Министерство образования Республики Беларусь

Учреждение образования
БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
ИНФОРМАТИКИ И РАДИОЭЛЕКТРОНИКИ

Факультет Компьютерных сетей и систем

Кафедра Информатики

ОТЧЕТ ПО ЛАБОРАТОРНОЙ РАБОТЕ №1

по курсу «Машинное обучение»

Изучение криптографических атак с помощью машинного обучения на физически неклонируемые функции

Студент:
гр. 758641
Ярош Г.И.

Проверил:
Заливако С. С.

Минск, 2018

СОДЕРЖАНИЕ

ИЗУЧЕНИЕ КРИПТОГРАФИЧЕСКИХ АТАК С ПОМОЩЬЮ МАШИННОГО ОБУЧЕНИЯ НА ФИЗИЧЕСКИ НЕКЛОНИРУЕМЫЕ ФУНКЦИИ

1. Цель

Изучить методы криптографических атак с помощью машинного обучения на физически неклонируемые функции. Сформулировать задачу в терминах машинного обучения. Предложить возможные варианты решения. Оценить размер необходимой выборки.

2. Физически неклонируемая функция

Физически неклонируемая функция представляет собой аппаратную функцию, которая принимает на вход последовательность бит, называемую запрос (Challenge), и возвращает последовательность бит, называемую ответ (Response). Суть физической неклонируемости заключается в том, что каждая такая функция уникальна для каждого устройства, т.е. на набор запросов каждая отвчеает уникальным набором ответов. Иными словами, одну и ту же функцию нельзя создать для двух разных устройств.

Запрос физически неклонируемой функции представляет собой последовательность бит $C = c_0, c_1, \dots, c_N$ длинной N. Ответом данной функции будет служить один бит R (в данной работе рассматриваются ФНФ с ответом длинной в один бит).

Существует множество реализаций физически неклонируемых функций. В данной работе рассматривается ФНФ типа арбитр. В ней ответ вычисляется как разница между двумя конкурирующими сигналами, проходящими через N элементов. Каждый такой элемент определяет различную задержку для каждого из сигналов основываясь на соответствующем бите из запроса ФНФ (рис. 1).

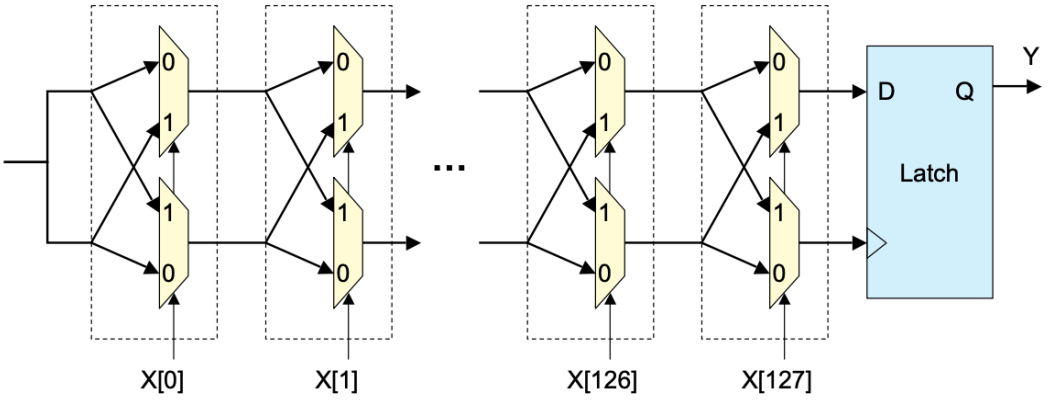

Рис. !. Модель ФНФ типа арбитр.

Свойство неклонируемости в данном типе ФНФ обеспечивается тем фактом, что невозможно воспроизвести точные значения задержек сигналов в каждом элементе ФНФ.

3. Формулировка задачи машинного обучения

Задача предсказания ответов ФНФ основываясь на запросах относится к классу задач классификации. Каждый бит запроса может быть рассмотрен, как последовательность признаков. Количество признаков равно длинне запроса N. Классами в данной задаче являются значения ответов {0, 1}. Следовательно задача является задачей бинарной классификации.

Необходимо построить модель, которая по набору бит запроса будет способна предсказать ответ, совпадающий с ответом ФНФ.

Для успешной классификации, необходимо последовательность бит запроса привести к знаковому виду. Это преобразование производится в соответствии с линейной аддитивной моделью распространения сигнала ФНФ [1] по формуле:

$$c'_l = \prod_{i=0}^{l}(1 - 2c_i), l = 0, \dots, N;$$

Данная задача классификации может быть решена с помощью применения следующих алгоритмов машинного обучения:

- Логистическая регрессия;
- Деревья решений;
- Метод опорных векторов;
- Нейронные сети.

4. Необходимый размер выборки

Необходимый размер выборки может быть оценен с помощью формулы, полученной в работе [2]:

$$L = 0.5\frac{N+1}{e};$$

где L – необходимый размер выборки, N – длинна запроса ФНФ, e – максимальное значение ошибки предсказания.

5. Вывод

В результате работы был изучен принцип функционирования ФНФ, изучен метод атак на физически неклонируемую функцию, сформулирована соответствующая задача машинного обучение.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

[1] - Ruhrmair, U. PUF modeling attacks on simulated and silicon data / U. Ruhrmair, et al. // IEEE Transactions on Information Forensics and Security. -– 2013. -– № 8(11). -– P. 1876-–1891.

[2] - U. Ruhrmair et al., “Modeling attacks on physical unclonable functions,” in Proc. ACM Conf. on Comp. and Comm. Secur. (CCS’10), Oct. 2010, pp. 237–249.