Министерство образования Республики Беларусь

Учреждение образования
БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
ИНФОРМАТИКИ И РАДИОЭЛЕКТРОНИКИ

Факультет Компьютерных сетей и систем

Кафедра Информатики

ОТЧЕТ ПО ЛАБОРАТОРНОЙ РАБОТЕ №3

по курсу «Машинное обучение»

Реализация криптографических атак с помощью машинного обучения на модифицированные физически неклонируемые функции

Студент:
гр. 758641
Ярош Г.И.

Проверил:
Заливако С. С.

Минск, 2018

СОДЕРЖАНИЕ

ИЗУЧЕНИЕ КРИПТОГРАФИЧЕСКИХ АТАК С ПОМОЩЬЮ МАШИННОГО ОБУЧЕНИЯ НА МОДИФИЦИРОВАННЫЕ ФИЗИЧЕСКИ НЕКЛОНИРУЕМЫЕ ФУНКЦИИ

1. Цель

Создать модель, которая могла бы предсказать ответы ФНФ по запросам, которых нет в обучающей выборке. Запросы перед подачей на ФНФ хешируются, что усложняет предсказание ответов по изначальным запросам ФНФ.

2. Эффективность применения логистической регрессии

Для доказательства того, что хеширование запросов значительно усложняет процесс построения модели для предсказания ответов, мною было проведено исследование эффективности алгоритма логистической регрессии для поставленной задачи. Результаты приведены на рисунке 1. Обучение проводилось на выборке длинной 10^5 запросов и ответов. Точность подсчитывалась на выборке размером $9 \cdot 10^5$.

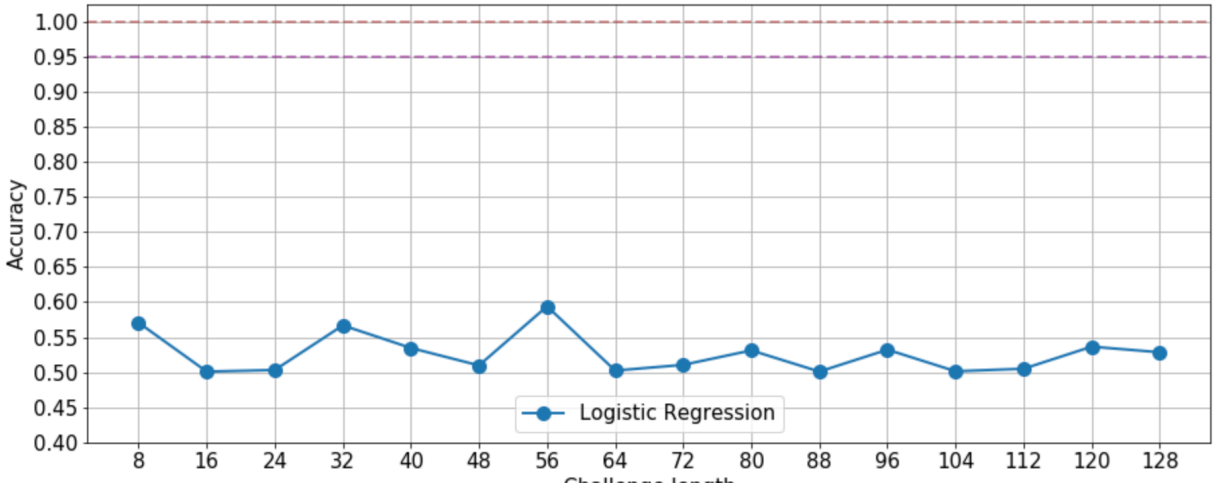

Рис. 1. Зависимость точности предсказания от длинны запроса

3. Алгоритм CMA-ES

Алгоритм эволюционной стратегии адаптации ковариационных матриц предназначен для решения задач оптимизации нелинейных невыпуклых функций.

Эволюционные стратегии представляют собой алгоритмы, где на каждой итерации генерируется новый набор решений. Для каждого решения вычисляется фитнесс функция, которая показывает, насколько решение близко к оптимальному. Новые решения генерируются на основе лучших решений из предыдущей итерации. Сам алгоритм в процессе своей работы минимизирует значение фитнесс-функции.

Метод адаптации ковариационных матриц заключается в следующем. Новые решения на каждой итерации генерируются на основе нормального распределения с заданным математическим ожиданием и матрицей ковариации. Затем для всех решений подсчитывается значение фитнесс-функции. Далее решения сортируются по убыванию значения фитнесс функции. После этого пересчитывается значение мат-ожидания и ковариационная матрица.

4. Применение CMA-ES для решения поставленной задачи

Для решения задачи классификации ответов ФНФ по запросам был применен алгоритм CMA-ES. Входными параметрами фитнесс-функции был выбран вектор x длинной 4 + N + 1, где первые три элемента определяют параметры хеш-функции: инверсия до преобразования, порядок бит, инверсия после преобразования. Так как выход хеш-функции SHA256 имеет длину 256 бит, следующий параметр определяет номер бита, с которого необходимо выбрать N битов запроса. Следующие N параметров запроса определяют вектор разностей задержек сигналов для построения линейной модели ФНФ. Последний параметр определяет смещение линейной модели. В общем виде, вход фитнесс-функции определяется следующим вектором:

$$fitness(reverse1, endian, reverse2, n, w, b)$$

Фитнесс функция преобразует входные параметры к необходимым типам, производит хеширование запросов ФНФ с заданными параметрами, выбирает N бит из хеш-значения, преобразует полученный запрос в знаковый вид. Затем фитнесс-функция считает значение логистической функции от $wx + b$, где x – хешированные запросы. Эти значения принимаются за значения ответов ФНФ. На выход фитнесс-функция возвращает значение разности полученных значений ФНФ и необходимых.

Оптимизация производилась на тестовой выборке длинной в 10^4 запросов. График изменения фитнесс-функции приведен на рисунке 2.

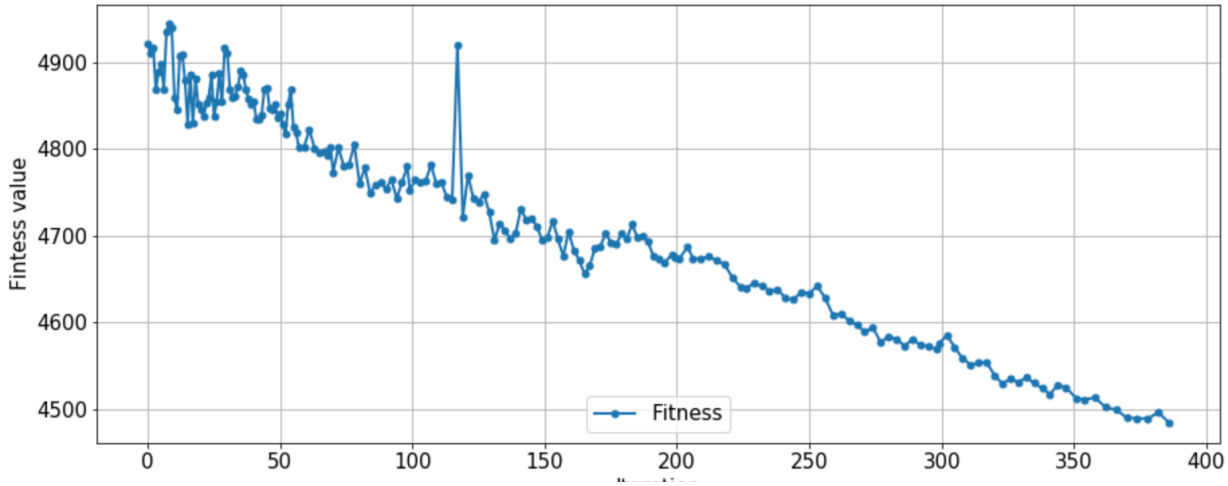

Рис. 2. График изменения значения фитнесс-функции

Не смотря на то, что значение фитнесс-функции уменьшалось с каждой итерацией, подсчет точности на тестовой выборке показал неудовлетворительные

результаты. Точность составила 50%, что соответствует точности случайного угадывания.

Неудача может быть связана с особенностями реализации хеш-функции в питоне и той хеш-функции, которой хешировались запросы, подающиеся на ФНФ. Также фактором, сильно усложняющим оптимизацию, является малая устойчивость хеш-функции и функции преобразования к знаковому представлению. Возможно, что большей точности удалось бы добиться на выборке значительно большего размера.

5. Вывод

В результате работы была исследована возможность предсказания ответов ФНФ по хешированным запросам с помощью линейной регрессии и алгоритма CMA-ES. Оба метода показали неудовлетворительную точность в 50%.