Ежегодная международная научно-практическая конференция
«РусКрипто’2020»

Детектирование атак по времени на реализации криптографических алгоритмов

Набоков Денис, инженер по безопасности приложений,
Российский Квантовый Центр
МГТУ им. Н.Э. Баумана

Атаки по сторонним каналам

- Направлены на реализации криптосистем
- Атаки используют информацию о физических процессах в устройстве
- Типы: атаки по энергопотреблению, по времени, по электромагнитному излучению и т.д.

Атаки по времени

- Анализ времени выполнения алгоритма в зависимости от входных данных
- Классический пример – алгоритм быстрого возведения в степень
- В контексте RSA расшифрование – возведение в секретную степень d

```
function Power(value, pow: int): int
  int result = 1
  while (pow > 0)
    if pow mod 2 == 1
      result *= value
    value *= value
    pow /= 2;
  return result;
```

Атаки по времени

- Причины различия во времени выполнения в зависимости от входных данных:
  - Ветви кода с разным временем выполнения
  - Предсказатель переходов
  - Попадание в кэш и кэш-промахи
  - Время выполнения некоторых инструкций процессора может зависеть от операндов
- Программа потенциально уязвима к атакам по времени, если данные, которые вызывают различия во времени выполнения, являются секретными.

Детектирование атак по времени

- Анализ кода (на уровне исходного кода, компилятора или ассемблера)
- Непосредственный запуск программы со сбором времени выполнения и последующим его анализом

Детектирование на основе запуска программ

- Подготовительный этап – выделение двух множеств входных данных
- Этап сбора измерений – измерение времени выполнения
- Этап анализа измерений – применение статистического теста к двум множествам измерений

Подготовительный этап

- Fixed-vs-fixed: множество данных разбивается на две части в зависимости от какого-либо внутреннего значения
- Fixed-vs-random: первое множество – единственный фиксированный вход, второе – множество случайных файлов, то есть для каждого измерения подаётся новый случайный файл

Подготовительный этап

- Обычно используется fixed-vs-random, так как множество внутренних значений алгоритма может быть большим, а в этом подходе «покрываются» все из них
- Возможна ситуация, когда для одного фиксированного входа уязвимость не обнаруживается, но обнаруживается для другого. Поэтому проводят несколько тестов с различными фиксированными входами
- Фаззер – хороший источник для таких входов

Этап сбора измерений

- При измерении множества случайно чередуются
- Это позволяет уменьшить влияния шума среды

Этап анализа измерений

- К двум множествам измерений применяется статистический тест
- Нулевая гипотеза – две выборки произошли из одного и того же распределения, то есть множества неразличимы
- Задача: оценить вероятность принятия этой гипотезы
- Установим порог для этой вероятности (0.00001)
- Рассмотрим Welch’s t-test и тест Колмогорова-Смирнова

Welch’s t-test

- Тест выдаёт вероятность, что матожидаение двух выборок различается
- Широко применяется для анализа атак по сторонним каналам
- Статистика t распределена в соответствии с распределением Стьюдента
- Степень свободы $v \approx n_0 + n_1$, если $s_0 \approx s_1$ и $n_0 \approx n_1$

$$t = \frac{\mu_0 - \mu_1}{\sqrt{\frac{{s_0}^2}{n_0} + \frac{{s_1}^2}{n_1}}}$$

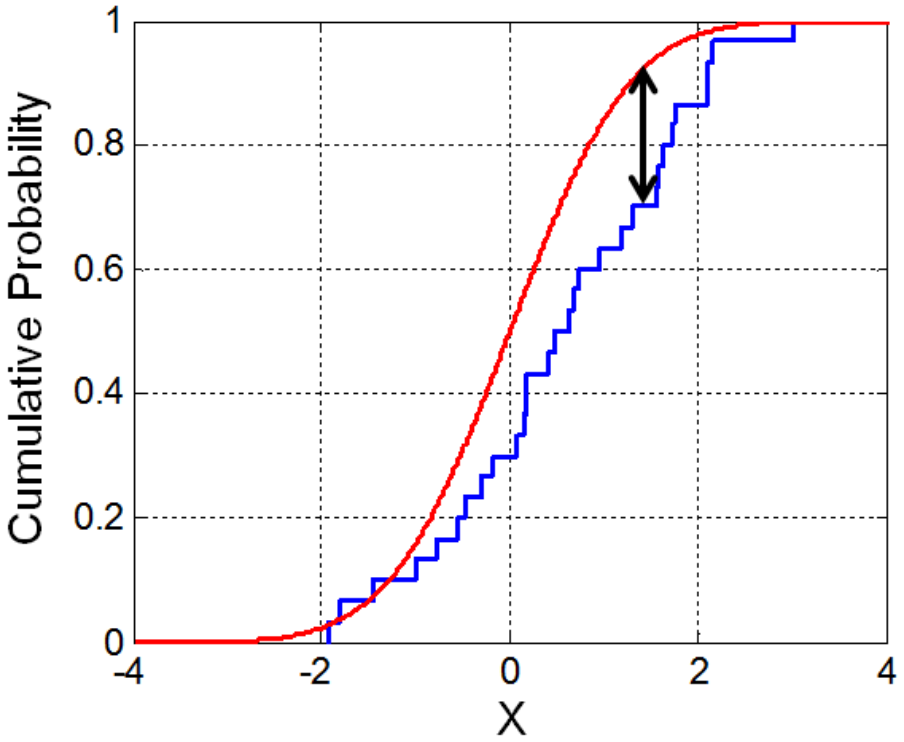
$$v = \frac{\left(\frac{{s_0}^2}{n_0} + \frac{{s_1}^2}{n_1}\right)^2}{\frac{\left(\frac{{s_0}^2}{n_0}\right)^2}{n_0 - 1} + \frac{\left(\frac{{s_1}^2}{n_1}\right)^2}{n_1 - 1}}$$

Welch’s t-test

- Результат теста можно оценить как $p = 2F(-|t|, v)$
- F – функция распределения Стьюдента
- Обычно используют порог для |t| > 4.5, при котором опровергают гипотезу
- $p = 2F(-4.5, v > 1000) < 0.00001$

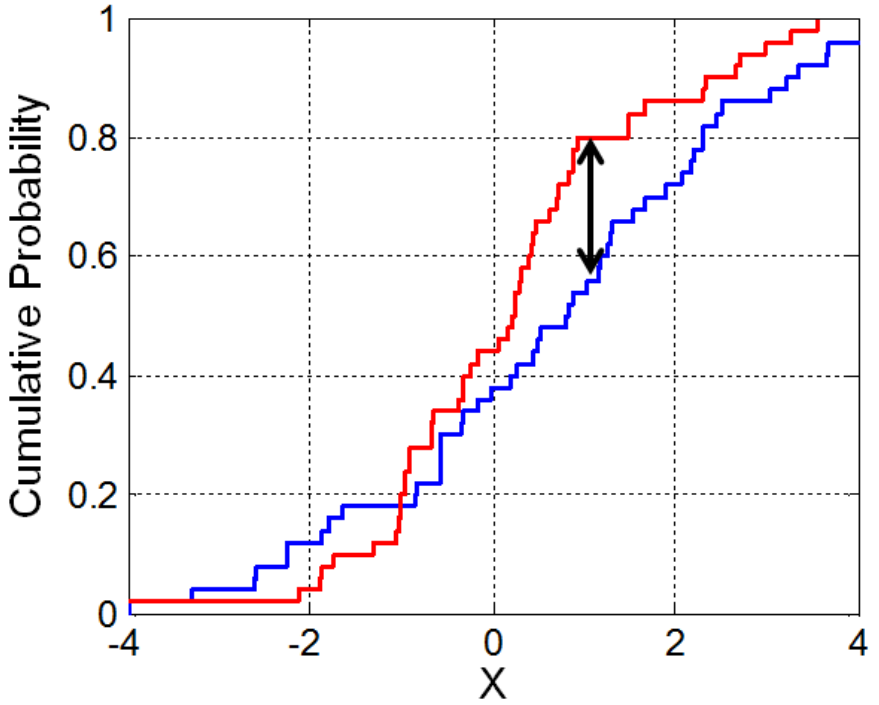
Тест Колмогорова-Смирнова

- В классическом случае (one-sample тест) определяет, что выборка произошла из теоретического распределения F
- Статистика $D_n = \sup_x |F_n(x) - F(x)|$
- Тест сравнивает сразу функции распределения, вместо каких-то определенных параметров (матожидание, дисперсия)



Тест Колмогорова-Смирнова

- Существует two-sample тест: определить, что две выборки произошли из одного **непрерывного** распределения
- Время выполнения (количество тактов процессора) – величина дискретная. В этом случае p зависит не только от статистики, но и от самих данных
- Нельзя установить порог для D_n, при превышении которого тест можно завершить



Тест Колмогорова-Смирнова

- Необходимо вычислять p для выборок. Эта задача нетривиальная
- Для приближенного вычисления взят подход из Dimitrova, D. S., Kaishev, V. K. and Tan, S. (2017). Computing the Kolmogorov-Smirnov Distribution when the Underlying cdf is Purely Discrete, Mixed or Continuous.

Практические результаты

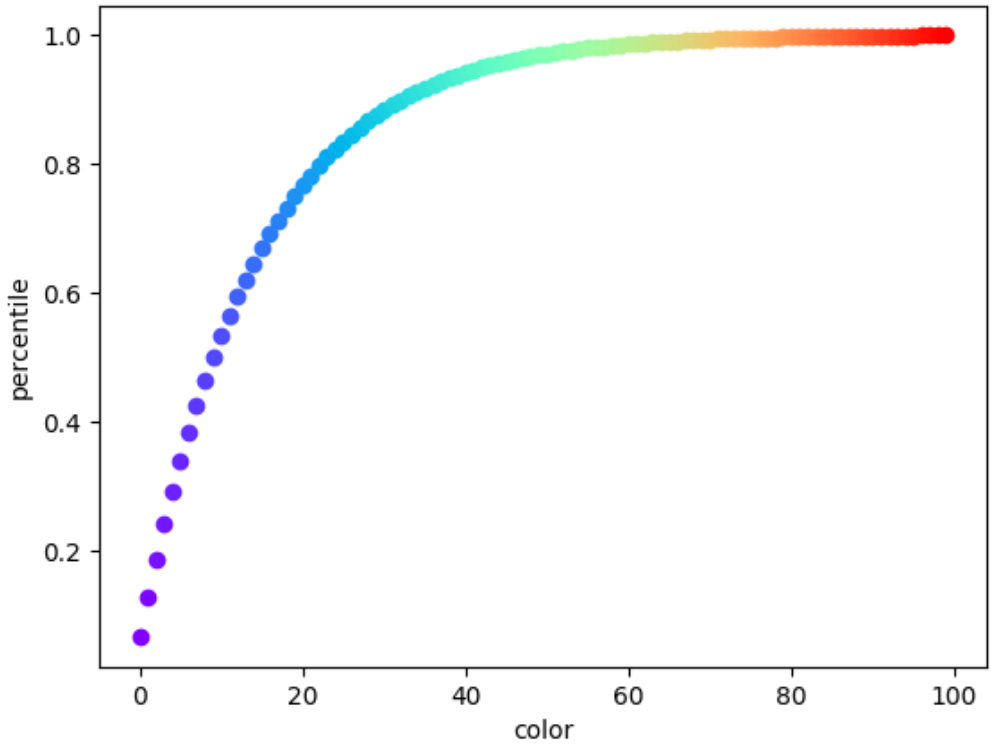
- В процессе реализации фреймворка для детектирования атак была протестирована реализация алгоритма NewHope (один из претендентов в конкурсе пост-квантовой криптографии NIST) от Российского Квантового Центра. Обнаружена потенциальная уязвимость к атакам по времени и успешна исправлена
- Рассмотрена реализация AES с использованием таблиц поиска.

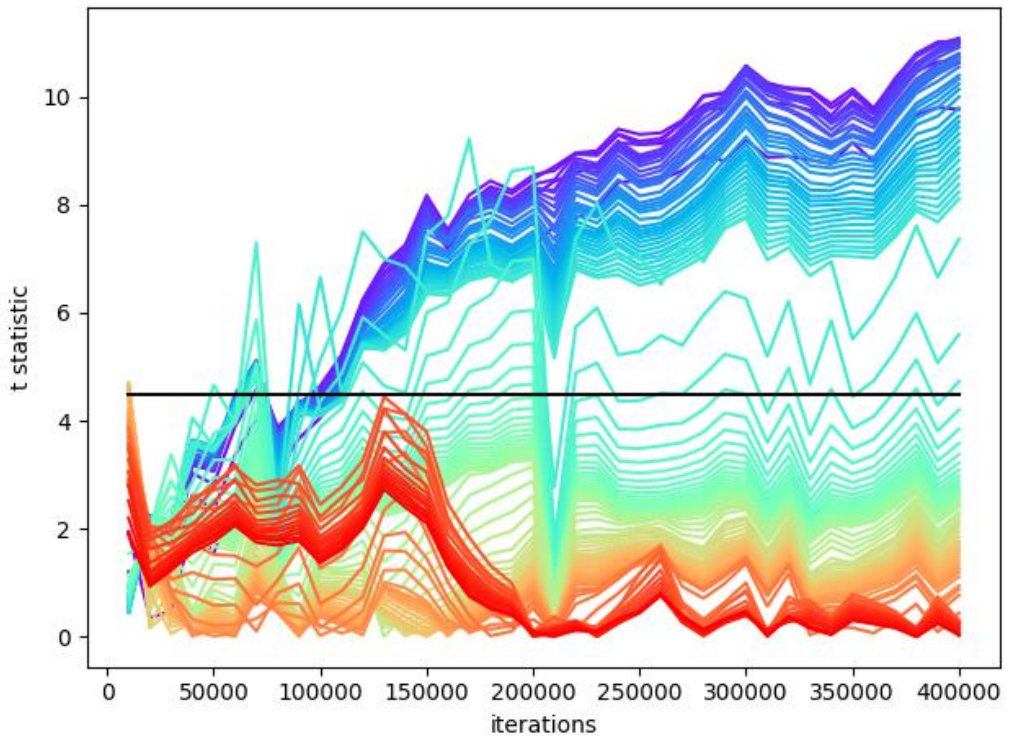
Дополнительная обработка измерений

- При измерении времени неизменно влияет среда. Этот шум может только повысить (иногда значительно) время выполнения
- Значение t остаётся небольшим и тест теряет силу
- В качестве решения можно отбрасывать верхние перцентили

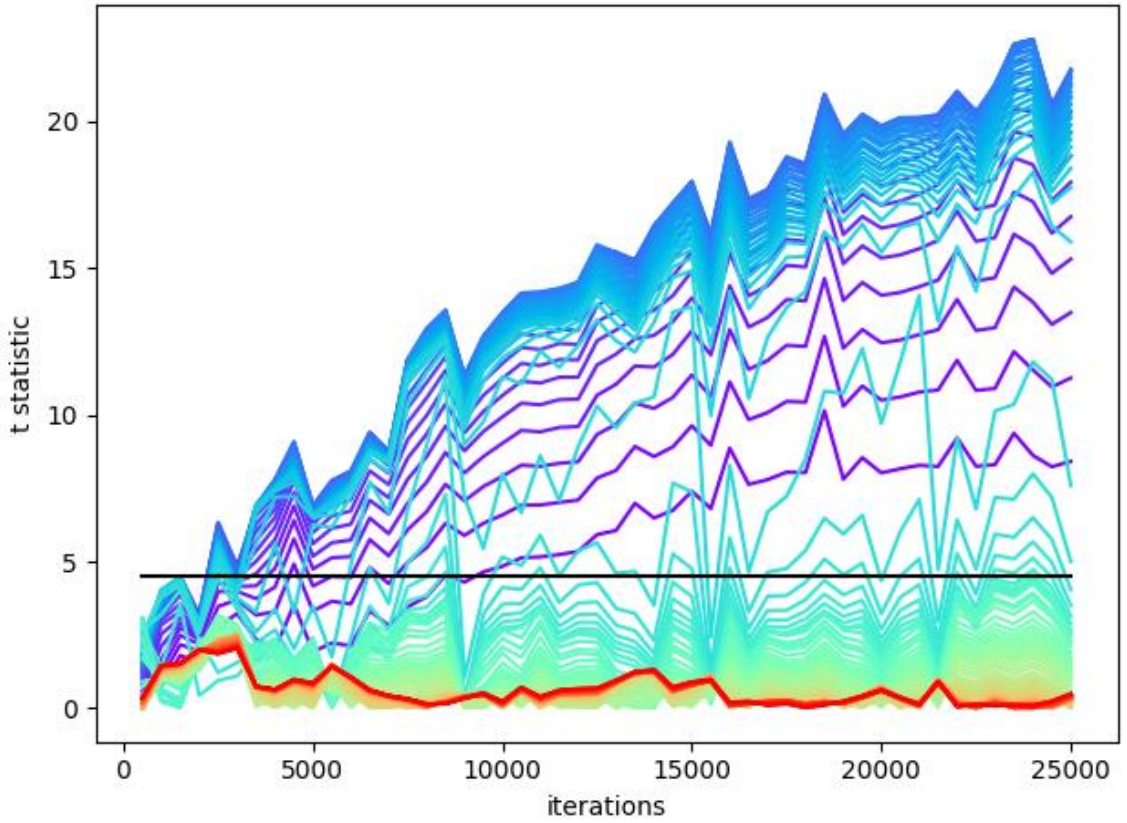
$$t = \frac{\mu_0 - \mu_1}{\sqrt{\frac{{s_0}^2}{n_0} + \frac{{s_1}^2}{n_1}}}$$

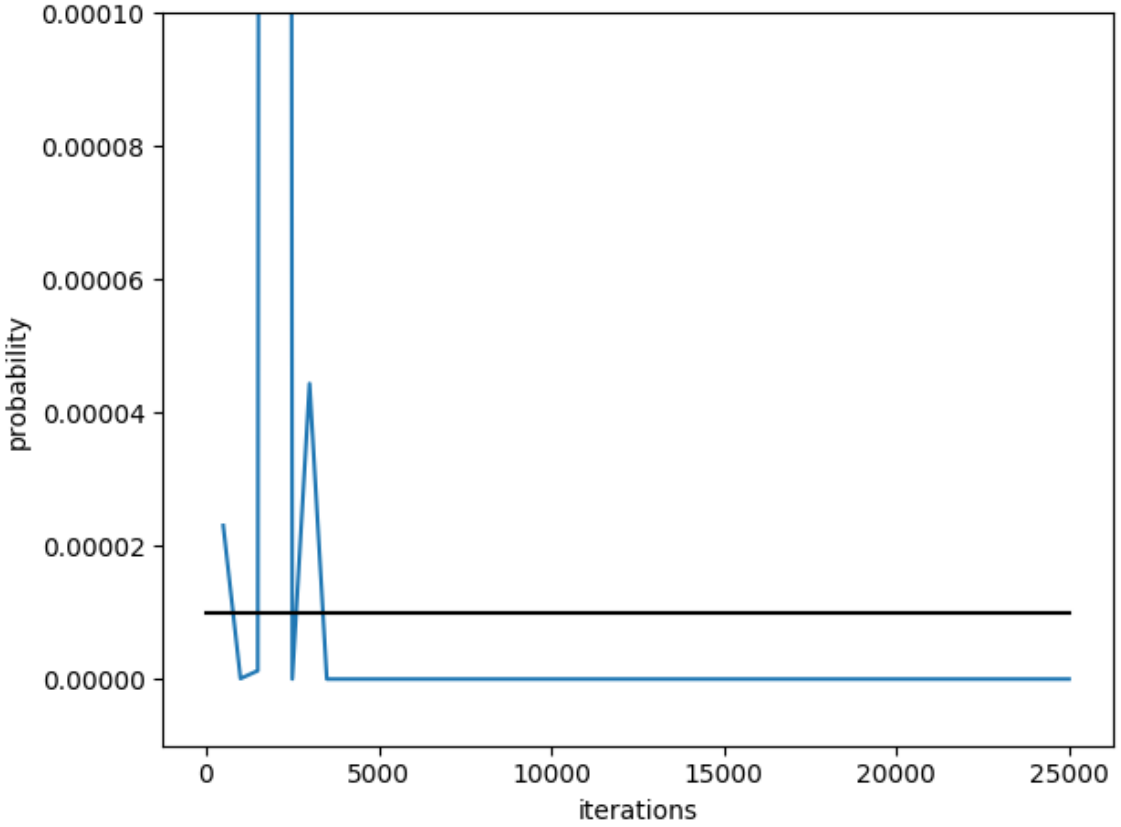
Отбрасывание перцентилей



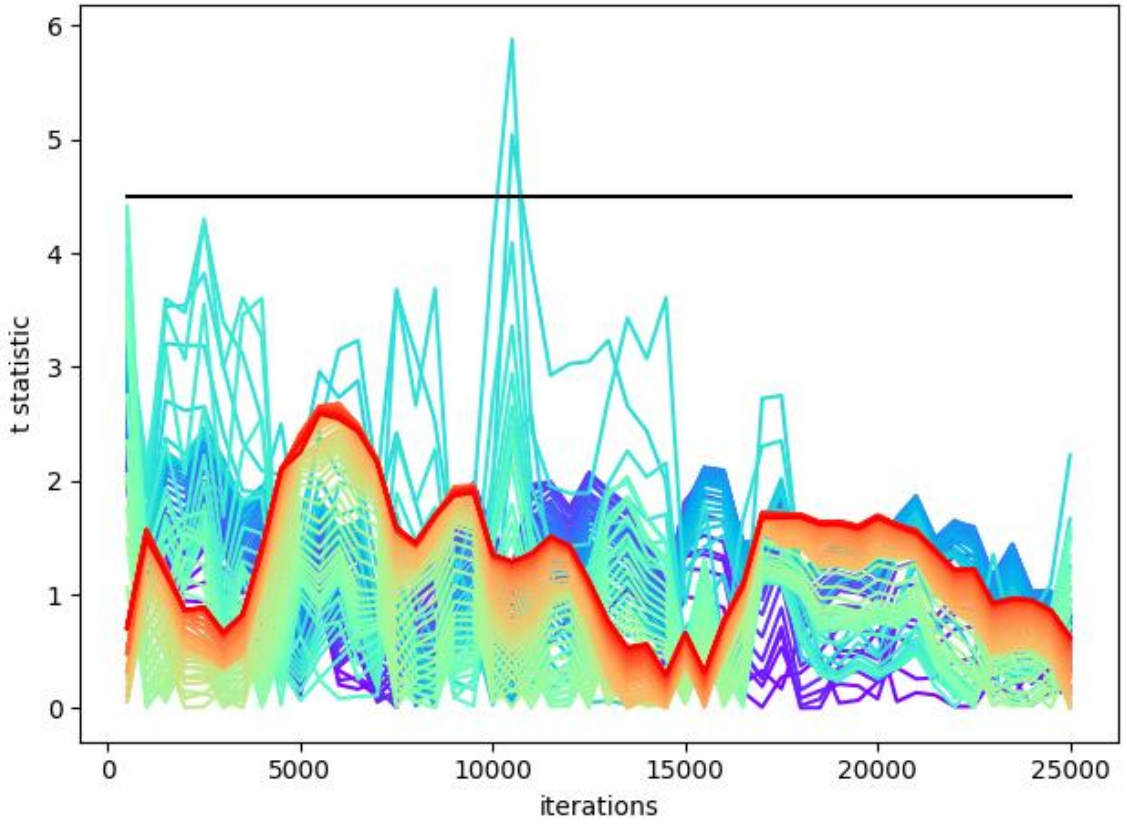


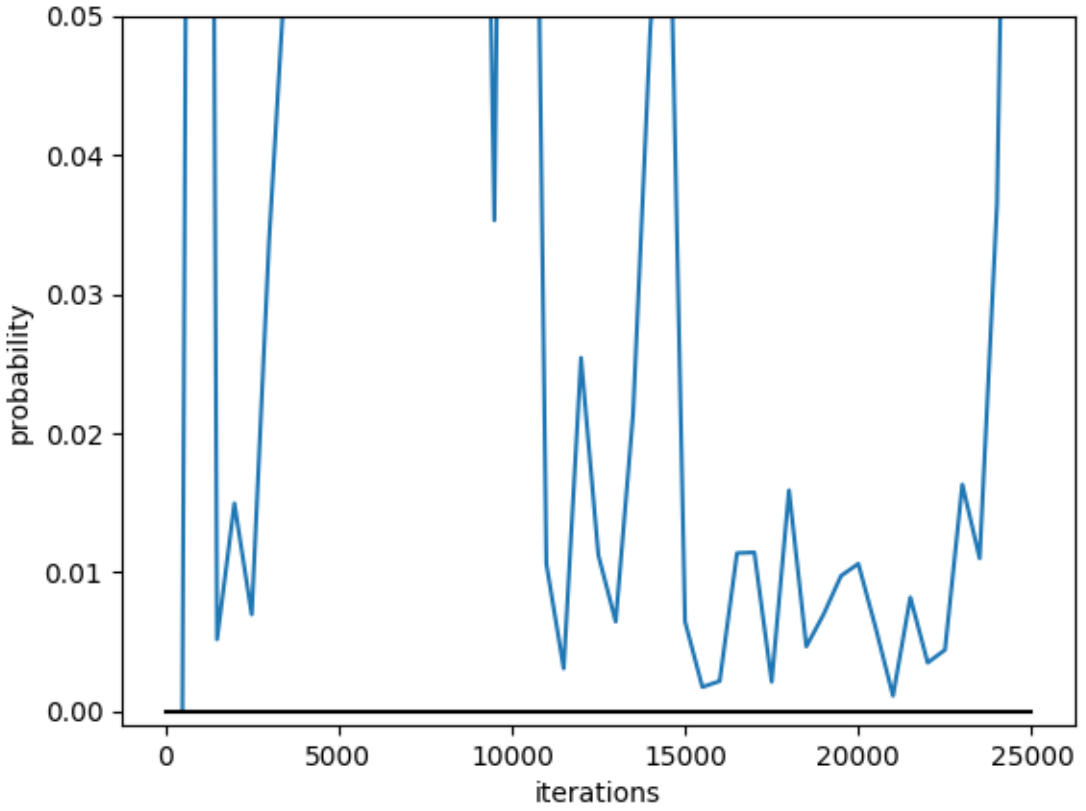
NewHope с уязвимостью



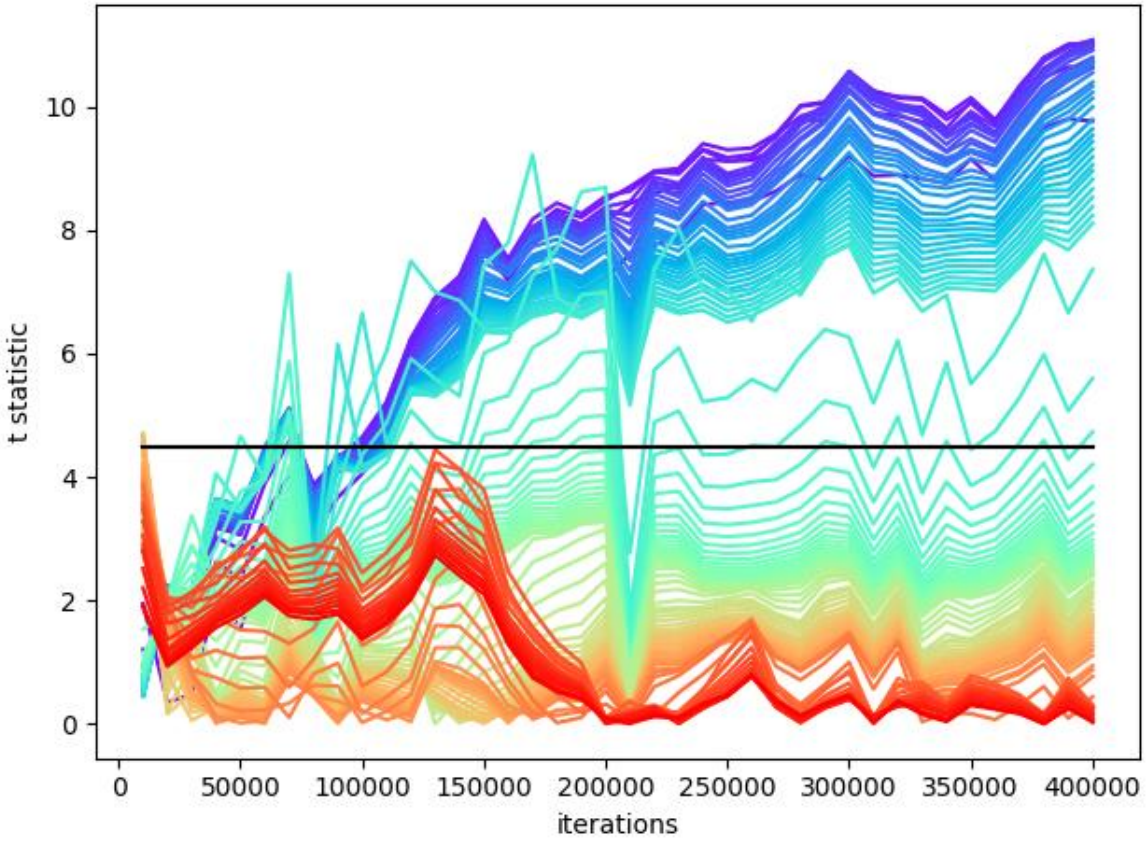


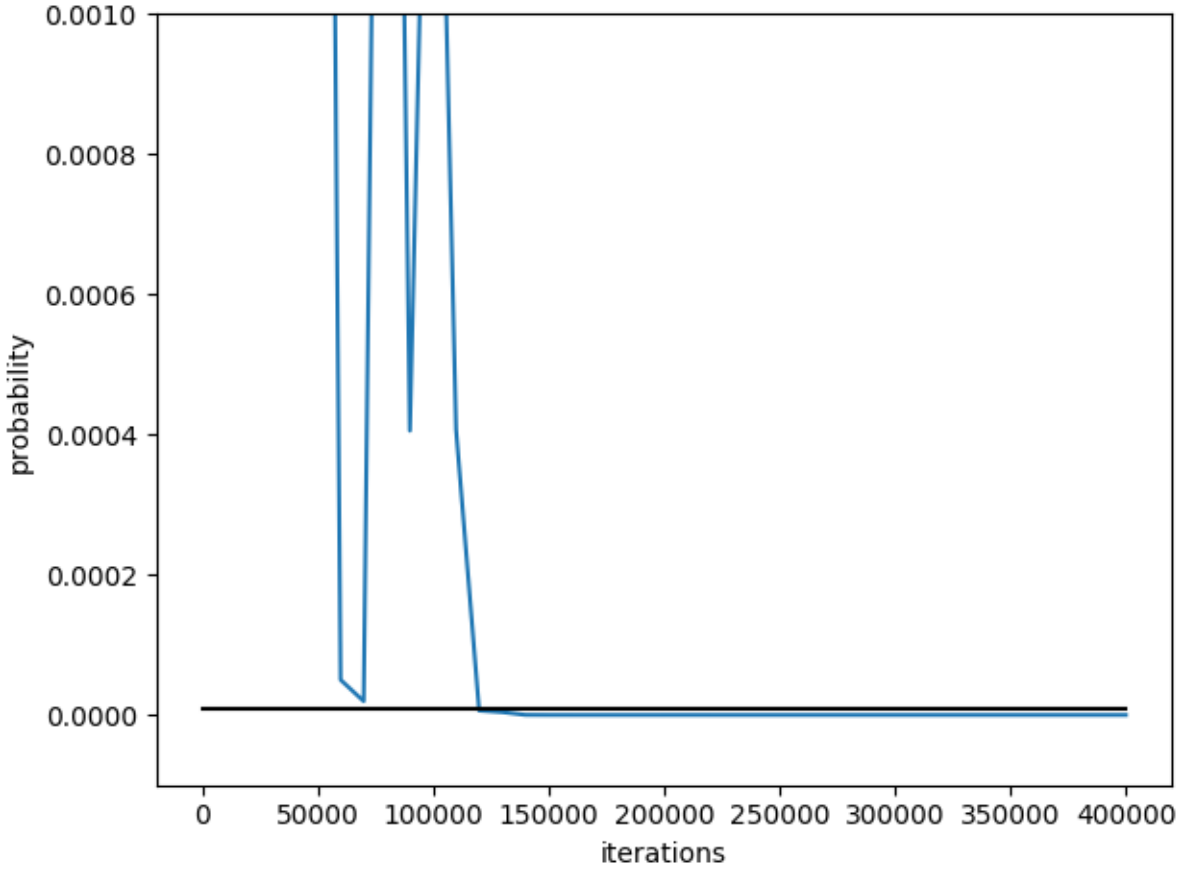
Исправленный NewHope





AES


t statistic
iterations
0
2
4
6
8
10
0
50000
100000
150000
200000
250000
300000
350000
400000


probability
iterations
0.0000
0.0002
0.0004
0.0006
0.0008
0.0010
0
50000
100000
150000
200000
250000
300000
350000
400000

Дальнейшая работа

- Определить, улучшится ли тест Колмогорова-Смирнова при использовании фильтрации
- Установить, как лучше выбирать значение перцентилей
- Welch’s t-test с обработкой измерений позволяет сравнивать не только матожидание, но и дисперсию, а также другие статистические моменты

$$SM_d = E\left(\left(\frac{X-\mu}{s}\right)^d\right), d > 2$$

- Протестировать все алгоритмы с конкурса NIST

Вопросы

Контактная информация

Электронная почта:

nabokov.da@yandex.ru

Телефон:

+7 912 399-47-87

Сайт:

www.rqc.ru