КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 2 (26), 2024
ISSN 2663 - 4023
DOI 10.28925/2663-4023.2024.26.674
УДК 004.8+519.1+519.2

Сюе Цзян
аспірант
Університет Бенгбу, Бенгбу, провінція Аньхой, Китай
Національний університет біоресурсів і природокористування України, Київ, Україна
ORCID ID: 0009-0000-1676-2331
jx1283@163.com

Лахно Валерій Анатолійович
д.т.н., професор, професор кафедри комп'ютерних систем, мереж та кібербезпеки
Національний університет біоресурсів і природокористування України, Київ, Україна
ORCID ID: 0000-0001-9695-4543
lva964@nubip.edu.ua

Сагун Андрій Вікторович
к.т.н., доцент, доцент кафедри комп'ютерних систем, мереж та кібербезпеки
Національний університет біоресурсів і природокористування України, Київ, Україна
ORCID ID: 0000-0002-5151-9203
a.sagun@nubip.edu.ua

Мамченко Сергій Миколайович
д.п.н., професор, професор кафедри комп'ютерних систем, мереж та кібербезпеки
Національний університет біоресурсів і природокористування України, Київ, Україна
ORCID ID: 0009-0006-8743-5606
s.mamchenko@nubip.edu.ua

РОЗРОБКА СИМЕТРИЧНОГО КРИПТОГРАФІЧНОГО ДИФЕРЕНЦІЙНОГО РОЗРІЗНЮВАЧА НА ОСНОВІ ГЛИБОКОГО НАВЧАННЯ

Анотація. Дослідження в галузі криптоаналізу демонструють, що диференційні розрізнювачі (ДР), основані на нейронних мережах (НМ), значно перевершують традиційні методи в виявленні слабкостей простих алгоритмів шифрування. Це пов'язано з їх здатністю виявляти складні патерни в даних, які можуть залишатися непоміченими для класичних підходів. Однак, попри їхньої високої продуктивності, існують обмеження щодо точності розрізнення та максимального числа раундів, яке можливо скомпрометувати для певних шифрів. Мета даного дослідження полягає в подоланні зазначених недоліків шляхом оптимізації архітектури НМ та структури вхідних даних, відповідно до моделі Гора (Gohr). У рамках цієї роботи було вдосконалено кілька ключових компонентів ДР: модуль згортання, залишковий модуль та модуль прогнозування. Оптимізація цих компонентів дозволила значно підвищити ефективність у розпізнаванні диференційних патернів у шифротекстах. Крім того, особлива увага була приділена оптимізації структури вхідних даних, що дало змогу точніше ідентифікувати характеристики шифротексту та інформацію про структуру шифрування. Результати дослідження, проведеного на прикладі криптоаналізу шифру Speck32/64, підтверджують досягнуті вдосконалення: точність роботи ДР зросла на 5–7 раундів, а можливість розпізнавання була розширена до 8 раундів шифру. Ці досягнення свідчать про високу ефективність запропонованого підходу, який має значний потенціал для подальших досліджень у сфері криптоаналізу. У зв'язку з важливістю безпеки інформаційних систем, результати цього дослідження можуть суттєво вплинути на розвиток нових методів криптоаналізу та вдосконалення алгоритмів шифрування, що, своєю чергою, може призвести до підвищення надійності захисту даних у сучасному цифровому середовищі.

Ключові слова: глибоке навчання; криптоаналіз; модель Гора; симетричний криптографічний диференційний розрізнювач (ДР); Speck32/64.

ВСТУП

У сучасному світі зростаюча потреба в надійних механізмах захисту інформації вимагає постійного вдосконалення криптографічних алгоритмів. Проте, з розвитком технологій, з'являються нові методи атаки, які ставлять під загрозу безпеку наявних систем. Однією з актуальних проблем у сфері криптоаналізу є розробка ефективних ДР, здатних виявляти слабкості шифрів. Традиційні методи, хоча й демонструють певну ефективність, часто не можуть конкурувати з новітніми підходами, зокрема тими, що ґрунтуються на використанні НМ. Останні дослідження [1] – [10] виявили, що НМ здатні забезпечити значні переваги в точності та швидкості виявлення криптографічних слабкостей. Однак теперішні моделі стикаються з обмеженнями, пов'язаними з точністю розрізнення та кількістю раундів, які можливо компрометувати. У зв'язку з цим, актуальним стає питання оптимізації архітектури НМ і структури вхідних даних, що можуть суттєво підвищити ефективність ДР.

Мета дослідження полягає у підвищенні ефективності та практичній застосовуванності ДР з використанням методів, в яких використовується НМ з глибоким навчанням. Для чого доцільно зосередитись на двох ключових питаннях: моделі архітектури та форматі вхідних даних.

Аналіз останніх досліджень і публікацій. На конференції US Secret у 2019 році Гор [1] (Gohr) представив новий підхід до криптоаналізу із застосуванням НМ з глибоким навчанням. Його метою було покращення криптоаналізу за допомогою здатності машинного навчання у розпізнаванні патернів, що може перевершити традиційні методи. Це дослідження надихнуло багатьох криптографів на глибше вивчення даної тематики.

Базуючись на роботі Гора, Баксі (Baksi) [2] змінив структуру вхідних даних від однієї пари шифротексту до кількох пар з однаковим значеннями диференціалів. Застосування цього підходу до великих блокових шифрів, таких як ASCON і KNOT, дало вражаючі результати при їх диференційному аналізі. У дослідженні порівняно ефективність методів MLP, CNN і LSTM для диференційного аналізу та отримано результат, який показав, що метод MLP був найефективнішим. При цьому інші архітектури мали обмеження у точності та швидкості навчання.

Аайюш Джайн (Aayush Jain) [3] далі вдосконалив дослідження Баксі, зберігши початкову структуру вхідних даних та оптимізувавши MLP мережу. Він інтегрував оптимальні вхідні диференціали для шифру PRESENT, що призвело до покращення точності криптоаналізу для 3–5 раундів шифру PRESENT.

Емануеле Белліні (Emanuele Bellini) [5] для надання початкової вибірки при навчанні НМ інтегрував характеристики криптографічного алгоритму до архітектури НМ. Запропонований ДР складався з двох компонентів: розрізнювача і екстрактора ознак. Вхідна пара шифротексту була ним поділена на чотири рівні сегменти, кожен з яких оброблявся двома щільними шарами нейронів в кількості по 32 кожен. Такий підхід мав на меті виділити ознаки диференціалів пар незалежно від результатів кожного блоку шифротексту, мінімізуючи взаємодію між блоками. Це більшою мірою відповідало структурі криптографічного алгоритму. В інших дослідженнях автори використовували MLP-мережу для прогнозування. Вони представили новий нейронний розрізнювач для проведення диференційного аналізу на 4–7 раундах алгоритмів шифрування в алгоритмах TEA і RAIDEN. Такий підхід перевершив продуктивність трьох традиційних ДР. Подальші дослідження здебільшого зосереджувалися на покращенні здатності НМ отримувати попередні криптографічні знання. Наприклад, Ліцзюн Лю (Lijun Lyu) [6]

інтегрував MILP для побудови нейронного ДР. За допомогою попередньо визначеного необхідного значення різниці (δ), використавши MILP, автори оброблювали скорочений шифротекст і виділяли пари шифротекстів з різницею δ, в якості вхідних дантх НМ, що призводило до регулярізації вхідних даних.

Хенг Чуань Су (HengChuan Su) [7] перейшов від незалежних диференційних пар до політопічних диференційних пар, використовуючи політопічні різниці для встановлення тісніших зв'язків між вхідними даними, тим самим дозволяючи НМ виділяти більше ознак в шифротексті. В 2021 році Адріен Бенаміра (Adrien Benamira) [8] проаналізував дослідження Гора з криптоаналізу. У ньому було вперше досліджено принципи роботи нейронного розрізнювача. В 2022 році Хаято Кімура (Hayato Kimura) [9] розшифровував алгоритм низькочастотного шифрування, ітеративно вдосконалюючи ознаки мережі на основі експериментальних результатів по методу атак «білого ящика». На відміну від попередніх досліджень, що проводилися на покращенні структури НМ та вхідних даних, робота Кімури акцентувала увагу на інтерпретованості, вивчаючи процес прийняття рішень НМ з врахуванням криптографічної перспективи.

Наразі ДР на основі НМ продемонстрували значні успіхи у диференційному криптоаналізі різних простих алгоритмів шифрування [10] – [12].

Постановка проблеми. На сьогодні залишаються проблемні питання, включаючи обмежену різноманітність структур НМ, яка залежність від простого зворотного поширення, недостатні дослідження щодо інтеграції попередніх криптографічних знань в архітектуру мережі та обмеження, що накладаються фіксованими характеристиками шифротекстів на різницю в отриманій інформації. Крім того, поточна структура вхідних даних не забезпечує достатньої інформації для повноцінного навчання НМ, а точність ДР в класифікації пар шифротекстів залишається обмеженою.

МЕТОДИКА ДОСЛІДЖЕННЯ

Диференційний криптоаналіз (далі ДКА) є потужною технологією, яка використовується для зламу блокових шифрів. Нейронні мережі можуть покращити ефективність ДКА шляхом автоматизації та покращення процесу виявлення та використання диференційних патернів. Глибоке навчання [15] є технологією машинного навчання, яка базується на штучних НМ (ШНМ), які обробляють та аналізують дані, імітуючи взаємопов'язану структуру та функції людського мозку. Таке навчання добре вирішує такі складні завданнями, як розпізнавання зображень і мови, так і обробку природної мови. В цій області згорткові нейронні мережі (ЗНМ) [16] утворюють важливий напрям, спеціально розроблений для обробки зображень.

У 2015 році Хе Каймінг (He Kaiming) та ін. представили модель ResNet [16] — архітектуру ЗНМ, яка використовує обхідні зв'язки. В такій архітектурі фінальний модуль включає два або більше згорткових рівні нейронів і обхідне з'єднання, яке безпосередньо додає вхідні та вихідні дані, щоб передати вихід неглибокої мережі на глибші рівні, зменшуючи тим самим проблему згасання градієнтів. На рис. 1 показано структуру мережі ResNet. Незважаючи на отримані досягнення, ResNet все ще має можливості для підвищення точності розпізнавання, обчислювальної ефективності та виділення кількості ознак моделі. Дана використовує декілька принципів конструювання залишкових структур для оптимізації архітектури нейронного ДР.

У 2019 році Гор (Gohr) [17] вперше поєднав глибоке навчання з ДА. У цій роботі він запропонував використати метод бінарної класифікації для аналізу пар шифротекстів, базуючись на існуючих методах шифрування алгоритму Speck.

В дослідженні планується створити модель ДР, яка забезпечить розрізнення між реальними та випадковими ознаками шифротексту для випадку вхідної різниці/диференціалу, що дорівнює 0x0040/0000 з високою точністю.

Реальні пари «відкритий текст/закритий» текст походять від пар відкритого тексту з зазначеною різницею, тоді як випадкові пари отримуються з довільних пар відкритого тексту. Розроблена модифікація ДКА застосована до шифру Speck32/64. Завдяки оптимізованій конструкції ДР вона має перевершити традиційні методи ДКА за точністю і може бути застосована також і до інших простих шифрів. В якості НМ ДР взята НМ Гора. Архітектура НМ Гора, показана на рис. 2. Вона складається з чотирьох модулів: 1) вхідного; 2) початкової згортки; 3)залишкового модуля; 4) модуля прогнозування.

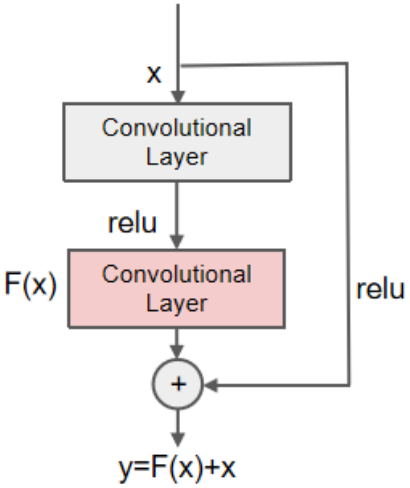

Рис. 1. Структура нейромережі ResNet

Вхідний модуль передає дані шифротексту до модуля згортки, структурованого у вигляді ResNet-мережі з 1×1 згортковими ядрами нейронів. Даний модуль призначений для отримання ознак шифрування. Залишковий модуль покращує отримані ознаки. Для цього даний модуль має десять двозгорткових НМ та залишкові зв'язки, що дозволяє мінімізувати втрати інформації. Модуль прогнозування використовує декілька повнозв'язних рівнів для відображення вхідних ознак на вихідні мітки. Класифікація пар відбувається по типу «справжні»/«випадкові», що зрештою і визначає точність методу.

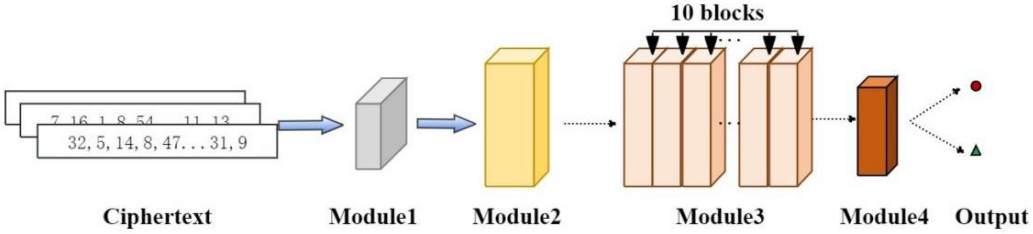

Рис. 2. Структура нейтронної мережі Гора

РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

В запропонованій модифікації для зламу блокового шифру Speck32/64 застосовано вдосконалену архітектуру НМ Гора, що показана на рис. 3. Шифр Speck [13] — це простий блоковий шифр, представлений Рей Больє та іншими розробниками з Національної агенції безпеки (NSA) у червні 2013 року. дослідження зосереджується на варіанті шифру Speck32/64, який використовує блок розміром 32 біти та ключ розміром 64 біти.

Схема вдосконалення описаної моделі заснована на оптимізації та вдосконаленні структури НМ в модулі введення та залишковому модулі (рис. 2). Такі вдосконалення підвищують точність класифікації ДР НМ.

Отже, загальний дизайн схеми базується на оригінальному ДР Гора. Результатом модифікації став більш точний ДР для шифру Speck32/64 у варіанті, що зменшений до 5–7 раундів шифрування. Конкретні вдосконалення детально описані у подальшій частині статті, де також отримано показники точності диференційної класифікації для 5–7 раундів алгоритму шифрування Speck. Це зроблено для перевірки оптимізації і стратегії вдосконалення. Після визначення оптимальної структури ДР, структура вхідного шифротексту додатково оптимізована для покращення продуктивності даного ДР.

З метою забезпечення коректного та послідовного експерименту середовище, набір даних і гіперпараметри залишаються фіксованими протягом усього дослідження. Крім того, ознаки випадкових даних при класифікації НМ стабілізується для зменшення впливу на результати експериментів можливих похибок при обробці числових значень з плаваючою точкою.

Параметри НМ при проведенні експерименту. Тренування НМ відбувалося на навчальному наборі даних протягом 200 раундів. Розмір пакету з навчальною вибіркою становив 5000. Для оптимізації функції втрат перехресної ентропії використовувався алгоритм Adam з параметрами за замовчуванням, заданих у Keras із невеликим штрафом для регуляризації ваг шару нейронів L2 (параметр регуляризації $c = 10^{-5}$). Параметром швидкості навчання НМ є циклічна швидкість навчання з початковою для параметру $epoch_i$, встановленою відповідно виразу: l_i *для* $epoch_i$ *розуміється як* $l_i=(((n-1)\cdot mod(n+1))\div n)\cdot(\beta-\alpha)$, *де* $\alpha=10^{-4}$, $\beta=2\cdot10^{-3}$, $n=9$.

В кінці кожного раунду навчання отримана мережа зберігалася, а найкраща навчена мережа оцінювалася на основі тестового набору даних (вибірки).

Генерування даних. У даному дослідженні використано генератор випадкових чисел ОС Linux з фіксованою випадковою генерацією для генерування потрібного ключа та 10^7- 10^6 навчальних і тестових наборів даних відповідно. Диференціал з фіксованої пара шифротекстів отримується шляхом шифрування пари відкритих текстів із різницею (0×0040, 0x×0000) для n раундів, тоді як випадкова пара шифротекстів шифрується ознаками відкритих текстів із рівномірним розподілом. Мітка Y фіксованого шифру різниці позначається, як «1», випадковий шифр — як «0».

Витрати на тренування моделі. Відповідно до наведеної вище базової програми навчання в тренувальній виборці розміром 5000 значень один раунд навчання на одному графічному адаптері GTX 3090 займає близько 90 секунд. Тому, повний цикл навчання НМ можна завершити менше ніж за одну добу.

Подальші вдосконалення модуля залишків на основі ідеї уваги полягають у наступному: відповідно до структури НМ Гора, модуль залишків ДР складається з кількох взаємозв’язаних модулів залишкової мережі (залишкових веж). Вихід кожної залишкової вежі додається до вхідних даних наступної вежі, утворюючи залишкове

ISSN 2663 - 4023

з’єднання. Для п’яти та шести раундів шифрування Speck стандартна модель ДР використовує НМ з глибиною десять шарів (десять залишкових веж) у залишковому модулі для оптимізації продуктивності розрізнення. Виходячи з цього факту, дана робота досліджує різні вдосконалення архітектури залишкового модуля, а саме:

1) досліджується кількість згорткових рівнів усередині залишкової вежі, а в якості тестових об’єктів обираються залишкові структури з 2, 3 і 4 одно-вимірними згортковими рівнями шарів нейронів розмірністю 3×3. До кожного згорткового рівня додаються функція нормалізації пакету та функція активації нейронів ReLU, а три нові ДР позначимо послідовно, як: S1, S2 і S3. Шість структур залишкових веж показано на рисунку 3 (a), (b) та (c).
2) Посилений архітектурою SENet, новий модуль вилучення уваги каналів був інтегрований у залишкову вежу, поєднуючи три згадані структури та механізм уваги [18]. Залишкова вежа після обробки даних шифротексту об’єднує вихідні дані своїх згорткових рівнів. Це перетворення трансформує початкову двовимірну структуру шифротексту в тривимірне представлення. Після цього об’єднані дані групуються по різних каналах (виходи окремих згорткових рівнів шарів нейронів), а потім, на основі згорткової НМ проводиться навчання та визначення ознак класифікації. Отримані ваги нейронів множаться на початкові об’єднані дані, а додавання каналів відновлює двовимірну структуру без зміни загального обсягу даних. Завдяки інтеграції цього модуля були отримані три нові варіанти мережі під назвами: SENet-S1, SENet-S2 і SENet-S3. Вони інтегровані в три початкові залишкові структури, як це показано на рис. 3 (d), (e) та (f).

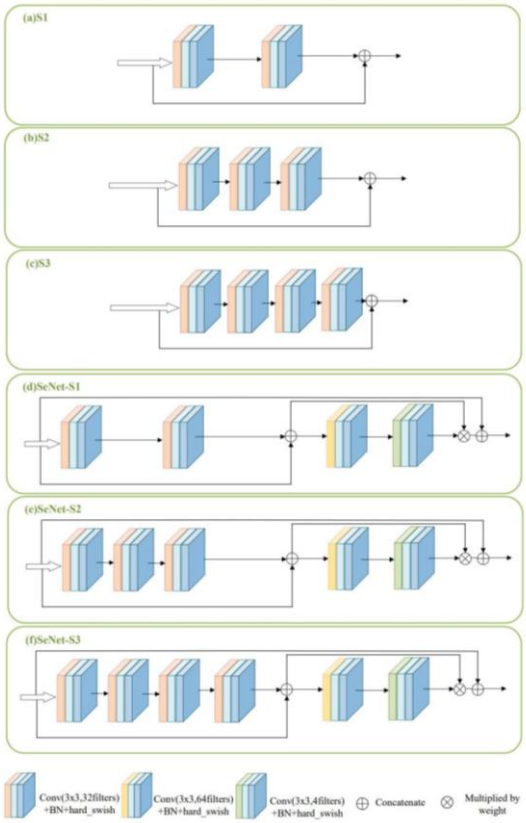

Рис. 3. Шість структур залишкових веж

Робота шість залишкових архітектур були проаналізовані при роботі п’яти раундів пар шифротекстів алгоритму Speck, а результати цього аналізу наведені в табл. 1.

Результати експериментів показують, що варіант мережі SENet-S2 демонструє оптимальні результати в операціях згортки. Завдяки покращенню представлення ознак, введенню автоматизованого навчання та визначення ваг, оптимізації потоку градієнтів, зменшенню надлишковості ознак, інтеграції локальних ознак та підвищенню стабільності НМ, дана модель суттєво перевершує своїх попередників за показником точності.

Таблиця 1

Точність різних ДР із вдосконаленою моделлю

Структура мережі	Глибина мережі	Точність
S1	10	92.95%
S2	10	92.95%
S3	10	92.92%
SENet-S1	10	93.01%
SENet-S2	10	93.04%
SENet-S3	10	93.00%

Експериментальні результати вказують, що трирівнева згортка досягає ідеального балансу між вилученням ознак, вибором, поширенням градієнтів, зменшенням надлишковості, інтеграцією локальних ознак і гнучкістю моделі, перевершуючи як дворівневі, так і чотирирівневі конфігурації шарів нейронів НМ. Ця рівновага дозволяє моделі ефективно вловлювати складні ознаки, зберігаючи обчислювальну ефективність, що призводить до покращення точності класифікації ознак.

Таким чином встановлено ефективність механізмів уваги у покращенні точності мережі. На основі цього можна виділити додаткові ознаки та вдосконалити модуль механізму уваги для посилення ознак різниць пар. З цією метою у залишкову структуру НМ введено гілку зі згортковим рівнем, що реалізує глибше визначення ознак. Це дозволяє моделі навчатися на основі більш широкого та високорівневневого представленням даних, що є вирішальним фактором для обробки складних і детальних патернів шифротексту. За рахунок інтеграції кількох згорткових рівнів, створена модель може обробляти ознаки на різних масштабах. Водночас, необхідно дослідити оптимальну структуру навчання ваг у модулі уваги, порівнюючи методи MLP і CNN для визначення ознак і налаштування НМ.

Розширюючи найкращу отриману модель НМ SENet-S2, додаємо шар, що містить один згортковий рівень шарів нейронів, крім існуючої трирівневої згортки. Виходи обох шарів об’єднуються, після чого обчислюються і застосовуються обраховані ваги нейронів. Отримана гілка складається з одновимірного згорткового рівня нейронів з ядром розміром 3, доповненого нормалізацією пакету та функцією активацією нейронів ReLU. На рис. 6 показано архітектуру одновимірного згорткового рівня. Крім того, проведені експерименти з різними структурами навчання ваг і кількістю нейронів, а результати цих експериментів наведені в табл. 2.

Результати експериментів, наведені в табл. 2 демонструють, що включення древовидних структур до НМ значно покращує продуктивність роботи згорткових мереж, особливо у варіанті з меншою кількістю нейронів (наприклад, 32, 4 тощо). У цих експериментах згорткові мережі в більшості випадків перевершували за точністю ті мережі, що збудовані на базі методу MLP.

Таблиця 2

Порівняння точності різних ДР із вдосконаленою моделлю

Структура мережі	Додаткова гілка	Структура, використана для навчання ваг	Кількість нейронів на рівень	Точність
NoBranch-MLP1(SENet-S3)	НІ	MLP	64, 3	93.04%
NoBranch-MLP2	НІ	MLP	32, 3	93.01%
NoBranch-CNN1	НІ	Згортка	64, 3	93.07%
Branch-MLP1	ТАК	MLP	64, 4	93.09%
Branch-CNN1	ТАК	Згортка	128, 4	93.09%
Branch-CNN2	ТАК	Згортка	256, 4	93.07%
Branch-CNN3	ТАК	Згортка	32, 4	93.11%

Збільшення ширини НМ виявилося для задачі криптоаналізу Speck ефективнішим, ніж збільшення ширини при захопленні характеристик вхідних даних. Це призвело до покращення продуктивності моделі в цілому. Більш широкі НМ досягають більшої ємності представлення з меншою кількістю шарів нейронів, зменшуючи проблему згасання градієнта та навчання, які пов'язані з НМ з глибоким навчанням. Спільне згорткове ядро в згорткових рівнях ДР ефективно виявляло патерни у всьому вхідному потоці, покращуючи узагальнення моделі та розпізнавання ознак. Отже, додавання варіантів стає цінною стратегією оптимізації НМ.

Аналіз результатів експериментів з архітектурою побудови ДР дозволив зосередити увагу на покращенні функції активації нейронів НМ. Функції активації та нормалізації є важливими компонентами НМ. Вони підвищують їх експресивність, точність прогнозування, стабільність і швидкості збіжності. Це досягається завдяки вдосконаленням ДР, які можливі завдяки дослідженням функції активації, методам нормалізації та їхньому застосуванні в НМ.

Залишкові структури зазвичай націлені на отримання числових результатів в певному інтервалі в «залишковому» варіанті. Однак, використання функції активації нейронів ReLU в кінці цієї гілки нейронів призводить до невід'ємного зростання «залишкових» значень, що може вплинути на потужність представлення.

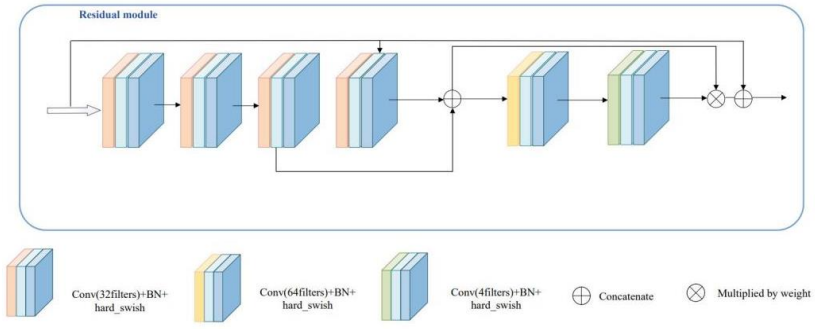

Рис. 4. Структура мережі Branch-CNN3

Щоб вирішити цю проблему, було змінено розташування функції активації. В деяких випадках заміні піддавалася функція активації ReLU на Swish, LeakyReLU або інші альтернативні варіанти. В табл. 3 показані конкретні результати тестів для п'яти раундів пар шифротекстів алгоритму Speck. Результати активації при заміні на фінальному раунді функції ReLU на Hard-swish представлені на рис. 5.

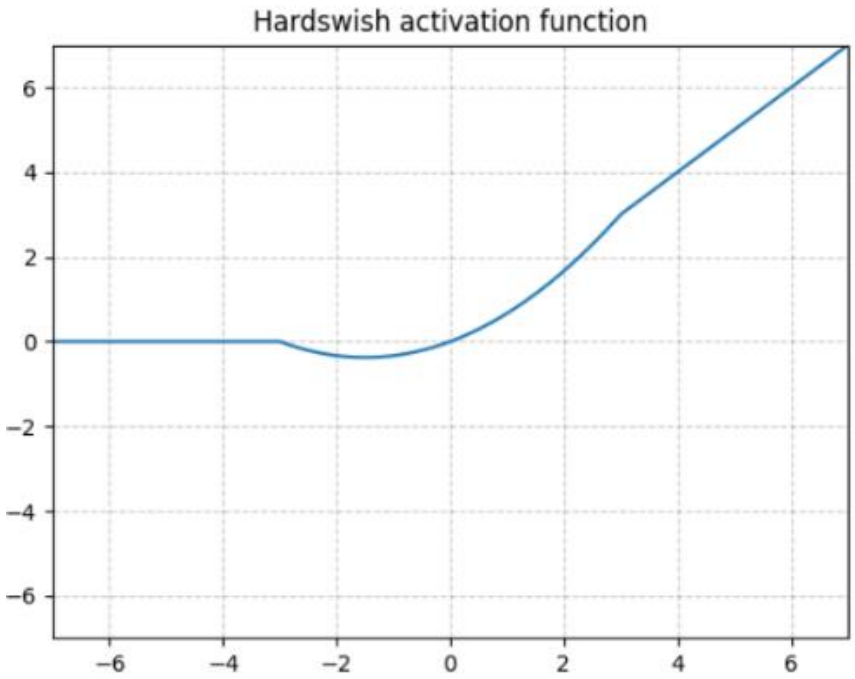

Рис. 5. Результати активації при використанні функції активації Hard_swish

Нормалізація може покращити стабільність і швидкість збіжності моделі НМ та зменшити ризик перенавчання. Після порівняння і аналізу експериментів було виявлено, що техніка активації BatchNorm, яка використовується в ДР цього експерименту, є оптимальним рішенням на поточний момент. Тому, BatchNorm і використовується для ДР в цьому дослідженні. Порівняння результатів тестування навченої моделі на базі НМ показано в табл. 3.

Як видно з табл. 3, дослідження, зосереджені на вдосконаленні нейронного ДР шляхом вдосконалення функції активації та нормалізації в початковому згортковому модулі, залишковому модулі та модулі прогнозування є потенційно вірними з огляду на покращення показників точності ДР.

Застосування функцій активації, таких як Hard_swish і GeLU, замість функції ReLU дає кращі результати точності розрізнення ознак. Крім того, метод нормалізації суттєво впливає на продуктивність функції активації Hard_swish, при цьому техніка активації BatchNorm перевершує за показниками метод LayerNorm та інші альтернативи.

Таким чином, розроблена модифікація НМ для криптоаналізу шифру Speck, що містить функцію ReLU замість Hard_swish у початковому згортковому модулі, залишковому модулі та модулі прогнозування архітектури Branch-CNN3, зберігаючи при цьому метод нормалізації BatchNorm. На рис. 6 показано загальну структуру отриманого оптимізованого ДР.

На етапі порівняльного аналізу точності різних варіантів ДР загальний ДР отримав назву B-C3-HSwish. Схему його деталізованої архітектури наведено на рис. 7. Він використовується для розрізнення для 5–7 раундів алгоритму шифрування Speck. Результати порівняння показників роботи створеного ДР B-C3-HSwish із існуючими ДР представлено в табл. 4.

Таблиця 3

Порівняння результатів точності ознак точності ДР за різних функцій активацій нейронів

Функція активації	Нормалізація	Точність
RelU	BatchNorm	93.11%
PRelu	BatchNorm	93.06%
Swish	BatchNorm	93.14%
GelU	BatchNorm	93.14%
ELU	BatchNorm	93.06%
SelU	BatchNorm	92.99%
LeakyRelU (0.3)	BatchNorm	92.96%
Hard_swish	BatchNorm	93.16%
Hard_swish	LayerNorm	92.91%
Hard_swish	InstanceNorm	92.63%

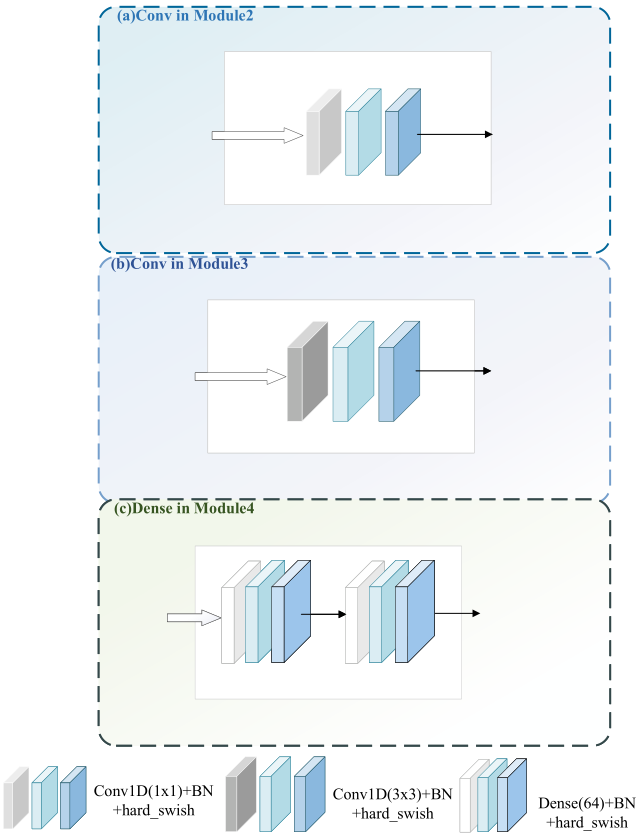

Рис. 6. Покращення функції активації та нормалізації для Branch-CNN3 в оптимізованому ДР

На рис. 7 помітні відмінності між моделями ДР для 7 раундів та 5 або 6 раундів. Основна увага в перших з них приділяється модулю навчання ознак з увагою, що використовує двошарову НМ на основі MLP-архітектури з 64 і 4 нейронами, а загальна модель використовує функцію активації нейронів Swish.

Як показано в експериментальних результатах таблиці 4, модель B-C3-HSwish перевершує в точності інші моделі в усіх раундах, що означає її високу здатність розрізняти пари при шифруванні Speck32/64. Ця модель не тільки досягає високої точності на початкових раундах (наприклад, п’ятому раунді), але й зберігає постійну високу точність роботи у старших раундах (шостому і сьомому).

Для порівняння, модель Goh19 займає друге місце в кожному раунді, тоді як модель CSYY22, хоча й має меншу точність, ніж перші дві, перевершує в точності традиційний ДР, особливо на результатах шифрування в старших раундах. Традиційний ДР, особливо в сьомому раунді, демонструє найгірші результати, що підкреслює його обмеження в обробці складних (багатораундових) режимах шифрування.

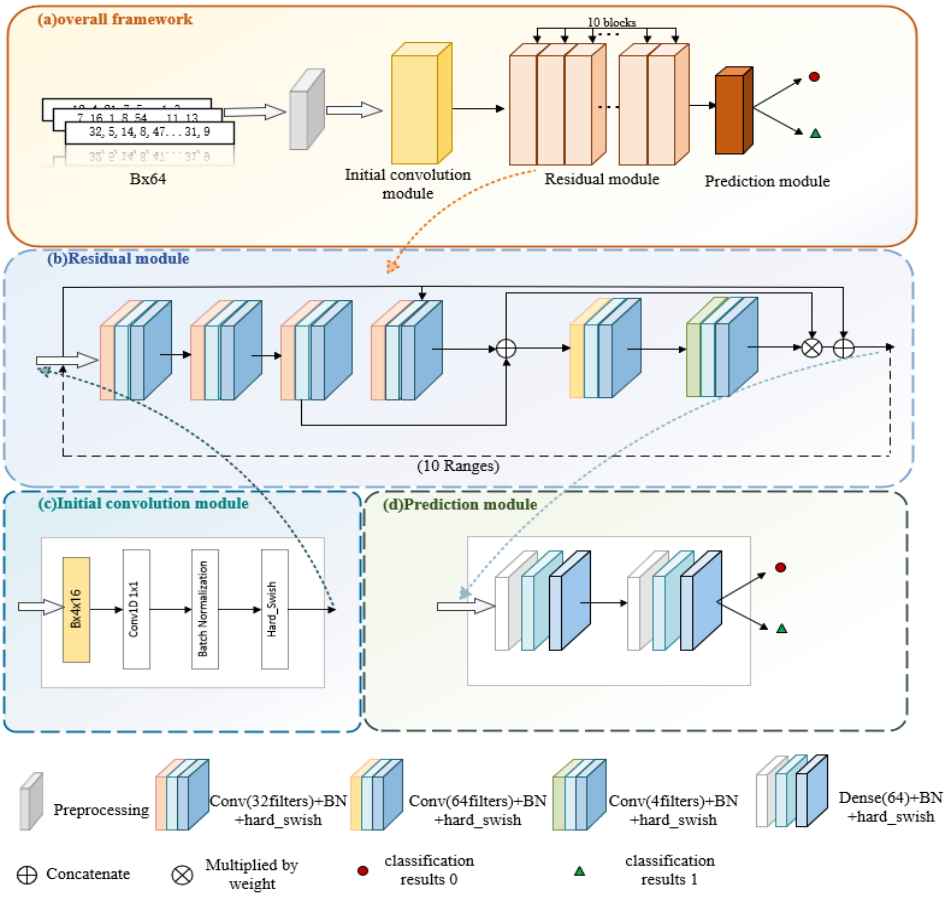

Рис. 7. Деталізована схема архітектури ДР B-C3-HSwish

Таблиця 4

Порівняння результатів точності ДР

Раунд Speck32/64	Нейронний розрізнювач	Точність
5	D5*[17]	91.1%
	CSYY22[11]	92.6%
	Goh19[17]	92.9%
	B-C3-Hswish	93.2%
6	D6[17]	75.8%
	CSYY22[11]	78.4%
	Goh19[17]	78.8%
	B-C3-HSwish	79.0%
7	D7[17]	59.1%
	CSYY22[11]	60.7%
	Goh19[17]	61.6%
	B-C3-HSwish	61.7%

**D — позначається традиційний ДР.*

Таким чином, виняткова здатність і стійкість моделі B-C3-HSwish до розрізнення робить її оптимальним вибором в якості ДР для алгоритму шифрування Speck32/64.

На основі отриманих результатів проведемо вдосконалення вхідного модуля ДР. Експерименти, проведені в ході виконання дослідження показали, що модифікація архітектури нейронного розрізнювача може значно покращити точність диференційного розрізнення. Однак, також було виявлено, що тільки оптимізація структури НМ недостатня для результативних диференційних атак на старші раунди шифру. Для того, щоб ще більше підвищити точність і загальну продуктивність моделі, далі зосередимся на оптимізації вхідного набору даних. Маніпулюючи структурою набору даних, наприклад, об'єднуючи кілька пар шифротекстів, НМ може потенційно виділити більше інформації про шифротекст та структурні характеристики функції шифрування. Це призводить до підвищення якості і різноманітності вхідних даних, що в свою чергу підвищує здатність моделі до узагальнення, ефективності навчання та загальної продуктивності.

В існуючих на сьогодні роботах, наприклад, в роботі Чень І (Chen Yi) [20], досліджено використання об'єднання кількох пар шифротекстів (MCP) в якості вхідних даних замість використання однієї пари шифротекстів. Такий підхід продемонстрував можливість підвищення точності ДР, тим самими дозволяючи моделі тримати та вивчити більше інформації про ознаки вхідного шифротексту. Однак, оптимальна кількість пар шифротекстів в роботі була обмежена кількістю 16, а збільшення цього числа призводило до зниження точності, що і показано в роботі [20]. Інші науковці, включаючи Хоу Цзезоу (Hou Zezhou) та Лю Цзяшуо (Liu Jiashuo) [21], досліджували використання значень різниць шифротекстів або шифрування шифротекстів на один раунд в якості вхідних даних (MOD) для того, щоб досягти кращих результатів розрізнення.

Спираючись на попередні дослідження, в даній роботі було прийнято рішення покращити структуру вхідного шифротексту. Для цього було використано кілька пар відкритих текстів: p1, p2, ..., p32 і після їхнього шифрування протягом одного раунду випадковим ключем були отримано шифротексти: c1, c2, ..., c32. Значення різниць цих кількох пар відкритих текстів і шифротекстів разом зі значеннями різниць: d1, d2, ..., d32 після одного раунду шифрування використовувалися в якості навчальних даних для тренування НМ. Далі вони ж вводяться в нейронний ДР. Така модель отримала назву RSCE (шифрування одноразундового шифру з випадковим ключем), а її структурна схема показана на рис. 8.

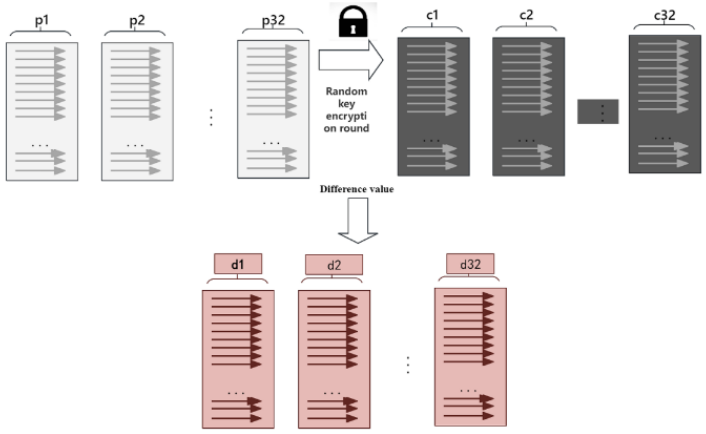

Рис. 8. Нова структура вхідних даних RSCE (в процесі шифрування одноразундового шифру)

Запропонована структура вхідних даних RSCE вирішує проблему зниження точності, що виникає при використанні більш ніж 16 пар шифротекстів. Результати проведених експериментів показують, що така структура досягає найвищої точності при застосуванні від 17 до 32 пар шифротекстів, що видно з даних, наведених в табл. 5.

В цьому експерименті структура RSCE використовує розрізнювач Гора. Як показано в табл. 5, в експериментах з класифікації ознак НМ, які орієнтовані на 7 та 8 раундів пар шифрованих шифротекстів Speck, RSCE постійно перевершувала найкращі результати класифікації по параметру точності для 7-и та 8-раундових класифікацій в шифруванні, ніж ті, що досягнуті з використанням структур MCP і MOD.

Помітно, що в експерименті на 7 раундів шифрування структура RSCE продемонструвала виняткову продуктивність з рівнем покращення, що досягає 36.32%. Однак, зі збільшенням кількості раундів шифрування ефективність усіх методів значно знижується. Щоб підтвердити підвищену продуктивність нової структури RSCE для шифротексту у поєднанні з новим ДР B-C3-HSwish, було проведено експеримент з порівняння по точності, результати якого представлені в табл. 6.

Таблиця 5

Результати порівняння точності розрізнення

Раунд Speck32/64	Структура шифротексту	Точність
7	MCP[20]	66.94%
	MOD[21]	88.19%
	RSCE	91.25%
8	MCP[20]	Неможливо атакувати
	MOD[21]	56.49%
	RSCE	63.01%

Таблиця 6

Тести ДР B-C3-HSwish у поєднанні з новою структурою шифротексту RSCE

Раунд Speck32/64	Структура шифротексту	Нейронний розрізнювач	Точність
7	RSCE	Ghor[17]	91.25%
	RSCE	B-C3-HSwish	92.03%
8	RSCE	Ghor[17]	63.01%
	RSCE	B-C3-HSwish	63.32%

Результати показують, що ДР B-C3-HSwish перевершує в точності визначення ДР на базі НМ Goh у різних раундах, що підтверджує припущення, що структура шифротексту RSCE у поєднанні з розрізнювачем B-C3-HSwish є оптимальним поєднанням.

РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

Як показано вище, НМ можуть з успіхом використовуватися для заміни традиційних ДР при класифікації пар шифротекстів. Як видно з проведених досліджень традиційні ДР на основі НМ мають кілька значних обмежень, що характеризуються низькою точністю класифікації та обмеженою кількістю розпізнаваних раундів шифрування. Щоб вирішити вказані проблеми, в роботі зосереджується увага на двох

ключових аспектах: розробці архітектури нейронної мережі для ДР та розробці покращеної структури вхідного шифротексту. Так само важливим для підвищення точності ДР, що використовує НМ є вибір оптимальної функції активації нейронів.

ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ.

На основі накопиченого досвіду та існуючих структур НМ було оптимізовано архітектуру НМ. Для цього вдосконалено початкові згортуові модулі, залишкові модулі, обрано оптимальну функцію активації та функції нормалізації в структурі ДР. Крім того, запропонувано нову структуру вхідних даних, яка є оптимізацією структури вхідного шифротексту, що дозволяє НМ захопити більше ознак шифротексту та інформації про структуру шифрування. Проведені вдосконалення призвели до створення більш продуктивного і точного ДР, який досяг точності розрізнення в 92.03% при 7 раундах шифрування блокового шифру SPECK32/64. Крім того, кількість розпізнаваних раундів була розширена до 8, а точність за такої кількості раундів склала 63.32%, що перевершує результати, отримані з використанням існуючих відомих методів (наведено в [20] – [22]) за точністю класифікації. Результати симуляції в ході обчислювальних експериментів підтверджують ефективність і перевагу архітектури ДР на базі НМ з глибоким навчання, запропонованим в цій роботі. В якості можливих подальших напрямків можна розглянути експериментування з функціями активації нейронів на більшій за 8 раундах шифрування та оптимізацію формат вхідних даних, накопичуваних для навчання моделі мережі.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Gohr, A. (2019). Improving attacks on round-reduced Speck32/64 using deep learning. In: *Advances in Cryptology – CRYPTO 2019. LNCS, vol. 11693,* 150–179. https://doi.org/10.1007/978-3-030-26951-7_6
2. Baksi, A., et al. (2020). Machine Learning Assisted Differential Distinguishers for Lightweight Ciphers (Extended Version). In: *Classical and Physical Security of Symmetric Key Cryptographic Algorithms. Computer Architecture and Design Methodologies,* 141–162. https://doi.org/10.1007/978-981-16-6522-6_6
3. Jain, A., Kohli, V., & Mishra, G. (2020). Deep learning based differential distinguisher for lightweight cipher PRESENT. *Cryptology ePrint Archive.*
4. Wang, M. (2008). Differential cryptanalysis of reduced-round PRESENT. In: *Cryptology – AFRICACRYPT 2008. AFRICACRYPT 2008. Lecture Notes in Computer Science, vol. 5023,* 40–49. https://doi.org/10.1007/978-3-540-68164-9_4
5. Bellini, E., & Rossi, M. (2021). Performance comparison between deep learning-based and conventional cryptographic distinguishers, *Intelligent Computing, LNNS, vol. 285,* 681–701. https://doi.org/10.1007/978-3-030-80129-8_48
6. Lyu, L., Tu, Y., & Zhang, Y. (2022). Improving the Deep-Learning-Based Differential Distinguisher and Applications to Simeck. In: *IEEE 25th International Conference on Computer Supported Cooperative Work in Design (CSCWD),* 465–470. https://doi.org/10.1007/978-3-030-80129-8_48
7. Su, H. C., Zhu, X. Y., & Ming, D. (2021). Polytopic attack on round-reduced simon32/64 using deep learning. *International Conference on Information Security and Cryptology. LNCS, vol. 12612,* 3–20. https://doi.org/10.1007/978-3-030-71852-7_1
8. Benamira, A., Gerault, D., Peyrin, T., & Tan, Q. Q. (2021). A Deeper Look at Machine Learning-Based Cryptanalysis. *Advances in Cryptology – EUROCRYPT 2021. EUROCRYPT 2021, LNCS, vol. 12696,* 805–835. https://doi.org/10.1007/978-3-030-77870-5_28
9. Sun, L., Gerault, D., Benamira, A., & Peyrin, T. (2020). Neurogift: Using a machine learning based sat solver for cryptanalysis. In: *Cyber Security Cryptography and Machine Learning: Fourth International Symposium, CSCML 2020, LNCS, vol. 12161,* 62–84. https://doi.org/10.1007/978-3-030-49785-9_5
10. Hou, Z., Ren, J., & Chen, S. (2021). Cryptanalysis of round-reduced SIMON32 based on deeplearning. *Cryptology ePrint Archive*.

11. Chen, Y., Shen, Y., Yu, H., & Yuan, S. (2023). A New Neural Distinguisher Considering Features Derived from Multiple Ciphertext Pairs. *The Computer Journal, 66(6),* 1419–1433. https://doi.org/10.1093/comjnl/bxac019
12. Rajan, R., et al. (2022). Deep Learning-Based Differential Distinguisherfor Lightweight Cipher GIFT-COFB. Machine Intelligence and Smart Systems: Proceedings of MISS 2021, 397–406. https://doi.org/10.1007/978-981-16-9650-3_31
13. Beaulieu, R., et al. (2015). The SIMON and SPECK families of lightweight block ciphers. *DAC'15: Proceedings of the 52nd Annual Design Automation Conference, 175,* 1–6. https://doi.org/10.1145/2744769.2747946
14. Biham, E., Shamir, A. (1991). Differential cryptanalysis of DES-like cryptosystems. *Journal of CRYPTOLOGY, 4(1),* 3–72.
15. Sarker, I. H. (2021). Deep Learning: A Comprehensive Overview on Techniques, Taxonomy, Applications and Research Directions. *SN Computer Science, 2 (6),* 1–20. https://doi.org/10.1007/s42979-021-00815-1
16. He, K., et al. (2016). Deep residual learning for image recognition. *IEEE Conference on Computer Vision and Pattern Recognition,* 770–778. https://doi.org/10.1109/CVPR.2016.90
17. Gohr, A. (2019). Improving attacks on round-reduced Speck32/64 using deep learning. *CRYPTO 2019, LNCS, vol. 11693,* 150–179. https://doi.org/10.1007/978-3-030-26951-7_6
18. Hu, J., Shen, L., & Sun, G. (2018). Squeeze-and-Excitation Networks. *The Conference on Computer Vision and Pattern Recognition, IEEE,* 7132–7141. https://doi.org/10.1109/CVPR.2018.00745
19. Shalev-Shwartz, S., & Ben-David, S. (2014). Understanding machine learning: From theory to algorithms. *Cambridge university press.*
20. Chen, Y., & Yu, H. (2021). A New Neural Distinguisher Model Considering Derived Features from Multiple Ciphertext Pairs. *The Computer Journal.*
21. Hou, Z., Ren, J., & Chen, S. (2021). Improve neural distinguisher for cryptanalysis. *Cryptology ePrint Archive.*
22. Hulak, H. M., Zhiltsov, O. B., Kyrychok, R. V., Korshun, N. V., & Skladannyi, P. M. (2024). *Information and cyber security of the enterprise.* Textbook. Lviv: Publisher Marchenko T. V.

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 2 (26), 2024
ISSN 2663 - 4023

Xue Jiang
Ggraduate student
Bengbu University, Bengbu City, Anhui Province, China
National University of Life and Environmental Sciences of Ukraine, Kiev, Ukraine
ORCID ID: 0009-0000-1676-2331
jx1283@163.com

Valerii Lakhno
Doctor of Technical Sciences, Professor, Department of
Computer Systems, Networks and Cybersecurity
National University of Life and Environmental Sciences of Ukraine, Kiev, Ukraine
ORCID ID: 0000-0001-9695-4543
lva964@nubip.edu.ua

Andrii Sahun
Associated Professor, Department of Computer Systems and Networks
National University of Life and Environmental Sciences of Ukraine, Kyiv, Ukraine
ORCID ID: 0000-0002-5151-9203
a.sagun@nubip.edu.ua

Sergii Mamchenko
Doctor of Technical Sciences, Professor, Department of
Computer Systems, Networks and Cybersecurity
National University of Life and Environmental Sciences of Ukraine, Kiev, Ukraine
ORCID ID: 0009-0006-8743-5606
s.mamchenko@nubip.edu.ua

DESIGN OF SYMMETRIC CRYPTOGRAPHIC DIFFERENTIAL DISTINGUISHER BASED ON DEEP LEARNING

Abstract. Research in the field of cryptanalysis demonstrates that differential discriminators based on neural networks significantly outperform traditional methods in identifying weaknesses in simple encryption algorithms. This is due to their ability to detect complex patterns in data that may go unnoticed by classical approaches. However, despite their high performance, there are limitations in terms of the accuracy of the discrimination and the maximum number of rounds that can be compromised for certain ciphers. The purpose of this study is to overcome these shortcomings by optimizing the architecture of the neural network (NN) and the structure of the input data, according to the Gohr model. As part of this work, several key components of the differential discriminator were improved: the convolutional module, the residual module, and the prediction module. The optimization of these components allowed to significantly increase the efficiency in recognizing differential patterns in ciphertexts. In addition, special attention was paid to optimizing the structure of the input data, which made it possible to more accurately identify the characteristics of the ciphertext and information about the encryption structure. The results of the study, conducted on the example of cryptanalysis of the Speck32/64 cipher, confirm the improvements achieved: the accuracy of the differential distinguisher has increased by 5–7 rounds, and the recognition capability has been extended to 8 cipher rounds. These achievements demonstrate the high efficiency of the proposed approach, which has significant potential for further research in the field of cryptanalysis. Due to the importance of information system security, the results of this study can significantly affect the development of new cryptanalysis methods and the improvement of encryption algorithms, which, in turn, can lead to increased data protection reliability in the modern digital environment. The results of the study, conducted on the example of cryptanalysis of the Speck32/64 cipher, confirm the improvements achieved: the accuracy of the differential distinguisher has increased by 5–7 rounds, and the recognition capability has been extended to 8 cipher rounds. These achievements demonstrate the high efficiency of the proposed approach, which has significant potential for further research in the field of cryptanalysis. Due to the importance of information system security, the results of this study can significantly affect the development of new cryptanalysis methods and the improvement of encryption algorithms, which, in turn, can lead to an increase in the reliability of data protection in the modern digital environment.

Keywords: deep learning; cryptanalysis; Gore's model; symmetric cryptographic differential discriminator; Speck32/64.

REFERENCES (TRANSLATED AND TRANSLITERATED)

1. Gohr, A. (2019). Improving attacks on round-reduced Speck32/64 using deep learning. In: *Advances in Cryptology – CRYPTO 2019. LNCS, vol. 11693,* 150–179. https://doi.org/10.1007/978-3-030-26951-7_6
2. Baksi, A., et al. (2020). Machine Learning Assisted Differential Distinguishers for Lightweight Ciphers (Extended Version). In: *Classical and Physical Security of Symmetric Key Cryptographic Algorithms. Computer Architecture and Design Methodologies,* 141–162. https://doi.org/10.1007/978-981-16-6522-6_6
3. Jain, A., Kohli, V., & Mishra, G. (2020). Deep learning based differential distinguisher for lightweight cipher PRESENT. *Cryptology ePrint Archive.*
4. Wang, M. (2008). Differential cryptanalysis of reduced-round PRESENT. In: *Cryptology – AFRICACRYPT 2008. AFRICACRYPT 2008. Lecture Notes in Computer Science, vol. 5023,* 40–49. https://doi.org/10.1007/978-3-540-68164-9_4
5. Bellini, E., & Rossi, M. (2021). Performance comparison between deep learning-based and conventional cryptographic distinguishers, *Intelligent Computing, LNNS, vol. 285,* 681–701. https://doi.org/10.1007/978-3-030-80129-8_48
6. Lyu, L., Tu, Y., & Zhang, Y. (2022). Improving the Deep-Learning-Based Differential Distinguisher and Applications to Simeck. In: *IEEE 25th International Conference on Computer Supported Cooperative Work in Design (CSCWD),* 465–470. https://doi.org/10.1007/978-3-030-80129-8_48
7. Su, H. C., Zhu, X. Y., & Ming, D. (2021). Polytopic attack on round-reduced simon32/64 using deep learning. *International Conference on Information Security and Cryptology. LNCS, vol. 12612,* 3–20. https://doi.org/10.1007/978-3-030-71852-7_1
8. Benamira, A., Gerault, D., Peyrin, T., & Tan, Q. Q. (2021). A Deeper Look at Machine Learning-Based Cryptanalysis. *Advances in Cryptology – EUROCRYPT 2021. EUROCRYPT 2021, LNCS, vol. 12696,* 805–835. https://doi.org/10.1007/978-3-030-77870-5_28
9. Sun, L., Gerault, D., Benamira, A., & Peyrin, T. (2020). Neurogift: Using a machine learning based sat solver for cryptanalysis. In: *Cyber Security Cryptography and Machine Learning: Fourth International Symposium, CSCML 2020, LNCS, vol. 12161,* 62–84. https://doi.org/10.1007/978-3-030-49785-9_5
10. Hou, Z., Ren, J., & Chen, S. (2021). Cryptanalysis of round-reduced SIMON32 based on deeplearning. *Cryptology ePrint Archive*.
11. Chen, Y., Shen, Y., Yu, H., & Yuan, S. (2023). A New Neural Distinguisher Considering Features Derived from Multiple Ciphertext Pairs. *The Computer Journal, 66(6),* 1419–1433. https://doi.org/10.1093/comjnl/bxac019
12. Rajan, R., et al. (2022). Deep Learning-Based Differential Distinguisherfor Lightweight Cipher GIFT-COFB. Machine Intelligence and Smart Systems: Proceedings of MISS 2021, 397–406. https://doi.org/10.1007/978-981-16-9650-3_31
13. Beaulieu, R., et al. (2015). The SIMON and SPECK families of lightweight block ciphers. *DAC'15: Proceedings of the 52nd Annual Design Automation Conference, 175,* 1–6. https://doi.org/10.1145/2744769.2747946
14. Biham, E., Shamir, A. (1991). Differential cryptanalysis of DES-like cryptosystems. *Journal of CRYPTOLOGY, 4(1),* 3–72.
15. Sarker, I. H. (2021). Deep Learning: A Comprehensive Overview on Techniques, Taxonomy, Applications and Research Directions. *SN Computer Science, 2 (6),* 1–20. https://doi.org/10.1007/s42979-021-00815-1
16. He, K., et al. (2016). Deep residual learning for image recognition. *IEEE Conference on Computer Vision and Pattern Recognition,* 770–778. https://doi.org/10.1109/CVPR.2016.90
17. Gohr, A. (2019). Improving attacks on round-reduced Speck32/64 using deep learning. *CRYPTO 2019, LNCS, vol. 11693,* 150–179. https://doi.org/10.1007/978-3-030-26951-7_6
18. Hu, J., Shen, L., & Sun, G. (2018). Squeeze-and-Excitation Networks. *The Conference on Computer Vision and Pattern Recognition, IEEE,* 7132–7141. https://doi.org/10.1109/CVPR.2018.00745
19. Shalev-Shwartz, S., & Ben-David, S. (2014). Understanding machine learning: From theory to algorithms. *Cambridge university press.*
20. Chen, Y., & Yu, H. (2021). A New Neural Distinguisher Model Considering Derived Features from Multiple Ciphertext Pairs. *The Computer Journal.*
21. Hou, Z., Ren, J., & Chen, S. (2021). Improve neural distinguisher for cryptanalysis. *Cryptology ePrint Archive.*
22. Hulak, H. M., Zhiltsov, O. B., Kyrychok, R. V., Korshun, N. V., & Skladannyi, P. M. (2024). *Information and cyber security of the enterprise.* Textbook. Lviv: Publisher Marchenko T. V.