Научная статья
УДК: 621.38
DOI: 10.26583/bit.2025.1.05

# МЕТОД ИССЛЕДОВАНИЯ АТАК НА ОСНОВЕ МАШИННОГО ОБУЧЕНИЯ НА ФИЗИЧЕСКИ НЕКЛОНИРУЕМЫЕ ФУНКЦИИ ТИПА АРБИТР

**Юрий А. Коротаев**
*МИРЭА – Российский технологический университет, пр-кт Вернадского, 78, Москва, 119454, Россия*
*korotaevyua@yandex.ru, https://orcid.org/0009-0000-3976-7872*

***Аннотация.*** В статье рассматриваются современные подходы к атакам на различные варианты физически неклонируемых функций типа арбитр (АФНФ). Выполнена постановка соответствующей задачи с точки зрения машинного обучения. Предложен метод, повышающий эффективность атак на АФНФ. Он основан на предварительном подборе подходящего алгоритма машинного обучения с использованием моделей АФНФ. Такой подход позволяет выполнить предварительную оценку эффективности различных алгоритмов для атак на АФНФ в отсутствие доступа к наборам пар запрос-ответ, полученным при исполнении реальных экземпляров физически неклонируемых функций. Проведены атаки на модели базового и модифицированных вариантов АФНФ из открытой библиотеки pypuf с помощью классического алгоритма логистической регрессии и искусственных нейронных сетей (ИНС). Сделан вывод о большей эффективности ИНС по сравнению с классическими алгоритмами машинного обучения при осуществлении атак на АФНФ. С помощью pypuf разработана архитектура ИНС, которая после минимальной модификации была применена для эффективной атаки на вариант АФНФ, сбалансированный за счет использования дополнительного модуля задержки в структуре базового элемента. Соответствующая АФНФ была реализована на базе программируемой логической интегральной схемы (ПЛИС). Точность предсказания ответов после обучения составила 97,46%.

***Ключевые слова****: физически неклонируемые функции (ФНФ), АФНФ, программируемые логические интегральные схемы (ПЛИС), атаки на ФНФ, машинное обучение, искусственная нейронная сеть.*

***Для цитирования:*** *Коротаев, Юрий А. Метод исследования атак на основе машинного обучения на физически неклонируемые функции типа арбитр. Безопасность информационных технологий, [S.l.], т. 32, № 1, с. 85–94, 2025. ISSN 2074-7136. URL: https://bit.spels.ru/index.php/bit/article/view/1748. DOI: http://dx.doi.org/10.26583/bit.2025.1.05.*

****Благодарности.*** Работа выполнена при поддержке Министерства науки и высшего образования РФ (Государственное задание для университетов № ФГФЗ-2023-0005) и с применением оборудования Центра коллективного пользования РТУ МИРЭА (соглашение от 01.09.2021 № 075–15-2021-689, уникальный идентификационный номер 2296.61321X0010).

Scientific article

# A METHOD FOR INVESTIGATING MACHINE LEARNING ATTACKS ON ARBITER-TYPE PHYSICALLY UNCLONABLE FUNCTIONS

**Yuri A. Korotaev**
*MIREA – Russian Technological University, Vernadsky Ave., 78, Moscow, 119454, Russia*
*korotaevyua@yandex.ru, https://orcid.org/0009-0000-3976-7872*

***Abstract.*** The paper explores modern approaches to attacking various types of Arbiter Physical Unclonable Functions (APUF). The problem is described from a machine learning perspective. A method

is proposed to enhance the efficiency of attacks on APUFs by preliminarily selecting an appropriate machine learning algorithm using PUF models. This approach allows for a preliminary evaluation of the effectiveness of different algorithms for attacking APUFs without access to challenge-response datasets from real instances of physically unclonable functions. Attacks were conducted on models of basic and modified variants of APUFs from the open-source library "pypuf", using classical logistic regression and artificial neural networks (ANNs). The research infers that ANNs outperform traditional machine learning algorithms in carrying out attacks on Arbiter PUFs. An ANN architecture was developed using "pypuf", which, after minimal modification, was effectively applied to attack a balanced variant of an APUF achieved by incorporating an additional delay module into the basic element's structure. The corresponding APUF was implemented on a field-programmable gate array (FPGA). The prediction accuracy after training reached 97.46%.

***Keywords:*** *Physical Unclonable Functions (PUFs), APUF, Field-Programmable Gate Arrays (FPGAs), PUF attacks, machine learning, artificial neural network.*

***For citation:*** *Korotaev, Yuri A. A method for investigating machine learning attacks on arbiter-type physically unclonable functions. IT Security (Russia), [S.l.], v. 32, no. 1, p. 85–94, 2025. ISSN 2074-7136. URL: https://bit.spels.ru/index.php/bit/article/view/1748. DOI: http://dx.doi.org/10.26583/bit.2025.1.05.*

***Acknowledgement.*** This work was supported by the Ministry of Science and Higher Education of the Science and Higher Education of Russian Federation (State task for universities No. FGFZ-2023-0005) and using the equipment of the Center for Collective Use of RTU MIREA (agreement dated September 01, 2021, No. 075-15-2021-689, unique identification number 2296.61321X0010).

## Введение

Физически неклонируемые функции (ФНФ, PUF – Physical Unclonable Functions) являются широко используемыми примитивами аппаратной безопасности. Благодаря уникальным физическим характеристикам ФНФ обеспечивают высокоэффективную защиту электронных компонентов от нелегального копирования и подделки. В современной криптографии они активно используются для генерации криптографических ключей, реализации криптографических протоколов и приложений, а также для создания аппаратных систем, устойчивых к клонированию и обратному проектированию [1].

ФНФ типа арбитр (далее АФНФ) являются первым предложенным типом электронных ФНФ [2]. Принципиальная схема классического варианта АФНФ показана на рис. 1. Она представляет из себя последовательность соединенных определенным образом базовых элементов, каждый из которых является парой мультиплексоров. На оба мультиплексора каждого базового элемента подается один бит $C_i$ запроса $C$. Поданный запрос определяет 2 пути распространения сигнала. Арбитр, представляющий собой D–триггер, формирует бинарный ответ $R$ в зависимости от того, какой сигнал достигнет выхода быстрее.

Основные требования, предъявляемые к физически неклонируемым функциям [3], в случае АФНФ обеспечиваются физической неоднородностью элементов и межсоединений интегральных схем, наличием вариаций в процессе изготовления. Преимуществом ФНФ типа арбитр является то, что они могут быть легко интегрированы в существующие цифровые устройства без необходимости в существенной модификации процессов разработки и производства.

С развитием машинного обучения стало очевидно, что оно может быть использовано для моделирования поведения ФНФ, нивелируя их преимущества в приложениях к аутентификации и аппаратной безопасности электронных изделий [4]. Атаки, основанные на машинном обучении, показали свою высокую эффективность в предсказании откликов ФНФ на новые запросы, используя ограниченный набор известных пар запрос-ответ.

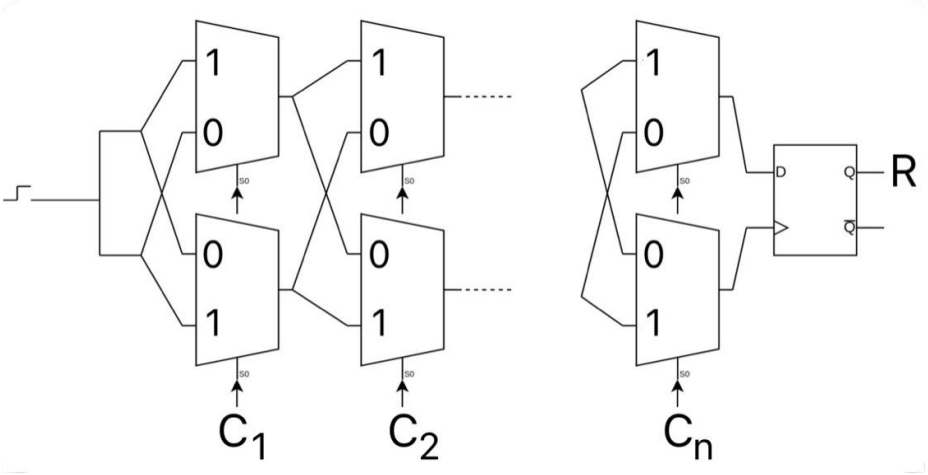



*Рис 1. Принципиальная схема АФНФ*

АФНФ, будучи первым и одним из наиболее простых типов ФНФ, оказался особенно уязвимым к таким атакам. Это связано с тем, что базовый вариант АФНФ имеет относительно простую линейную структуру, которая может быть эффективно смоделирована с помощью алгоритмов машинного обучения, таких как логистическая регрессия или метод опорных векторов. В дальнейшем исследования применений подобных атак были расширены и на другие типы физически неклонируемых функций, что повлияло на их развитие функций как инструментов обеспечения аппаратной безопасности. Можно отметить общий тренд на усложнение предлагаемых вариантов ФНФ [5]. Как следствие, многие современные виды ФНФ имеют более низкий потенциал к реальному применению по сравнению с такими классическими вариантами как АФНФ и SRAM ФНФ [6]. Исследование устойчивости подобных ФНФ к атакам на основе машинного обучения является актуальной задачей в части разработки новых подходов к их осуществлению, применения актуальных алгоритмов машинного обучения, а также оценки устойчивости современных модификаций классических типов физически неклонируемых функций к соответствующим атакам.

Следует отметить, что помимо устойчивости к атакам, существуют и иные метрики, позволяющие оценить ключевые характеристики физически неклонируемых функций, такие как уникальность и стабильность [1]. Их детальное рассмотрение выходит за рамки данной работы. Для улучшения характеристик базового варианта АФНФ были разработаны модификации, которые помимо улучшения основных характеристик продемонстрировали и повышение устойчивости к различным атакам. Наиболее известными из них являются XOR АФНФ [7], Interpose ФНФ [8], Lightweight Secure ФНФ [9]. Однако, некоторые исследования показали, что даже эти улучшенные конструкции могут быть успешно атакованы с использованием более продвинутых методов машинного обучения.

Начало развития темы исследования подобных атак на ФНФ было положено в фундаментальной работе У. Рюрмайра и коллег [4]. Применяя логистическую регрессию и метод опорных векторов, они смогли создать математические модели, которые с высокой точностью предсказывают ответы АФНФ на новые запросы. Исследование показало, что даже «сильные» ФНФ, которые считались безопасными из-за их сложности, могут быть раскрыты при наличии достаточного количества пар запрос-ответ и вычислительных ресурсов. Позднее соответствующие исследования были распространены ими и на один из наиболее защищенных вариантов физически неклонируемых функций типа арбитр – XOR АФНФ [5].

В последние годы многие исследователи сместили фокус на применение ИНС для создания моделей с целью раскрытия ФНФ, в отличие от более ранних работ, где чаще всего применялись такие классические алгоритмы как логистическая регрессия, метод опорных векторов и эволюционные стратегии. Заслуживает внимания работа Р. Визиола и коллег [10], которые впервые внедрили сверточные нейронные сети в область атак на физически неклонируемые функции. Рассматривая биты запроса как одномерное изображение, они использовали возможности сверточных нейронных сетей по извлечению признаков для эффективного моделирования XOR АФНФ. Этот подход позволил достичь более высокой точности предсказаний с использованием меньшего количества пар запрос-ответ для обучения. Другая значимая работа представляет детальное исследование устойчивости нескольких основных вариантов АФНФ к атакам на основе глубокого обучения [11]. При этом в экспериментальной части были указаны недостатки результатов, получаемых при прототипировании ФНФ на ПЛИС и использованы математические модели соответствующих физически неклонируемых функций.

По результатам анализа работ по тематике атак на физически неклонируемые функции типа арбитр, направленных на создание моделей, были сделаны следующие выводы:

- Одним из самых защищенных вариантов АФНФ по отношению к описанным атакам является XOR АФНФ;
- Наиболее эффективные атаки выполняются с использованием глубоких нейронных сетей, способных моделировать сложные нелинейные зависимости между запросами и ответами и улавливать глубокие паттерны взаимодействия в данных. Перспективным является применение сверточных ИНС;
- На сегодняшний день продолжаются попытки модификаций физически неклонируемых функций типа арбитр с целью улучшить их характеристики, в частности устойчивость к атакам на основе машинного обучения;
- Предлагаемые варианты АФНФ должны проверяться на устойчивость к атакам с помощью методов машинного обучения, в особенности, искусственных нейронных сетей;
- Помимо использования данных, полученных с АФНФ, которые были реализованы на ПЛИС, перспективным в исследовании их устойчивости к атакам является использование пар запрос-ответ, сгенерированных с помощью моделей ФНФ, а также открытых наборов пар запрос-ответ.

## 1. Постановка задачи атаки на АФНФ с точки зрения машинного обучения

***Определение 1.*** Атака на физически неклонируемую функцию – намеренное действие, направленное на получение возможности определять значения ответов ФНФ, соответствующее её запросам.

Целью атаки на ФНФ является её раскрытие.

***Определение 2.*** Раскрытие физически неклонируемой функции – успешная атака на ФНФ.

Можно выделить несколько типов атак, такие как атаки, направленные на построение моделей, атаки по сторонним каналам, инвазивные атаки. В рамках данной работы рассматривается первый из перечисленных вариантов атак.

***Определение 3.*** Атака на основе машинного обучения на физически неклонируемую функцию – создание модели, позволяющей предсказывать ФНФ ответы на произвольные запросы, с целью раскрытия функции.

В данной работе рассматривается ситуация, при которой происходит утечка некоторого набора пар запрос-ответ. По этим данным создается модель, которая с

высокой степенью точности предсказывает ответ на любой запрос отличный от существующего в начальном наборе. Точность соответствующего предсказания будет определять степень успешности атаки и, соответственно, уязвимости ФНФ. Сформулируем задачу атаки на АФНФ с точки зрения машинного обучения.

Вектор-признаков составляется из $n$ бит запроса:

$$\boldsymbol{c_i} = \{c_{i1}, c_{i2} \ldots\ldots c_{in}\}, i = 1, 2 \ldots\ldots m,$$

где $n$ – разрядность ФНФ, то есть количество бит запроса, а $m$ – количество возможных различных запросов, которое для АФНФ составляет $2^n$.

Так как ответ арбитра является бинарным, с точки зрения машинного обучения атака на АФНФ является задачей бинарной классификации. В терминах машинного обучения ответ АФНФ является меткой класса:

$$r \in R = \{0, 1\}.$$

Обучающей выборкой является набор пар запрос-ответ, подвергшийся утечке. Тестовым и/или валидационным вектором-запросом может служить любой произвольно выбранный запрос из пространства запросов, отсутствующий в обучающей выборке.

Основной метрикой в задаче классификации является точность (accuracy), которая представляет собой долю правильно предсказанных откликов среди всех предсказаний:

$$Accuracy = \frac{TP + TN}{TP + TN + FP + FN},$$

где TP (True Positives) – количество истинно положительных предсказаний, TN (True Negatives) – количество истинно отрицательных предсказаний, FP (False Positives) – количество ложноположительных предсказаний, FN (False Negatives) – количество ложноотрицательных предсказаний.

Также при оценке классификатора могут применяться такие метрики, как точность (precision), полнота (recall), F1-мера (F1-score), кривая ROC-AUC. Помимо метрик качества модели, при оценке эффективности атак необходимо учитывать размеры обучающей и тестовой выборок и время обучения.

При решении практических задач машинного обучения важную роль играет предварительная обработка данных. В частности, стандартизация признаков, то есть приведение их к среднему значению нуля и единичному стандартному отклонению, что значительно ускоряет обучение моделей и повышает качество предсказаний. В контексте рассматриваемой задачи это достигается простой операцией над каждым входным признаком:

$$c_i = c_i \times 2 - 1.$$

В результате происходит следующее преобразование значений, принимаемых признаками:

$$\{0, 1\} \rightarrow \{-1, 1\}.$$

Для линейных алгоритмов стандартизация обеспечивает равномерное влияние каждого признака на модель и улучшает сходимость оптимизационных методов, а для ИНС способствует более стабильному и эффективному обучению, облегчая процесс оптимизации за счёт центрирования данных вокруг нуля, тем самым улучшая работу функций активации и ускоряя распространение градиентов по сети.

## 2. Исследование атак на АФНФ с помощью библиотеки pypuf

Pypuf – это открытая библиотека на языке Python, предназначенная для моделирования физически неклонируемых функций на основе аддитивной модели задержек [12]. Она предоставляет возможность создания экземпляров различных типов ФНФ с регулированием их параметров, симуляции их поведения и оценки устойчивости к атакам. Библиотекой поддерживаются классический вариант АФНФ, XOR АФНФ, Lightweight Secure ФНФ и другие типы физически неклонируемых функций. Благодаря тому, что pypuf реализована на языке Python, она легко интегрируется в единый маршрут с другими инструментами машинного обучения. Таким образом, библиотека pypuf представляется удобным инструментом для базового анализа эффективности различных моделей в атаках на основные типы АФНФ.

Для первоначальной проверки применимости библиотеки pypuf к описанной выше задаче, выполнена простейшая атаки с помощью логистической регрессии, используя библиотеку Sklearn на 64 битный экземпляр классического варианта АФНФ. Параметры модели:

solver = «liblinear», penalty = «l2», max_iter=1000.

Было сгенерировано 100000 пар запрос-ответ, 80% которых составили обучающую выборку, 20% – тестовую. Количество итераций 1000. Для достижения максимальной точности был применен метод кросс-валидации для поиска наилучшего регуляризационного параметра с помощью инструмента GridSearchCV. В результате, с использованием минимального количества вычислительных ресурсов удалось выполнить успешную атаку. Достигнута точность 99,95%. Аналогичная простая атака была применена к заведомо более устойчивой к атакам 64 битной 2-XOR АФНФ. Точность составила 50.72%, оказалась близка к случайному классификатору несмотря на то, что использовалась увеличенная обучающая выборка. С помощью расширения параметров кросс-валидации, увеличения в 10 раз обучающей выборки и времени обучения точность предсказания ответов была повышена до 76,73%. Таким образом можно сделать выводы о качественном согласии результатов, полученных при моделировании атак на АФНФ с помощью библиотеки pypuf и при физической реализации экземпляров АФНФ, и о том, что атаки на модифицированные варианты АФНФ с помощью классических алгоритмов могут требовать значительных затрат ресурсов [7].

Далее библиотека pypuf была использована для поиска оптимальной структуры ИНС, позволяющей достигать более высокой точности атаки с использованием меньшего количества ресурсов. Была проведена серия экспериментов с архитектурой модели и настройкой гиперпараметров для достижения наилучшей точности предсказания ответов. Процесс включал подбор количества и размера скрытых слоёв необходимых для улавливания сложных нелинейных зависимостей, применение методов регуляризации, а также предобработку данных и настройку параметров обучения, что в итоге привело к созданию модели, эффективно моделирующей поведение АФНФ. Модель была реализована с помощью фреймворка PyTorch и является многослойным перцептроном, состоящим из нескольких полносвязных слоев. Параметры модели приведены в табл. 1.

Данная ИНС показала высокую эффективность при атаках моделей АФНФ из библиотеки pypuf. В частности, была получена точность 99,66% для 2-XOR АФНФ. Модель может быть обучена на стандартном оборудовании, таком как современный CPU или доступный GPU, без необходимости в высокопроизводительных вычислительных кластерах.

*Таблица 1. Основные параметры полученной ИНС*

| Категория параметров | Параметр | Значение |
|---|---|---|
| Архитектура модели | Входной слой | Вход размерности 64 |
| | 1 скрытый слой | 512 нейронов, ReLU, Dropout(0.4), BatchNorm1d(512) |
| | 2 скрытый слой | 256 нейронов, ReLU, Dropout(0.3), BatchNorm1d(256) |
| | 3 скрытый слой | 128 нейронов, ReLU, Dropout(0.2), BatchNorm1d(128) |
| | 4 скрытый слой | 64 нейрона, ReLU, Dropout(0.1), BatchNorm1d(64) |
| | Выходной слой | 1 нейрон, Sigmoid-активация |
| Параметры обучения | Функция потерь | Бинарная кросс-энтропия (BCELoss) |
| | Оптимизатор | Adam |
| | Скорость обучения (lr) | 1e-4 |
| | L2-регуляризация | 1e-5 |
| | Размер батча | 2048 |
| | Количество эпох | 50 |
| | Планировщик обучения | ReduceLROnPlateau |

Основным источником возможных ошибок в классификации является переобучение модели, которое особенно характерно для искусственных нейронных сетей ввиду большого количества параметров. Одной из основных причин переобучения является недостаточное количество обучающих данных, поэтому успешность атак на ФНФ с помощью машинного обучения напрямую зависит от количества пар запрос-ответ, доступных злоумышленнику. При моделировании атаки применяется тестовая выборка, не используемая в обучении.

В полученной модели после каждой эпохи обучения проводится оценка на валидационной выборке, дополнительно выделяемой из тренировочной, что позволяет оценивать обобщающую способность модели и регулировать скорость обучения. Также для предотвращения переобучения используется механизм ранней остановки, при котором обучение прекращается, если качество на валидации не улучшается в течение нескольких эпох, и регуляризация с помощью Dropout.

## 3. Применение модели

Для реализации на ПЛИС и последующего сбора пар запрос-ответ с целью организации атаки была выбрана модификация АФНФ, основанная на работах В. Ярмолика и А. Иванюка [13, 14], в которых они проводят глубокий теоретический анализ ФНФ типа арбитр, выделяя в базовом элементе АФНФ три различные функции: генерации задержек сигнала, выбора пары путей и переключения путей. Авторы указывают, что совмещение всех трех функций в одном элементе – мультиплексоре приводит к асимметрии путей, ухудшая стабильность и уникальность АФНФ. Предлагается новый базовый элемент АФНФ, в который добавляется элемент задержки, реализующий функцию генерации задержек. Показано, что такой подход повышает симметрию путей, что улучшает такие ключевые характеристики АФНФ, как стабильность, уникальность и единообразие [14].

Ранее был неоднократно раскрыт процесс реализация базового варианта АФНФ на ПЛИС [15]. В абсолютном большинстве соответствующих работ применяются ПЛИС фирмы Xilinx. Особенностью данной работы является использование низко ресурсной ПЛИС Altera Cyclone 4 и, соответственно, среды разработки Altera Quartus. Общей особенностью реализации, непосредственно, АФНФ на языке Verilog в среде Altera Quartus по сравнению с Xilinx является использование отличных конструкций, встроенных в HDL описание с целью, предотвращения агрессивной оптимизации в процессе синтеза, что является необходимым условием для реализации АФНФ. В данном случае был использован атрибут *(* keep *)*.

Основной же сложностью реализации АФНФ на конкретном варианте ПЛИС является организация интерфейса взаимодействия с ПК. Для этой цели был реализован интерфейс UART в виде отдельных модулей RX и TX на основе физического интерфейса стандарта RS-232. Подключение к ПК осуществлялось через преобразователь RS-232/USB. На стороне ПК для отправки и передачи применялась библиотека языка Python pySerial.

Для реализации 64 битной сбалансированной АФНФ был разработан простейший модуль задержки, состоящий из четырех последовательных инверторов. Общая структура базового элемента после синтеза показана на рис. 2.

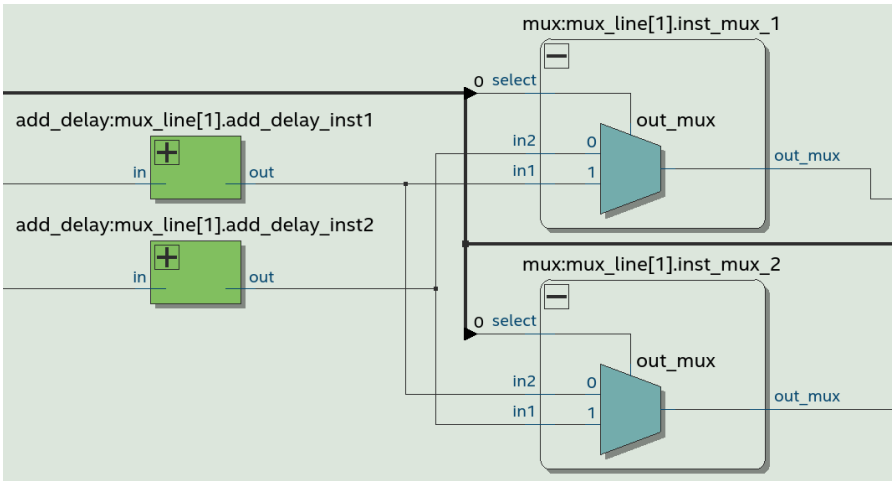



*Рис. 2. Базовый элемент сбалансированной АФНФ*

С помощью библиотеки pypuf было сгенерировано 500000 произвольных 64 битных запроса, которые были поданы на вход ФНФ. Вместе с полученными ответами они сформировали полный набор данных, 80% от которого составили обучающую выборку. Для выполнения атаки использовалась описанная выше модель. С целью получения наилучшей точности была выполнена настройка модели, состоящая в

увеличении количества эпох обучения до 100 и уменьшении batch_size до 256. Точность на тестовой выборке составила 97,46%.

## Заключение

При исследовании атак на физически неклонируемые функции помимо самого факта успешности атаки необходимо учитывать сложность построения соответствующей модели. В этой связи актуальным является изучение вспомогательных инструментов, в первую очередь, моделей ФНФ и доступных датасетов. Так как АФНФ являются наиболее распространенным типом физически неклонируемых функций, для них существует наибольшее количество таких инструментов, одним из которых является библиотека pypuf. В работе было показано, что с её помощью возможно подготовить модель, которая при минимальной настройке параметров способна продемонстрировать высокую точность в предсказании ответов на неизвестные при обучении запросы.

СПИСОК ЛИТЕРАТУРЫ:

1. Joshi S., Mohanty S.P. and Kougianos E. Everything You Wanted to Know About PUFs. IEEE Potentials, v. 36, no. 6, p. 38–46, 2017. DOI: 10.1109/MPOT.2015.2490261.
2. Blaise Gassend, Dwaine Clarke, Marten van Dijk, and Srinivas Devadas. 2002. Silicon physical random functions. In Proceedings of the 9th ACM conference on Computer and communications security (CCS '02). Association for Computing Machinery, New York, NY, USA, 148–160. DOI: https://doi.org/10.1145/586110.586132.
3. Коротаев Ю.А., Певцов Е.Ф. Физически неклонируемые функции на основе вариаций формирования переходных отверстий СБИС. Перспективные материалы и технологии (ПМТ-2024): Сборник докладов Международной научно-технической конференции ИПТИП РТУ МИРЭА, Москва, 12–16 апреля 2024 года. М.: МИРЭА - Российский технологический университет. 2024, с. 318–324. – EDN: YQTIRS.
4. Ulrich Rührmair, Frank Sehnke, Jan Sölter, Gideon Dror, Srinivas Devadas, and Jürgen Schmidhuber. 2010. Modeling attacks on physical unclonable functions. In Proceedings of the 17th ACM conference on Computer and communications security (CCS '10). Association for Computing Machinery, New York, NY, USA, p. 237–249. DOI: https://doi.org/10.1145/1866307.1866335.
5. Коротаев Ю.А. Оптические физически неклонируемые функции. Оптические технологии, материалы и системы (Оптотех - 2023): Сборник докладов Международной научно-технической конференции, Москва, 11–15 декабря 2023 года. М.: МИРЭА - Российский технологический университет. 2023, с. 439–445. – EDN: PTVUCX.
6. Korenda A.R., Afghah F., Cambou B. and Philabaum C. A Proof of Concept SRAM-based Physically Unclonable Function (PUF) Key Generation Mechanism for IoT Devices. 16th Annual IEEE International Conference on Sensing, Communication, and Networking (SECON), Boston, MA, USA. 2019, p. 1–8. DOI: 10.1109/SAHCN.2019.8824887.
7. Rührmair U., Sölter J., Sehnke F., Xu X., Mahmoud A., Stoyanova V., Dror G., Schmidhuber J., Burleson W., & Devadas S. (2013). PUF Modeling Attacks on Simulated and Silicon Data. Cryptology ePrint Archive, Paper 2013/112. URL: https://eprint.iacr.org/2013/112 (дата обращения: 15.09.2024).
8. The Interpose PUF: Secure PUF Design against State-of-the-art Machine Learning Attacks. (2019). IACR Transactions on Cryptographic Hardware and Embedded Systems. 2019(4), p. 243–290. DOI: https://doi.org/10.13154/tches.v2019.i4.243-290.
9. Majzoobi Mehrdad & Koushanfar Farinaz & Potkonjak Miodrag. (2008). Lightweight secure PUFs. P. 670–673. DOI: 10.1109/ICCAD.2008.4681648.
10. Wisiol R., Rührmair U., & Paar C. (2021). Breaking XOR Arbiter PUFs Using Convolutional Neural Networks. In Proceedings of the 30th USENIX Security Symposium (p. 1773–1790). URL: https://ia.cr/2021/555 (дата обращения: 15.09.2024).
11. Santikellur Pranesh, Aritra Bhattacharyay and Rajat Subhra Chakraborty. Deep Learning based Model Building Attacks on Arbiter PUF Compositions. IACR Cryptol. ePrint Arch. 2019 (2019): 566. URL: https://eprint.iacr.org/2019/566.pdf (дата обращения: 15.09.2024).
12. Wisiol N., Grabnitz C., C. Muhl, B. Zengin, T. Soroceanu, and N. Pirnay, pypuf: Cryptanalysis of Physically Unclonable Functions, june 2020. DOI: https://doi.org/10.5281/zenodo.3904267.
13. Ярмолик В.Н., Иванюк А.А. Симметричные физически неклонируемые функции типа арбитр. Информатика. 2024, т. 21, № 1, с. 9–27. DOI: 10.37661/1816–0301-2024-21-1-9-27. – EDN: MQBGUK.
14. Ярмолик Вячеслав Н.; Иванюк Александр А. Сбалансированные физически неклонируемые функции типа арбитр. Безопасность информационных технологий, [S.l.], т. 30, № 1, с. 92–107, 2023. ISSN 2074–7136. DOI: http://dx.doi.org/10.26583/bit.2023.1.07.

15. Лебедев В.Р., Певцов Е.Ф., Деменкова Т.А., Малето М.И., Филимонов В.В. Метод исследования реализации физически неклонируемых функций в информационных системах. International Journal of Open Information Technologies. 2024, № 1. URL: https://cyberleninka.ru/article/n/metod-issledovaniya-realizatsii-fizicheski-nekloniruemyh-funktsiy-v-informatsionnyh-sistemah (дата обращения: 20.09.2024).

REFERENCES:

[1] Joshi S., Mohanty S.P. and Kougianos E. Everything You Wanted to Know About PUFs. IEEE Potentials, v. 36, no. 6, p. 38–46, 2017. DOI: 10.1109/MPOT.2015.2490261.

[2] Blaise Gassend, Dwaine Clarke, Marten van Dijk, and Srinivas Devadas. 2002. Silicon physical random functions. In Proceedings of the 9th ACM conference on Computer and communications security (CCS '02). Association for Computing Machinery, New York, NY, USA, 148–160. DOI: https://doi.org/10.1145/586110.586132.

[3] Korotaev Yu.A., Pevtsov E.Ph. Physically unclonable functions based on vlsi variations of via formation. Advanced Materials and Technologies (AMT-2024): Proceedings of the International Scientific and Technical Conference IPTIP RTU MIREA, Moscow, 12–16 april 2024. M.: MIREA – Russian Technological University. 2024, p. 318–324. – EDN: YQTIRS (in Russian).

[4] Ulrich Rührmair, Frank Sehnke, Jan Sölter, Gideon Dror, Srinivas Devadas, and Jürgen Schmidhuber. 2010. Modeling attacks on physical unclonable functions. In Proceedings of the 17th ACM conference on Computer and communications security (CCS '10). Association for Computing Machinery, New York, NY, USA, p. 237–249. DOI: https://doi.org/10.1145/1866307.1866335.

[5] Korotaev Yu.A. Optical physically unclonable functions. Optical Technologies, Materials, and Systems (OptoTech-2023): Proceedings of the International Scientific and Technical Conference, Moscow, December 11–15, 2023. M.: MIREA - Russian Technological University. 2023, p. 439–445. – EDN PTVUCX (in Russian).

[6] Korenda A.R., Afghah F., Cambou B. and Philabaum C. A Proof of Concept SRAM-based Physically Unclonable Function (PUF) Key Generation Mechanism for IoT Devices. 16th Annual IEEE International Conference on Sensing, Communication, and Networking (SECON), Boston, MA, USA. 2019, p. 1–8. DOI: 10.1109/SAHCN.2019.8824887.

[7] Rührmair U., Sölter J., Sehnke F., Xu X., Mahmoud A., Stoyanova V., Dror G., Schmidhuber J., Burleson W., & Devadas S. (2013). PUF Modeling Attacks on Simulated and Silicon Data. Cryptology ePrint Archive, Paper 2013/112. URL: https://eprint.iacr.org/2013/112 (accessed: 15.09.2024).

[8] The Interpose PUF: Secure PUF Design against State-of-the-art Machine Learning Attacks. (2019). IACR Transactions on Cryptographic Hardware and Embedded Systems. 2019(4), p. 243–290. DOI: https://doi.org/10.13154/tches.v2019.i4.243-290.

[9] Majzoobi Mehrdad & Koushanfar Farinaz & Potkonjak Miodrag. (2008). Lightweight secure PUFs. P. 670–673. DOI: 10.1109/ICCAD.2008.4681648.

[10] Wisiol R., Rührmair U., & Paar C. (2021). Breaking XOR Arbiter PUFs Using Convolutional Neural Networks. In Proceedings of the 30th USENIX Security Symposium (p. 1773–1790). URL: https://ia.cr/2021/555 (дата обращения: 15.09.2024).

[11] Santikellur Pranesh, Aritra Bhattacharyay and Rajat Subhra Chakraborty. Deep Learning based Model Building Attacks on Arbiter PUF Compositions. IACR Cryptol. ePrint Arch. 2019 (2019): 566. URL: https://eprint.iacr.org/2019/566.pdf (accessed: 15.09.2024).

[12] Wisiol N., Grabnitz C., C. Muhl, B. Zengin, T. Soroceanu, and N. Pirnay, pypuf: Cryptanalysis of Physically Unclonable Functions, june 2020. DOI: https://doi.org/10.5281/zenodo.3904267.

[13] Yarmolik V.N., Ivaniuk A.A. Symmetric physically unclonable functions of the arbiter type. Informatics. 2024;21(1):9-27. DOI: https://doi.org/10.37661/1816-0301-2024-21-1-9-27 (in Russian).

[14] Yarmolik Vyacheslav N.; Ivaniuk Alexander A. Balanced arbiter physical uncloneable functions. IT Security (Russia), [S.l.], v. 30, no. 1, p. 92–107, 2023. ISSN 2074-7136. DOI: http://dx.doi.org/10.26583/bit.2023.1.07 (in Russian).

[15] Lebedev V.R., Pevtsov E.Ph., Demenkova T.A., Maleto M.I., Filimonov V.V. Method for studying the implementation of Physical Unclonable Function in information systems. International Journal of Open Information Technologies. 2024, № 1. URL: https://cyberleninka.ru/article/n/metod-issledovaniya-realizatsii-fizicheski-nekloniruemyh-funktsiy-v-informatsionnyh-sistemah (accessed: 20.09.2024) (in Russian).

*Статья поступила в редакцию 29.10.2024; одобрена после рецензирования 18.12.2024;*
*принята к публикации 28.12.2024*
*The article was submitted 29.10.2024; approved after reviewing 18.12.2024;*
*accepted for publication 28.12.2024*