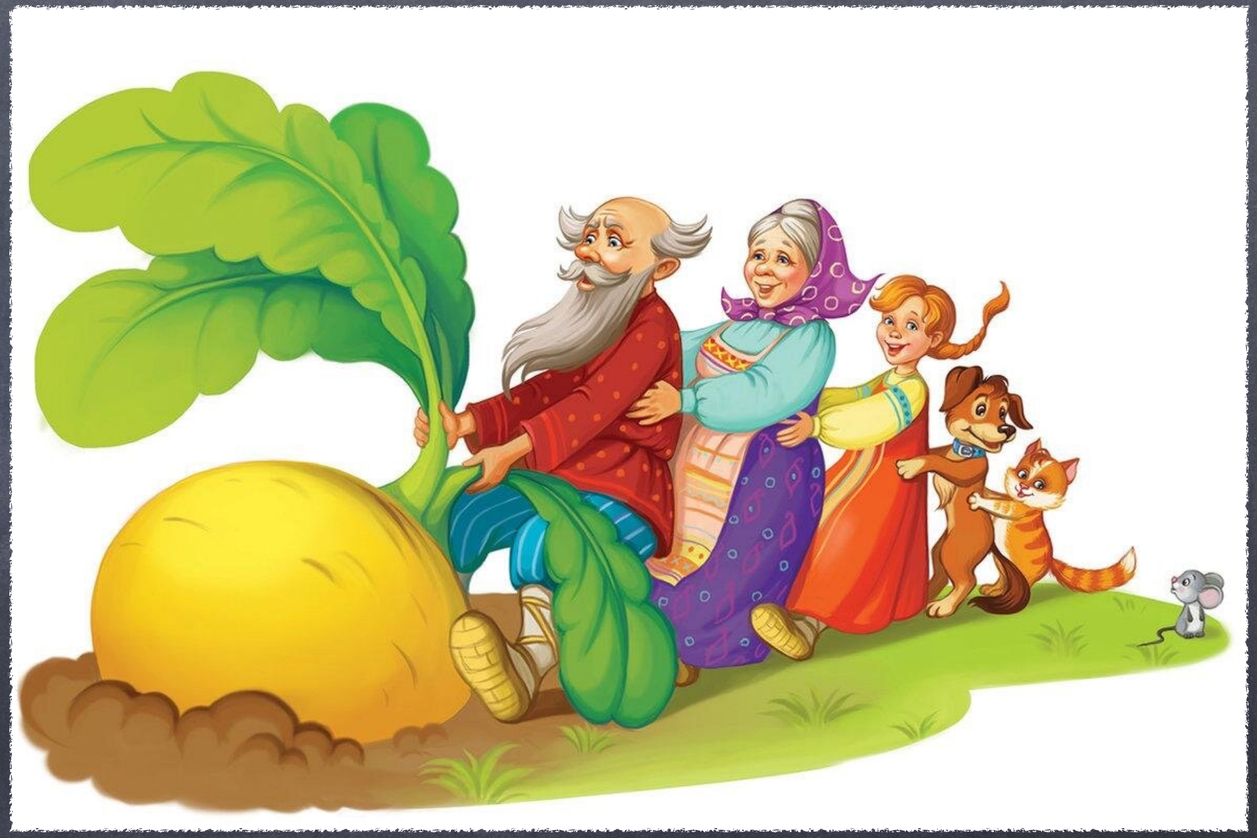
УКЭП

Что требуется от обоснования безопасности криптографического механизма?

- Убедительность
  - покрывать возможные варианты угроз
- Проверяемость
  - одинаково интерпретируемо для всех

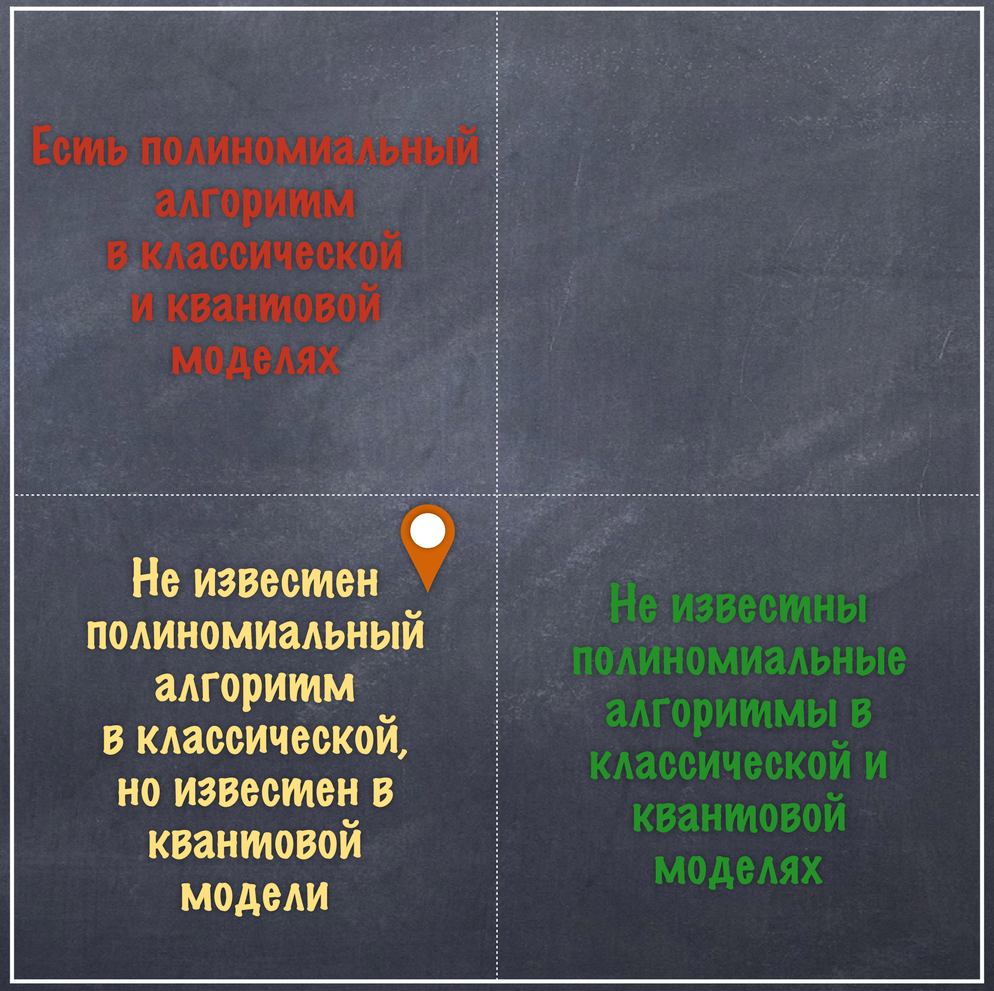
Почему асимметричные механизмы используются сейчас?

- Вычислительно трудные задачи
  - P=?=NP
  - не известен полиномиальный алгоритм решения - хорошая основа для механизма (факторизация, логарифмирование)
  - есть алгоритм решения для частных случаев - плохая основа для механизма (укладка рюкзака, задача RSA)
- Больше исследований - больше уверенность



Классическая и квантовая модели вычислений

- Модель определяет допустимый набор операций
  - классическая
  - квантовая адиабатическая
  - квантовая гейтовая
  - комбинированная



Варианты исследуемых вычислительно трудных задач

- Алгебраической теории кодирования
- Теории целочисленных решеток
- Теории решения систем нелинейных уравнений
- Теории однонаправленных функций
- ...

GSD, SD, CF, PE, CD

Варианты исследуемых вычислительно трудных задач

- Алгебраической теории кодирования
- Теории целочисленных решеток
- Теории решения систем нелинейных уравнений
- Теории однонаправленных функций
- ...

GSD, SD, CF, PE, CD

GapSVP, SVP, SIVP, CVP, GapCVP, uSVP, BDD

Варианты исследуемых вычислительно трудных задач

- Алгебраической теории кодирования
- Теории целочисленных решеток
- Теории решения систем нелинейных уравнений
- Теории однонаправленных функций
- ....

GSD, SD, CF, PE, CD

GapSVP, SVP, SIVP, CVP, GapCVP, uSVP, BDD

MQ

Варианты исследуемых вычислительно сложных задач

- Алгебраической теории кодирования
- Теории целочисленных решеток
- Теории решения систем нелинейных уравнений
- Теории однонаправленных функций
- ...

GSD, SD, CF, PE, CD

GapSVP, SVP, SIVP, CVP, GapCVP, uSVP, BDD

MQ

CR, PR

...

Конкурс NIST по выбору постквантовых механизмов

У нас было 27 схем на решетках, 22 — на кодах, две подписи на хэшах, 11 различных схем на многочленах, одна схема на изогениях и некоторое количество схем на разных экзотических вычислительно трудных задачах. Не то, чтобы это был необходимый запас для стандартизации, но раз уж начал проводить конкурс, то сложно остановиться. Единсивенное, что вызывало опасение — это постквантовая подпись RSA. В мире нет никого более беспомощного, чем разработчик, пытающийся запихнуть терабайтный открытый ключ в заголовок сообщения TLS 1.3

Конкурс NIST по выбору постквантовых механизмов

У нас было 27 схем на решетках, 22 — на кодах, две подписи на хэшах, 11 различных схем на многочленах, одна схема на изогениях и некоторое количество схем на разных экзотических вычислительно трудных задачах. Не то, чтобы это был необходимый запас для стандартизации, но раз уж начал проводить конкурс, то сложно остановится. Единсивенное, что вызывало опасение — это постквантовая подпись RSA. Нет ничего более беспомощного, чем разработчик, пытающийся запихнуть терабайтный открытый ключ в заголовок TLS 1.3

- Очень большое число базовых вычислительно трудных задач

Конкурс NIST по выбору постквантовых механизмов

У нас было 27 схем на решетках, 22 — на кодах, две подписи на хэшах, 11 различных схем на многочленах, одна схема на изогениях и некоторое количество схем на разных экзотических вычислительно трудных задачах. Не то, чтобы это был необходимый запас для стандартизации, но раз уж начал проводить конкурс, то сложно остановится. Единсивенное, что вызывало опасение — это постквантовая подпись RSA. Нет ничего более беспомощного, чем разработчик, пытающийся запихнуть терабайтный открытый ключ в заголовок TLS 1.3

- Откровенно слабые схемы

HK17 — схема на кватернионах (2017 г.)

Нестойкость таких схем показана М.М. Глуховым в 2012 г. (CTCrypt 2012)

Конкурс NIST по выбору постквантовых механизмов

У нас было 27 схем на решетках, 22 — на кодах, две подписи на хэшах, 11 различных схем на многочленах, одна схема на изогениях и некоторое количество схем на разных экзотических вычислительно трудных задачах. Не то, чтобы это был необходимый запас для стандартизации, но раз уж начал проводить конкурс, то сложно остановится. Единсивенное, что вызывало опасение — это постквантовая подпись RSA. Нет ничего более беспомощного, чем разработчик, пытающийся запихнуть терабайтный открытый ключ в заголовок TLS 1.3

- Откровенно слабые схемы: 14 схем взломаны на 1 раунде
- Взломаны финалисты
  - 3 раунда (Rainbow) и
  - последнего 4 раунда (SIKE)

На основе результата Е. Кани 1997 г.

Конкурс NIST по выбору постквантовых механизмов

У нас было 27 схем на решетках, 22 — на кодах, две подписи на хэшах, 11 различных схем на многочленах, одна схема на изогениях и некоторое количество схем на разных экзотических вычислительно трудных задачах. Не то, чтобы это был необходимый запас для стандартизации, но раз уж начал проводить конкурс, то сложно остановится. Единсивенное, что вызывало опасение — это постквантовая подпись RSA. Нет ничего более беспомощного, чем разработчик, пытающийся запихнуть терабайтный открытый ключ в заголовок TLS 1.3

- Откровенно слабые схемы: 14 схем взломаны на 1 раунде
- Взломаны финалисты
  - 3 раунда (Rainbow) и
  - последнего 4 раунда (SIKE)
- Атаки приводили к практической нестойкости схем в классической модели

Конкурс NIST по ~~выбору постквантовых механизмов~~ оценке стойкости механизмов на новых вычислительно трудных задачах в классической модели

- Для некоторых схем было доказано формальное сведение задачи нарушения стойкости к задаче решения вычислительно трудной задаче в квантовой модели
- Криптоанализ проводился в основном в классической модели

Улучшение алгоритмов решения вычислительно трудных задач (и снова о репке)

- Алгебраической теории кодирования — 2018 г.
- Теории решеток — 2015 г.
- Теории решения систем нелинейных уравнений — 2022 г.
- Факторизации больших целых чисел — 1993 г.
- Логарифмирования в группе точек эллиптической кривой — 1994 г.

В результате...

Efforts to standardize new "post-quantum" public-key cryptographic algorithms are underway, and will result in algorithm recommendations within the next few years. Future adoption of these algorithms is likely inevitable even if a quantum computer capable of Shor's algorithm is never built. These new algorithms will have a very different mathematical structure from the existing common public-key cryptographic algorithms, opening the door to decades of new research in cryptanalysis.

The State of the Art in Integer Factoring and Breaking Public-Key Cryptography

Fabrice Boudot, Pierrick Gaudry, Aurore Guillevic, Nadia Heninger, Emmanuel Thomé, Paul Zimmermann

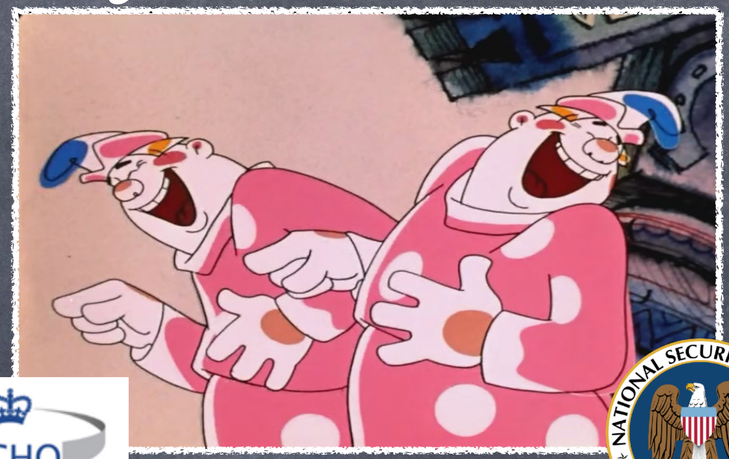
Отношение в мире

Bundesamt für Sicherheit in der Informationstechnik

I E T F

ANSSI

- Не устоявшаяся область исследований
- Консервативный подход: постквантовые схемы на хэшах наиболее исследованы
- Целесообразно гибридное внедрение: постквантовая схема + классическая



GCHQ

NATIONAL SECURITY AGENCY

UNITED STATES OF AMERICA

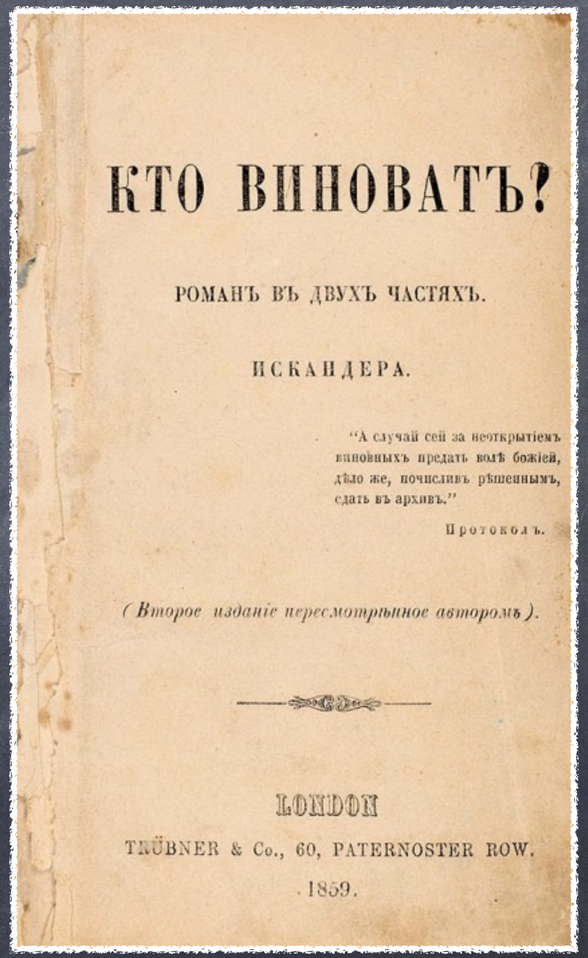
- Для общего использования — схемы на решетках
- Схемы на хэшах — для частных применений (обновления ПО)
- Сразу переход на постквантовые схемы

Работы в России (ТК 26)

- Подписи
  - Шиповник (коды)
  - Гиперикум (функции хэширования)
  - Крыжовник (решетки)
- Инкапсуляция ключа
  - Кодиеум (коды)

Работы в России (ТК 26)

- Те же вопросы:
  - Вычислительная трудность базовой задачи
  - Стойкость в классической модели
  - Стойкость в квантовой модели



КТО ВИНОВАТЪ?

РОМАНЪ ВЪ ДВУХЪ ЧАСТЯХЪ.

ИСКАНДЕРА.

"А случай сей за неоткрытіемъ виновныхъ предать волѣ божіей, дѣло же, почисливъ рѣшеннымъ, сдать въ архивъ."

Протоколъ.

(Второе изданіе пересмотрѣнное авторомъ).

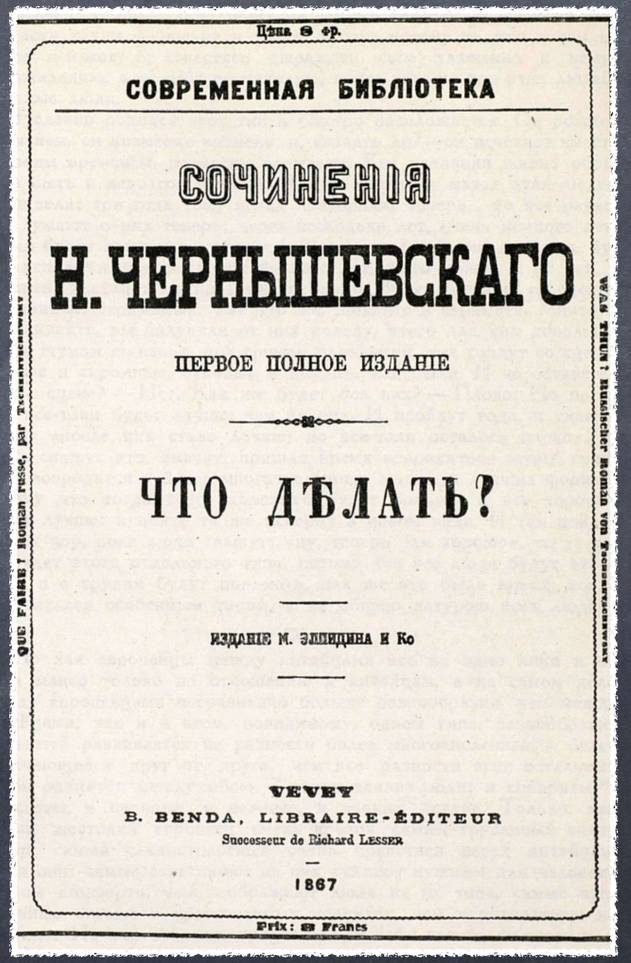
LONDON

TRÜBNER & Co., 60, PATERNOSTER ROW.

1859.

Работы в России (ТК 26)

- Определить цель:
  - какими свойствами должен обладать перспективный механизм
  - чем он отличается от существующих
- Определить задачи:
  - исследования математических проблем
  - выбора и обоснования принципов синтеза
  - выбора и обоснования параметров
  - развития методов анализа в классической и квантовой моделях


Цѣна 6 фр.

СОВРЕМЕННАЯ БИБЛІОТЕКА

СОЧИНЕНІЯ

Н. ЧЕРНЫШЕВСКАГО

ПЕРВОЕ ПОЛНОЕ ИЗДАНІЕ

ЧТО ДѢЛАТЬ?

ИЗДАНІЕ М. ЭЛПИДИНА И Ко

VEVEY

B. BENDA, LIBRAIRE-ÉDITEUR

Successeur de Richard Lesser

1867

Prix: 6 Francs

Работы в России (ТК 26)

- Определить цель:
  - какими свойствами должен обладать перспективный механизм
  - чем он отличается от существующих
- Определить задачи:
  - исследования математических проблем
  - выбора и обоснования принципов синтеза
  - выбора и обоснования параметров
  - развития методов анализа в классической и квантовой моделях

- Получить компетенции:
  - знать
  - уметь
  - владеть

Спасибо за внимание