# АЛГОРИТМЫ И МЕТОДЫ МАШИННОГО ОБУЧЕНИЯ ДЛЯ ОЦЕНКИ УСТОЙЧИВОСТИ ФИЗИЧЕСКИ НЕКЛОНИРУЕМЫХ ФУНКЦИЙ К КРИПТОГРАФИЧЕСКИМ АТАКАМ

Кузьма Ю. В., Хлопцев А. А.
Факультет компьютерных систем и сетей, Белорусский государственный университет информатики и радиоэлектроники
Минск, Республика Беларусь
E-mail: dzotcrew@gmail.com, redleonfire@yandex.by

*В статье рассмотрена возможность применения методов и алгоритмов машинного обучения для оценки устойчивости физически нелонируемых функций (ФНФ) к криптографическим атакам. Интерес к данной тематике обусловлен повышением риска криптографических атак, связанным с широким распространением устройств Интернета вещей и различных токенов, смарт-карт, банковских карт, интегральных схем, использующих ФНФ для построения неклонируемых идентификаторов и генерирования случайных числовых последовательностей.*

## Введение

Повсеместное распространение устройств Интернета вещей и различных токенов, смарт-карт, банковских карт, интегральных схем обусловило актуальность задачи их надёжной идентификации [1-2]. Одним из актуальных и активно развивающихся способов для генерации случайных числовых последовотельностей, ключей и невоспроизводимых идентификаторов является использование ФНФ.

По определению, данному в работе [3], физически неклонируемой функцией (от англ. Physical Unclonable Function, PUF) является характеристика физической (цифровой) системы, которая не поддается клонированию (копированию, воспроизведению) на других системах. Данное свойство цифровой системы обусловлено недостаточной точностью производства и/или намеренным использованием материалов с неоднородной структурой (например, использование пасты с частицами феррита бария, различающихся по форме и размеру, при производстве магнитного носителя карт с магнитной полоской).

Широкое применение физически неклонируемых функций повышает заинтересованность злоумышленников в осуществление успешных криптографических атак на них, с целью воспроизведения (подделки), подмены исходной ФНФ. Целью данной работы является исследование возможности применения алгоритмов и методов машинного обучения для оценки устойчивости ФНФ к криптографическим атакам.

## I. Физичске неклонируемые функции

Формально ФНФ описывается значениями пар входных и выходных векторов, которые в цифровых системах представляют входные $C$ (Challenge) и выходные $R$ (Response) сигналы. ФНФ может быть описана множеством всевозможных пар запрос-ответ (Challenge-Response Pairs, CRP), а так же функцией преобразования множества $_i$, во множество $R_i$:

$$R_i = PUF(C_i) \quad (1)$$

Существует множество видов ФНФ, для использования в целях идентификации важным свойством ФНФ является стабильность ответа ФНФ на многократно повторяющийся запрос при одних и тех же условиях. По этим параметрам для исследования выбрана ФНФ типа «арбитр» (АФНФ) [4]

## II. Выбор инструментов

Авторами, данной работы, для проведения исследования были выбраны следующие инструменты:

- язык программирования Python;
- математическая библиотека numpy;
- библиотека для обработки и анализа данных pandas;
- библиотека машинного обучения scikit-learn;
- библиотека визуализации данных matplotlib.

Поскольку библиотека scikit-learn предоставляет широкий выбор моделей и различных нейронных сетей, авторами были выбраны некоторые из них, а именно модели Perceptron и SGDRegressor, а также нейронная сеть MLPClassifier

## III. Результаты

Выбранные модели и нейронные сети были обучены на выборках различных размеров (1000, 5000, 10000, 50000, 100000) содержащих векторы признаков различной длинны (8, 16, 32, 64, 128 бит) и значения эталонных классов для них. Ниже представлены результаты оценки точности предсказания, обученных на выборках моделей и нейронной сети, проведённой методом кросс-валидации для

Perceptron (см. рис. 1), SGDRegressor (см. рис. 1), MLPClassifier (см. рис. 1).

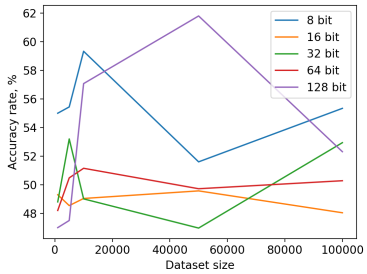


Рис. 1 – Точность предсказания Perceptron

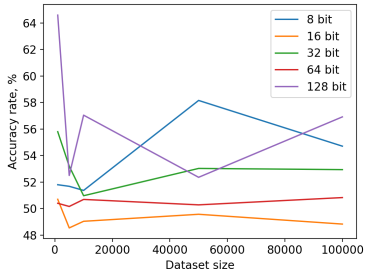


Рис. 2 – Точность предсказания SGDRegressor

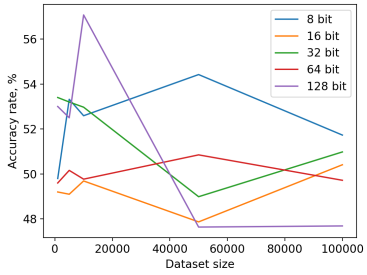


Рис. 3 – Точность предсказания MLPClassifier

Как видно из графиков, на исходных данных линейные модели и нейронная сеть не показывают значительных результатов, поэтому, основываясь на данных работы [5], было принято решение преобразовать входные данные с помощью функции $Z$ и повторить эксперимент.

$$Z(\omega_i) = \begin{cases} \omega_i = 1 & i = 1 \\ \omega_i = \omega_{i-1} * -1^{\omega_i} & i > 1 \end{cases}$$

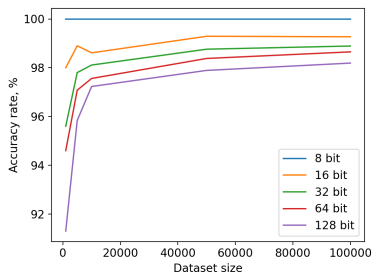


Рис. 4 – Точность предсказания Perceptron

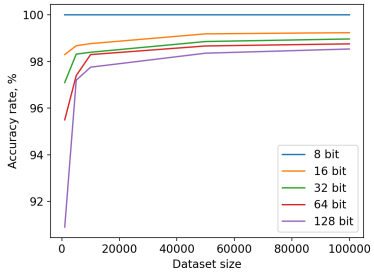


Рис. 5 – Точность предсказания SGDRegressor

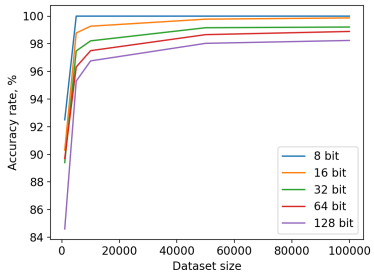


Рис. 6 – Точность предсказания MLPClassifier

Как видно из графиков (см. рис. 4-6), на предобработанных данных линейные модели и нейронная сеть показывают положительные результаты.

## IV. Заключение

В ходе исследования были получены положительные результаты применения алгоритмов и методов машинного обучения для оценки устойчивости АФНФ. Так же был сделан вывод о неустойчивости АФНФ к атакам, осуществляемым с помощью машинного обучения и необходимости разработки метода защиты функции от атак такого типа.


1. London Calling: Security technology takes time. UBM Tech Electronics [Electronic resource] / Peter Clark – EE Times, 2013. – Mode of access: https://www.eetimes.com/nxp-and-intrinsic-id-to-raise-smart-chip-security/. – Date of access: 12.10.2020
2. NXP and Intrinsic-ID to raise smart chip security [Electronic resource] / EETimes – EE Times, 2010. – Mode of access: https://www.eetimes.com/nxp-and-intrinsic-id-to-raise-smart-chip-security/. – Date of access: 12.10.2020
3. Architecture and Design Flow for a Highly Efficient Structured ASIC / H. Man-Ho // IEEE Transactions on VLSI Systems. –2012. – Vol. 21, iss. 3. – P. 423-433
4. A technique to build a secret key in integrated circuits for identification and authentication applications / J. W. Lee // Intern. Symp. VLSI Circuits (VLSI'04), Honolulu, USA, June 15–19, 2004 –Honolulu, 2004. – P. 176–179.
5. Клыбик, В. П. Метод увеличения стабильности физически неклонируемой функции типа «арбитр» / В. П. Клыбик, С. С. Заливако, А. А. Иванюк // Информатика –2017. – № 1. – С. 32–36.