DOI 10.31891/2307-5732-2024-335-3-60
УДК 004.4

СМІРНОВ ОЛЕКСІЙ
Хмельницький національний університет
https://orcid.org/0009-0008-2189-0096
e-mail: a.smirnov3825@gmail.com
ПОПЛАВСЬКИЙ СЕРГІЙ
Хмельницький національний університет
https://orcid.org/0009-0006-1949-8656
e-mail: sergey.poplavskii@gmail.com
ЖУКОВСЬКИЙ ПАВЛО
Хмельницький національний університет
https://orcid.org/0009-0007-3461-9919
e-mail: 777reiste777@gmail.com
ВІЖЕВСЬКИЙ ПЕТРО
Хмельницький національний університет
https://orcid.org/0009-0009-4851-0839
e-mail: petro.vizhevskyi@gmail.com
СОРОЧИНСЬКИЙ ОЛЕКСАНДР
Хмельницький національний університет
https://orcid.org/0009-0003-7966-4861
e-mail: sorochinskiy159@gmail.com

СТРАТЕГІЯ ТА АЛГОРИТМИ ВИЯВЛЕННЯ ВРАЗЛИВОСТЕЙ В ПРОГРАМНИХ МОДЕЛЯХ АПАРАТНИХ ЗАСОБІВ

Технології інтегральних схем постійно розвиваються. Спостерігається тенденція того, як багато комп'ютерних пристроїв стають широко доступними для громадськості, стимулюючи цікавість та інновації для багатьох через швидке створення, розгортання або навіть експлуатацію апаратних систем. Аналогічним чином, технологія і можливості їх також значною мірою зросли протягом десятиліть. Однак у міру того, як технології продовжували розвиватися, зросла і велика кількість інформації, яка стала легкодоступною майже для всіх у всьому світі. В результаті для багатьох людей без попередніх знань або досвіду стало можливим адекватно отримати навички, необхідні для проектування та впровадження апаратних систем, які можуть покращувати або використовувати повсякденні технології. Незважаючи на те, що пристрої, які сприяють цьому Інтернету речей були спрямовані на покращення якості життя та сприяння революції розумного будинку, вони стали звичайною мішенню для багатьох хакерів апаратного забезпечення. В роботі вирішується саме така проблема щодо унеможливлення внесення або виявлення сторонніх знаків в програмних моделях апаратних засобів.

Розроблена стратегія та засоби, які базуються на поданих узагальнених алгоритмах, є основою методу для захисту програмних моделей апаратних засобів. Основою розробленої стратегії є удосконалений генетичний алгоритм. Розроблений на основі стратегії метод захисту зашифрованого тексту включає динамічні керовані перестановки, які виробляють зміни, щоб гарантувати, що вихід під час наступного раунду не містить одноразових змін і не може бути реалізована класична методологія атаки.

Напрямами подальших досліджень є удосконалення наборів моделей сторонніх знаків для їх подальшого використання при дослідженні програмних моделей апаратних засобів.

Ключові слова: вразливості, програмні моделі, апаратні пристрої, генетичні алгоритми.

SMIRNOV OLEKSII, POPLAVSKYI SERHII, ZHUKOVSKYI PAVLO, VIZHEVSKYI PETRO, SOROCHYNSKYI OLEKSANDR
Khmelnytskyi National University

STRATEGY AND ALGORITHMS FOR DETECTING VULNERABILITIES IN SOFTWARE MODELS OF HARDWARE

Technologies of integrated circuits are constantly developing. There is a trend of many computing devices becoming widely available to the public, stimulating curiosity and innovation for many through the rapid creation, deployment, or even operation of hardware systems. Similarly, technology and their capabilities have also grown significantly over the decades. However, as technology continued to develop, so did the abundance of information that became readily available to almost everyone around the world. As a result, it has become possible for many people without prior knowledge or experience to adequately acquire the skills needed to design and implement hardware systems that can enhance or utilize everyday technology. Although the devices that facilitate this Internet of Things have been aimed at improving the quality of life and contributing to the smart home revolution, they have become a common target for many hardware hackers. The work solves just such a problem regarding the impossibility of entering or detecting third-party signs in software models of hardware.

The developed strategy and tools, which are based on the presented generalized algorithms, are the basis of the method for protecting software models of hardware. The basis of the developed strategy is an improved genetic algorithm. The strategy-based ciphertext protection method includes dynamic controlled permutations that produce changes to ensure that the output during the next round does not contain one-time changes and the classical attack methodology cannot be implemented.

The direction of further research is the improvement of sets of models of third-party signs for their further use in the study of software models of hardware.

Keywords: vulnerabilities, software models, hardware devices, genetic algorithms.

Вступ

У міру того, як технології інтегральних схем постійно розвиваються, спостерігається тенденція, як багато комп'ютерних пристроїв стають широко доступними для громадськості, стимулюючи цікавість та інновації для багатьох завдяки швидкому створенню, розгортанню або навіть експлуатації апаратних систем. Аналогічним чином, технологія і можливості їх також значною мірою зросли протягом десятиліть. Наприклад, іграшки, автомобілі, гаражні ворота, різні господарські машини, які зараз оснащуються вбудованими системами та можливостями бездротового зв'язку для покращення життя кінцевого користувача. Однак у міру того, як технології продовжували розвиватися, зростала і велика кількість інформації, яка ставала легкодоступною майже для всіх у всьому світі, причому зі швидким доступом. В результаті для багатьох людей без попередніх знань або досвіду стало можливим адекватно отримати навички, необхідні для проектування та впровадження апаратних систем, які можуть покращувати або використовувати повсякденні технології. Незважаючи на те, що пристрої, які сприяють цьому Інтернету речей (IoT), були спрямовані на покращення якості життя та сприяння революції розумного будинку. З тих пір вони стали звичайною мішенню для багатьох хакерів апаратного забезпечення. При цьому домашні пристрої стають мішенню для виявлення вразливостей, покращення або просто перепрофілювання. Хоча може бути зрозуміло, що багато з цих домашніх пристроїв не обов'язково потребують належних механізмів доступу та контролю. Очікувано, що пристрої, які в іншому випадку призначені для контролю доступу, будуть реалізовувати певну форму безпечного протоколу зв'язку. Однак веб-сайти стали звичайним явищем для хакерів спрямованих на обладнання, щоб змінити експлуатацію цих пристроїв IoT, які в іншому випадку повинні захистити будинки від інших впливів. Хоча це можна розглядати як невинне поширення знань та освітнього контенту, його негативна сторона викриває загальну відсутність турботи про безпеку з боку виробників пристроїв та існуючу сприйнятливість систем до технологій, що постійно розвиваються. І це дозволяє людям зі зловмисними намірами легко створювати зловмисні системи, які можуть бути використані для особистої вигоди. Зростання підробок інтелектуальної власності та крадіжки інтелектуальної власності інтуїтивно породило потребу в методах, які дозволяють розробникам апаратних засобів перевіряти та ідентифікувати свої ядра у випадку, якщо вони підозрюють неправильне використання або крадіжку інтелектуальної власності. Процес розмітки послідовних схем, скінченних автоматів розглянуто в [1], де використовуються стратегії для використання властивих характеристик пристроїв (стан, введення-виведення, крайове кодування та кодування стану). Однак найновіші сучасні системи [2] намагаються використовувати методи, які вирішують проблему ізоморфізму підграфів, що виникає під час вбудовування сторонніх знаків. Найбільш помітним недоліком є те, що не існує ефективного розв'язку задачі і не було показано, що ні евристичні, ні апроксимаційні алгоритми не дають оптимальних рішень [3]. Це пов'язано з відомою обчислювальною складністю, оскільки відомо, що це одна з найбільш ранніх NP-повних задач. Тому, розглянемо гібридизований генетичний алгоритм (ГА) для ефективного розв'язання цієї проблеми як з точки зору часу, так і якості отриманого рішення. Запропонований підхід походить від численних змін, внесених до традиційного підходу ГА, які базуються на твердженнях з [4] та спостережень, які регулярно здійснюються в природі. Традиційні ГА нав'язують концепцію біологічного кросинговеру, тоді як тут можемо реалізувати відомий біологічний метод квадрату для домінантних і рецесивних генів, щоб забезпечити більш природний механізм кросинговеру.

Актуальність роботи полягає в розробці стратегії і засобу криптографічного захисту від вразливостей в апаратному забезпеченні.

Аналіз відомих стратегій та засобів забезпечення захисту комп’ютерних пристроїв

Розглянемо атаки, які можуть бути виконані неруйнівним способом [5]. Приймемо для розгляду цю модель з припущенням, що здійсненність атаки більша не тільки з точки зору економічної ефективності, але й завдяки кількості доступних добре задокументованих методів [6]. Ці типи атак можуть бути зосереджені на зборі інформації про систему шляхом спостереження за її виконанням або синхронізацією кешу, коли атака на кеш дозволяє зловмисникам розкрити рядки даних кешу. Наприклад, AES використовує пошук таблиць, що зберігаються в кеші, які залежать від використовуваного ключа шифрування. Таким чином, зловмисник може спробувати завантажити варіації ключів, щоб визначити, які набори бітів є в ключі, через час попадання кешу або промаху, спричиненого завантаженням відповідних таблиць. Цей тип атаки полягає в тому, що зловмисник намагається використовувати якісь засоби для активного порушення цілісності даних, які зараз обробляються в системі. При розгляді апаратної реалізації це може бути досягнуто за допомогою ряду способів, які в іншому випадку впливають на значення транзистора або шини. Одним із таких способів може бути зниження напруги в системі, оскільки транзистори не працюватимуть при заданих напругах і видаватимуть неправильні значення. Розглянемо попередні приклади інверторів, що використовують технологію, яка працює від джерела живлення. При подачі дуже малої напруги живлення інвертор не працює належним чином і, таким чином, призводить до несправності в системі [7].

Атака типу бічний канал [8] використовує методи зондування для вимірювання та збору інформації про систему за допомогою різних засобів та пристроїв. Наприклад, одним із методів, який зазвичай використовується, є аналіз диференціальної потужності, який досліджує потужність системи за різних вхідних умов. Якщо розглядати інвертор, то досліджуючи потужність при конкретному значенні, можемо отримати знання про те, що таке конкретний вхід у будь-який момент часу. При зміні вхідної напруги система буде видавати помітно різні значення. Тобто, суть атаки типу бічний канал в тому, що вплив здійснюють опосередковано [8].

Криптоаналітичні атаки згідно їх моделі спираються не на апаратні або фізичні методи бічного каналу для збору інформації, а на ретельний аналіз самого криптографічного алгоритму, шифротексту або інших методів з метою виявлення слабких місць системи та отримання використовуваного секретного ключа. Крім того, визначаємо також основні типи генералізованих криптоаналітичних атак [9]: тільки шифротекст (зловмисник має доступ лише до набору шифротекстів); відомий відкритий текст (зловмисник має доступ до наборів як відкритих текстів, так і відповідних шифротекстів); вибраний відкритий текст (зловмисник вибирає випадкові відкриті тексти для шифрування, щоб отримати відповідні шифротексти); адаптивний обраний відкритий текст (зловмисник може вільно адаптувати введення відкритого тексту на основі раніше отриманих шифротекстів з вибраних відкритих текстів); обраний зашифрований текст (зловмисник збирає інформацію, вибираючи зашифрований текст, щоб отримати як ключ, так і відкритий текст); обраний ключ (зловмисник вибирає значення ключа, щоб отримати інформацію про процес перетворення відкритого тексту в зашифрований); метод грубої сили (зловмисник намагається отримати відкритий текст заданого зашифрованого тексту, вичерпно досліджуючи всі можливі ключі); диференціальний підхід (зловмисник намагається знайти статистичну кореляцію між значеннями ключів і перетвореннями шифру, використовуючи визначений відкритий текст для отримання ключа); лінійний метод (зловмисник намагається знайти лінійне наближення до шифру для пари відкритого тексту та шифротексту, зводячи наближення до простішого, де ключ можна легко отримати); протокол націлений на протоколи безпеки, такі як аутентифікація, при цьому атаки, такі як повторне відтворення, дозволяють зловмисникам повторно надсилати дані або з потенційною затримкою з метою маскування під справжнього користувача [10]; пов'язаний ключ (отримання ключової інформації шляхом спостереження за безліччю невідомих, але відомо, що математично пов'язаних, секретних ключів, які використовуються для процесу шифрування); інтегральний метод (метод, що використовує набори обраних відкритих текстів з деякою фіксованою різницею, операції XOR; якась частина відкритого тексту залишається незмінною, а інша частина змінюється); слайд (метод атаки, який зводить нанівець актуальність функцій числового раунду, що виконуються над даними, шляхом наближення до раундів як добутку однакових перестановок); об'єктний метод (мета полягає в тому, щоб використовувати один і той же шифр з двома відкритими текстами з різницею лише в один раунд між ними, націлюючись на шифри, відомі як слабкі шрифти проти атак з відомим відкритим текстом [11]); зустріч посередині (зловмисник шифрує деякий відкритий текст одним ключем, а отриманий зашифрований текст знову вторинним ключем; розшифровуючи другий шифрований текст за допомогою другого ключа і шифруючи відкритий текст за допомогою першого ключа, зловмисник може ефективніше перебирати шифр і формувати пари ключів-кандидатів, які можуть бути додатково протестовані на додаткових парах відкритий текст/шифрований текст [12]).

Таким чином, криптоаналітичні атаки згідно їх моделі спираються не на апаратні або фізичні методи бічного каналу для збору інформації, а на ретельний аналіз самого криптографічного алгоритму, шифротексту або інших методів з метою виявлення слабких місць системи та отримання використовуваного секретного ключа. Для розвитку цих методів використовуються активно генетичні алгоритми. Розглянемо їх в контексті поставленої проблеми. Застосовуємо цей підхід до усталеної системи сторонніх знаків на основі кодування стану, яка демонструє значні покращення в порівнянні з відомими підходами. Із середньою економією або прийнятним допуском з точки зору площі, затримки та літералів, необхідних для реалізації сторонніх знаків. Ці результати показують, що цей підхід можна вважати ефективним рішенням проблеми, яка виникає в процесі вбудовування сторонніх знаків [13]. Найновішим методом для виявлення сторонніх знаків, який використовує підхід є метод з [14]. Цей метод використовує схему сторонніх знаків на основі країв. Техніка на основі країв використовує як невизначені, так і існуючі краї для виконання техніки сторонніх знаків на основі вводу/виводу. Крім того, показано, що він [15] перевершує як методи встановлення сторонніх знаків на основі стану, так і вводу-виводу. Вперше представлений [16] метод сторонніх знаків на основі станів використовує додаткові стани для реалізації прихованої поведінки, доступ до якої можуть отримати лише ті, хто має доступ до секретного ключа. Додаткові стани, як правило, проявляються у вигляді декількох підсистем, таким чином, оригінальна частина може бути відтворена з модифікованою поведінкою і використовувати секретний ключ для свого ввімкнення. Техніка вперше представлена в [17] використовує розширений шлях станів, що містять невизначені комбінації введення-виведення, в яких сигнатура переставляється. Використання цих вільних країв має на меті збереження цілісності системи та секретності підписів, таким чином, незаперечення підтримується за допомогою ациклічного таємного шляху, який відповідає підпису автора. І навпаки, основним недоліком цієї системи є те, що коли система є повністю визначеною, то до системи необхідно додавати додаткові вхідні біти. Це дозволяє генерувати невизначені комбінації вводу-виводу з початковою кількістю вхідних бітів, що призводить до того, що система несе значні додаткові витрати від невизначених комбінацій вводу-виводу. Модифікація сторонніх знаків на основі вводу-виводу, подана в [18] і ця техніка спрямована на зниження додаткових витрат, що генеруються повторним використанням існуючих країв з комбінаціями вводу-виводу, які можуть бути відображені на деяку підсерію сигнатури. Сторонні знаки на основі кодування стану подано фреймворком в [19], де спочатку попередньо обробляється бажана сигнатура за допомогою алгоритму хешування, а постобробка отриманого хеш-рядка виконується з метою перетворення хешу в спрямований граф на основі станів, побудованих з довжини кодування і суміжностей, інкапсульованих в перетравленому хеші. Цей метод застосовує послідовності сторонніх знаків як значення кодування станів, таким чином, послідовність станів може бути обійдена, щоб

відтворити сторонній знак через існуючі або додані краї. Робота з використанням методу на основі ГА подана в [20]. Запропонований підхід істотно відрізняється від методу з [21]. Це пов'язано з тим, що в [20] представляється ГА, яка виконує додаткові завдання, засновані на синтезі, такі як злиття та скорочення, тоді як ця робота є узагальненим підходом до вирішення вищезгаданої проблеми та представляє її можливості через використання існуючого фреймворку та застосування.

Розглянемо рівень впливу синтезу на сторонні знаки скінченних автоматів на основі кодування станів. Оскільки проектні корпорації з розробки інтегральних схем продовжують шукати найбільш фінансово оптимальні моделі та методи для постачання великих обсягів схем споживчого класу, одночасно зменшуючи як вартість неповторюваних кроків, так і час виходу на ринок, то дана конструкція може змінюватися як у форматі, так і багато разів. Цим змінам сприяє лише постійний розвиток інструментів автоматизованого проектування, які дозволяють швидко створювати прототипи систем з поведінковими описами за допомогою мов опису апаратного забезпечення і синтезувати їх від високорівневого опису до макету плати, готової до виготовлення, за лічені хвилини. Подібна практика серед корпорацій, що займаються електронікою споживчого класу, будь-то наймання архітекторських фірм третьої сторони, закупівля готових компонентів або аутсорсинг виробництва, і все це в рамках зусиль з постійного скорочення витрат для конструкцій, є поширеною.

В даний час не існує галузевого методу або практики, за допомогою яких компанія могла б легко довести своє право власності, витративши значні витрати часу і ресурсів. Відсутність методів перевірки права власності, які були б включені в проекти, може бути пов'язана з різними причинами, наприклад, не існує простого методу, який би не впливав негативно на схему під час процесу проектування та життєвого циклу його розробки; або просто метод не може бути легко інтегрований або використаний з існуючими галузевими стандартними інструментами.

Таким чином, метою роботи є подальший розвиток стратегії на основі стороннього знаку з кодування та його структури. Використання техніки сторонніх знаків на основі кодування стану дозволить ефективно збирати відповідні дані. Ці дані згодом забезпечать візуалізацію того, як зусилля з синтезу протягом життєвого циклу розробки архітектури впливають на синтезовану схему після стороннього знаку. Проаналізовані відомі методи та засоби криптографічного захисту від вразливостей в апаратному забезпеченні, а також визначено стратегію для покращення ефективності цього процесу. Запропоновано використати генетичні алгоритми, оскільки вони здатні генерувати якісні рішення і в значній мірі досліджувати весь простір рішень для даної проблеми. Оскільки ГА є еволюційними алгоритмами, то вони досягають цього шляхом включення концепцій, зосереджених на природному відборі, та використанні біологічних операторів: мутація; кросовер; селекція. Встановлено, що генетичні алгоритми можуть бути ефективно використані при розв'язанні проблеми, в якій потрібно дослідити можливу наявність стороннього коду в програмній моделі при проектуванні апаратного пристрою чи наявність власного коду схеми в розробці схеми в конкуруючій компанії.

Стратегія криптографічного захисту від вразливостей в апаратному забезпеченні

Організація протидії текстовим атакам на шифри перестановок є перспективною стратегією для дослідження та розроблення. Розглянемо стратегію з включення ключ-залежних мереж заміщення і перестановки в криптографічних алгоритмах і апаратному забезпеченні за допомогою примітивів мереж взаємозв'язку. Цей метод проектування демонструється шляхом модифікації шифру з декількома архітектурними варіаціями для демонстрації гнучкості. Крім того, встановлено, що для цього шифру включення нової методології проектування, яка залежить від ключів, практично не впливає на кінцеву продуктивність або результати потужності, отримані в процесі синтезу, і служить лише для підвищення стійкості, діючи як контрзахід критичної сприйнятливості, яку демонструють шифри на основі перестановок. Удосконалений метод застосовний до криптосистем в обсязі одного комутатора, а не просто з надання методів перестановки через маршрутизації. Тому, необхідні дослідження того, як стійкість криптосистем може бути підвищена за допомогою комутаційних мереж і не вимагає використання додаткових складних математичних операцій для забезпечення безпеки. Крім того, враховані і застосовані контрзаходи в цій методології проектування і вона може бути застосована до альтернативних ключових методів або навіть до побудови шифрів виключно на основі цієї методології.

Тому, в контексті удосконалення методу розглянемо криптографію та інформаційну безпеку. Вони базуються на тріаді, яка складається з трьох основних послуг, необхідних для інформаційної безпеки: конфіденційність; цілісність; доступність. Тому, вони вимагають: конфіденційності та захисту даних від сторонніх осіб; дані не можуть бути змінені неавторизованими особами; щоб конфіденційні дані були легкодоступними та своєчасними. Однак прийнято вважати, що інформаційна безпека неповно представлена лише цією тріадою, що потребує додаткових послуг: автентичність; незаперечення. Щоб дані можна було перевірити як справжні – це четверта послуга і вимога. А остання така, що дані / дії могли б бути адекватно пов'язані з відповідним вихідним суб'єктом. Незважаючи на те, що цей набір послуг є основними принципами та вимогами до інформаційної безпеки, то вони також застосовні до криптографії та повинні бути дотримані. Однак, за будь-якими криптографічними алгоритмами стоять властивості: заплутування; змішування. Тобто, отриманий шифротекст повинен залежати від більше ніж від однієї частини ключа і зміна одного біту у відкритому тексті повинна привести до більших змін в отриманому зашифрованому тексті. Ця невелика зміна тексту, яка призводить до більшої зміни в шифротексті, відома як ефект лавини. Плутанина, яка зазвичай

виконується за допомогою поля підстановки, замінює блоки бітів у відкритому тексті якимось іншим блоком, наприклад, символ один замінюється на другий. Змішування потенційно з використанням поля перестановки переставляє відкритий текст. Ці дві концепції в кінцевому підсумку пов'язані з інтеграцією підстановки і транспозиції для перетворення відкритого тексту в шифротекст за допомогою деякого залученого процесу.

Модель атаки, яку розглядаємо, будує метод атаки на мережу перестановок шифру, який в кінцевому підсумку виявляється застосовним до всіх шифрів на основі перестановок. Таким чином, біти, на які потенційно впливає зміна одного стану, завжди будуть знаходитися в одному і тому ж положенні. Для наочності, система з одним ключем - це замок з поворотним набором, тобто тільки один ключ відкриє замок. Для боротьби з проблемами перемикання елементів використовується функція налаштування керування для керування прохідними та кросоверними операціями. Ця функція, породжена деяким набором булевих операцій, керує всіма ними в топології. Завдяки їй може бути покращена стратегія за допомогою генератору псевдовипадкових функцій стійкість. В кінцевому підсумку використання їх в криптографії є життєздатним методом для виконання перестановок при виконанні лавинної властивості. Інтеграція їх для виконання перестановок в криптографічному програмному забезпеченні дозволяє скоротити кількість інструкцій і циклів, необхідних в бітових перестановках. Це досягається шляхом розробки різних методів пермутації так, що кожен з цих методів скорочує цикл і інструкції в порівнянні з використанням примітивів таблиці пошуку. Тим самим встановлено, що застосування мережевих примітивів може бути корисним у криптосистемах. Істотна відмінність полягає в тому, як генеруються керуючі біти для комутаційних елементів, на відміну від відомих раніше методів. Різноманітні методи генерують керуючі послідовності, а функціональність комутаційного елемента розширена для обробки керуючих значень. Крім того, цей метод не реалізується в мережі комутації. Він використовує ряд регістрів з топологіями маршрутизації і з'єднує регістрові локації з мультиплексорами. Вибраний керуючим значенням вихід передається в тимчасовий регістр. У ньому використовується проблемна одиниця, яка заснована на методі управління, а не на генераторах функцій. Це дані, що містяться в пакеті інформації. Це задано на основі великої сітки, де передача пакетів здійснюється за допомогою окремих частин пакета і таким чином встановлено, що кінець списку слідує за конкретними кроками, які слідують за заголовком списку, який спочатку відправляється через перевірену проблемну одиницю системи. І навпаки, оскільки попередні методи використовують неблокуючі мережі, проблемна одиниця за своєю суттю є блокуючою і не має маршрутизації без суперечок. У випадку, якщо два пакети спробують використовувати один і той же маршрут, то один буде заблокований, а всі наступні частини, що слідують за заголовком списку, також зупиняться. Крім того, цей метод досліджує використання як рандомізованого, так і конвеєрного планування для серійного шифрування даних. Результати, отримані за допомогою методу рандомізованого планування, ще більше підтверджують той факт, що колізія / суперечка не обробляється в цій системі. Цей варіант удосконалення методу вимагає більш тривалого часу передачі через збільшення колізій і невпорядкованості пакетів і при цьому конвеєрний метод представлений для пом'якшення цього недоліку.

Запропонований підхід використовує керовану версію комутатору для індукції ключових перестановок круглих даних. Однак цей підхід все ще застосовний до будь-якого шифру, що використовує мережі перестановок, а не тільки до прямих варіантів. Дана архітектура була побудована на основі оригінального представлення та деталізації шифру за допомогою модифікованих типів перестановок для включення шару керованих структур, реалізованих в різних точках круглої архітектури. Він був побудований навколо шифру таким чином, що ширина шини вводу / виводу комутаторів базувалася на кількості блоків, які були інтегровані. Оскільки біти бітного ключа залишалися невикористаними за раунд. Архітектури були побудовані і перевірені з точки зору даних про продуктивність, площу та потужність, зібрані в процесі синтезу для кожної з архітектурних реалізацій, порівнюючи їх з незміненим шифром.

Апаратні реалізації алгоритму шифру і шифри з використанням структур є чутливими через невипадкову поведінку мереж перестановок всередині архітектури. Хоча шифр, спочатку забезпечував умови стійкості до диференціальних атак, для шифру та архітектури він не тільки сприйнятливий до диференціальних атак відкритого тексту, але й дана архітектура не вимагає використання методів для виконання диференціальних атак з відкритим текстом. Розглянемо заходи протидії таким атакам, застосовні до всіх шифрів, поряд з простішими контрзаходами для загальної стійкості та врахування криптографічного обладнання.

Розглянемо атаку з відкритим текстом, яка використовує статистичний аналіз для кореляції відмінностей у виводі шифротексту на основі змін у вхідних даних відкритого тексту, щоб краще розрізняти, які операції виконуються з метою реконструкції секретного ключа. При цьому використовується невипадкова поведінка мереж перестановок для його виконання на імплементації базового шифру. Хоча реалізація базового шифру, істотно відрізняється від тієї, що спочатку була спочатку аналізована, але це є незначним впливом на результат, і використання побайтових операцій замість побітових не має жодного відношення до стійкості проти цієї атаки. Успіх в атаці досягається за рахунок вимірювання електромагнітної індукції мікроконтролеру, в роботі якого знаходиться реалізація шифру. Це дозволяє зашифрувати серію вибраних значень відкритого тексту, а потім зафіксувати круглий вихідний диференціал для статистичного аналізу. Метод може містити такі наступні кроки:

1) вибір тексту для атаки;

2) вибір звичайного тексту для використання його як сторонніх знаків;

3) сформувати початковий текст з вставленням звичайного тексту, який додається;
4) зашифрувати два тексти: початковий без змін; початковий текст із вставленням сторонніх знаків;
5) визначення електромагнітного випромінювання;
6) обчислення різники електромагнітної індукції;
7) генерація ключових кандидатів в зашифрованих текстах;
8) застосування формули для визначення побітових раундів:
9) якщо на кроці 8 не встановлено фрагменти зі сторонніми знаками, тоді повторити кроки 5-8;
10) якщо встановлено фрагменти зі сторонніми знаками, тоді завершити роботу.

В цілому, це простий метод захисту зашифрованого тексту, що включає динамічні керовані перестановки, які виробляють зміни, щоб гарантувати, що вихід під час другого раунду не містить одноразових змін і не може бути реалізована класична методологія атаки. Вибравши цифровий підпис переправляємо його за допомогою функції, щоб отримати, наприклад, результуючий геш-рядок: 345ghbdbv67lbnbnb78ssvnnv9595g. Якщо розглядати можливі конфігуровані довжини файлу, то набір переправлюваних рядків для трансформування наведено в табл. 1. В той час як довжина файлу зазвичай не використовується в існуючому методі, то для ілюстрації використаємо саме її.

Таблиця 1

Шифр-таблиця

Текст	**Шифр**
5	345gh
2	bd
17	bv67lbnbnb78ssvnn
6	v9595g

Додатково для більшої стислості використовуємо довжину кодування. Це призводить до того, що рядок геш-файлу розбивається на блоки символьного стану. Ці блоки станів символів згодом обробляються циклічно кільцевим способом, і в тому порядку, в якому вони з'являються в геш-рядку для побудови списків суміжності станів. Зображення на рис. 1. Використовуючи інформацію про список суміжностей для кожного символічного стану, можемо скласти представлення ГА. Ці дані представляють структуру графіку, зображену на рис. 2. Після того, як рядок оброблений і зібрано достатньо даних для реалізації ГА, генерується файл для стороннього знака запиту, встановлюючи кількість бітів введення/виведення до довжин, відповідних зі значеннями стану скидання, який опускається, оскільки решта даних заголовку визначені відповідним чином. Файл, отриманий під час цього процесу, який представляє рис. 1 , подано на рис. 2.

Значення введення-виведення в ГА встановлюються спеціально для того, щоб збільшити можливість відображення цих станів запиту на цільові стани, оскільки умови вводу/виводу та поведінка для системи та ж, то сторонній знак може бути відновлений у регістрі стану. Знайшовши цей сторонній знак запиту ГА у вихідному цільовому запиту і змусивши ці ребра або прийняти поведінку цього знайдені в цільовій функції або явно не визначені.

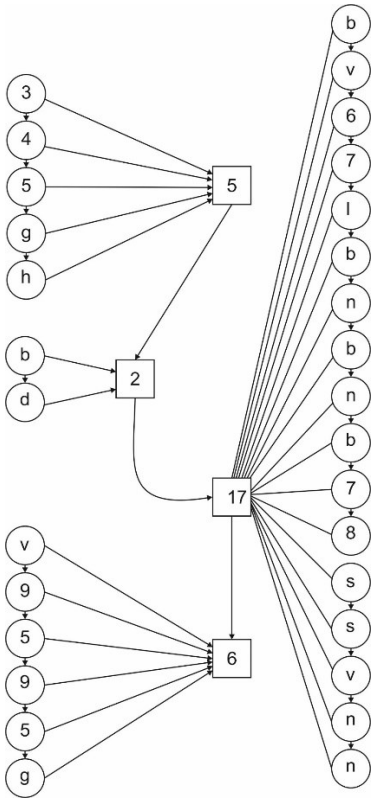

Рис.1 - Побудова станів символів і суміжностей

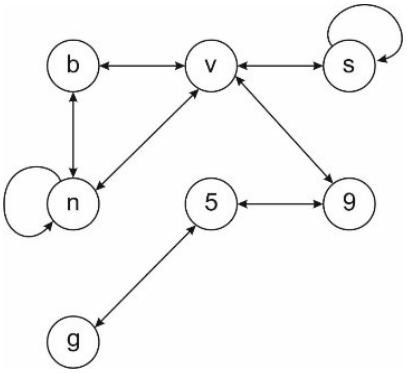

Рис. 2 - Представлення графіка символьних станів та списку суміжностей

На відміну від традиційної моделі ГА, націленої на проблему з однією ціллю в техніці сторонніх знаків на основі кодування стану, немає простої задачі з одним пристосунком, тому мета зіставлення запиту з цільовим значенням включає розгляд як ребер, так і бітів. У випадку, якщо значення є повністю визначеним, тоді повинні додати біт до системи, щоб врахувати необхідні додаткові переваги. І навпаки, коли значення є неповністю визначеним, то треба мінімізувати кількість ребер доданих до системи, зазначаючи, що ця стратегія також застосовна до наступного кроку. Таким чином, замість традиційної «цілі» маємо «цільові краї» та «цільові біти» в новій моделі ГА, яку зображено алгоритмом на рис. 3.

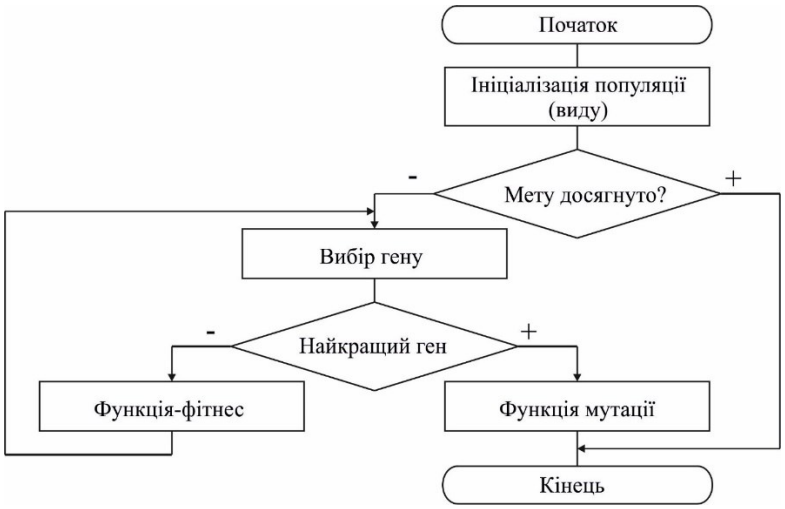

Рис. 3 – Схема розширеної моделі ГА

Не розглядаємо окрему популяцію, яка працює над якоюсь проблемою, в загальній схемі ГА. Хоча існує «острівна» модель для традиційної ГА, але для паралельної обробки в ГА розглядаємо «острів» у фізичному сенсі до обробки. Наприклад, існують дві популяції незалежного розміру, що мають однакову структуру генерації, які можуть взаємодіяти шляхом схрещування популяцій. Будемо вважати, що це не тільки для того, щоб точніше зобразити еволюційний процес, але й дозволити те, що можна розглядати як концепцію мінливості, обумовлену природою, оскільки подібно до мутації, вказуємо ймовірнісне значення, в якому ці популяції можуть здійснювати спарювання.

Таким чином, необхідно провести додаткові перевірки, щоб переконатися, що дуплікація генів не відбувається. Потрібно розділити геномне призначення на двофазний процес: призначити відповідні гени, переконавшись, що вони не дублюються, випадковим чином встановити решту рецесивних генів з пулу генів, що залишилися.

Запропоноване рішення ґрунтується на припущенні, що нормальні та аномальні дані розділені визначеним користувачем пороговим значенням. Запропонована продуктивність рішення змінюється залежно від порогового значення, і в застосунку найвищий бал F1 досягається з квантилем p, встановленим в 1 відсоток його щільності.

Висновки

Розроблена стратегія та засоби, які базуються на поданих узагальнених алгоритмах, є основою методу для захисту програмних моделей апаратних засобів. Основою розробленої стратегії є удосконалений генетичний алгоритм. Розроблений на основі стратегії метод захисту зашифрованого тексту включає динамічні керовані перестановки, які виробляють зміни, щоб гарантувати, що вихід під час наступного раунду не містить одноразових змін і не може бути реалізована класична методологія атаки.

Напрямами подальших досліджень є удосконалення наборів моделей сторонніх знаків для їх подальшого використання при дослідженні програмних моделей апаратних засобів.

Література

1. Swamy S. N., Solomon R. K. An empirical study on system level aspects of Internet of Things (IoT). *IEEE Access* 8. 2020. P. 188082-188134.

2. Denysiuk D., Savenko O., Lysenko S., Savenko B., Kashtalian A. Method for Detecting Steganographic Changes in Images Using Machine Learning. In: *2023 13th International Conference on Dependable Systems, Services and Technologies (DESSERT)*, Athens, Greece. 2023. P. 1-6. doi:10.1109/DESSERT61349.2023.10416453.

3. Letteri I., Antonio D. C., Giuseppe D. P. New optimization approaches in malware traffic analysis. In: *International Conference on Machine Learning, Optimization, and Data Science*. Cham: Springer International Publishing. 2021. P. 57-68.

4. Markowsky G., Savenko O., Lysenko S., Nicheporuk A. The technique for metamorphic viruses' detection based on its obfuscation features analysis. *CEUR-WS* 2104. 2018. P. 680-687.

5. Lysenko S., Savenko Ol., Bobrovnikova K. DDoS Botnet Detection Technique Based on the Use of the Semi-Supervised Fuzzy c-Means Clustering. *CEUR-WS* 2104. 2018. P. 688-695.

6. Savenko B., Lysenko S., Bobrovnikova K., Savenko O., Markowsky G.. Detection DNS Tunneling Botnets // *Proceedings of the 2021 IEEE 11th International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS), IDAACS'2021*, Cracow, Poland, September 22-25, 2021.

7. Xu X., Zheng Y., Liu X. Unsupervised Botnet Detection using Network Traffic Clustering Techniques. *Journal of Computer Networks and Communications.* 2021.

8. Ribeiro M., Vieira M. Deep Learning Clustering for Botnet Detection. *Cybersecurity and Privacy Journal.* 2020. V. 1. No. 1. P. 45-60.

9. Lysenko S., Bobrovnikova K., Shchuka R., Savenko O. A Cyberattacks Detection Technique Based on Evolutionary Algorithms. *11th International Conference on Dependable Systems. Services and Technologies (DESSERT).* 2020. V. 1. P. 127-132. DOI: 10.1109/DESSERT50317.2020.9125016

10. Zhu D. Efficient precision-adjustable architecture for softmax function in deep learning. *IEEE Transactions on Circuits and Systems II: Express Briefs.* 2020. V. 67. No. 12. P. 3382-3386.

11. Lerke A., Heßling H. On Strange Memory Effects in Long–term Forecasts using Regularised Recurrent Neural Networks. *IJC.* 2022. V. 21. No. 1. P. 19-24. https://doi.org/10.47839/ijc.21.1.2513

12. Savenko B., Kashtalian A. Method for Determining the Efficiency of a Distributed Anomaly Detection System. *CSIT.* 2022. V. 2. P. 14-22. https://doi.org/10.31891/csit-2022-2-2.

13. Sayed M. A., Anwar A. H., Kiekintveld C., Kamhoua C. Honeypot Allocation for Cyber Deception in Dynamic Tactical Networks: A Game Theoretic Approach. *14th International Conference on Decision and Game Theory for Security. GameSec 2023*. 2023. arXiv preprint. arXiv:2308.11817. DOI: 10.48550/arXiv.2308.11817.

14. Смірнов О.П., Поплавський С.Ю., Ковальчук В.К., Лутюк Л.І. Удосконалений метод та засоби криптографічного захисту від вразливостей в апаратному забезпеченні / *Збірник наукових праць за матеріалами XV Всеукраїнської науково-практичної конференції «Актуальні проблеми комп'ютерних наук АПКН-2023».* Хмельницький, 2023, С. 278-279. https://kn.khmnu.edu.ua/wp-content/uploads/sites/18/apkn-2023-corpuspaper.pdf

15. Anwar A. H., Kamhoua C., Leslie N. Honeypot allocation over attack graphs in cyber deception games. *International Conference on Computing, Networking and Communications (ICNC).* 2020. P. 502-506. IEEE. DOI: 10.1109/ICNC47757.2020.9049764.

16. Lysenko S., Savenko O., Bobrovnikova K., Kryshchuk A. Self-adaptive system for the corporate area network resilience in the presence of botnet cyberattacks. *Communications in Computer and Information Science.* 2018. V. 860. P. 385-401. DOI: 10.1007/978-3-319-92459-5_31.

17. Pomorova O., Savenko O., Lysenko S., Kryshchuk A., Bobrovnikova K. A Technique for the Botnet Detection Based on DNS-Traffic Analysis. In: Gaj, P., Kwiecień, A., Stera, P. (eds) *Computer Networks. CN 2015. Communications in Computer and Information Science.* 2015. V. 522. P. 127-138. DOI: 10.1007/978-3-319-19419-6_12.

18. Bobrovnikova K., Lysenko S., Savenko B., Gaj P., Savenko O. Technique for IoT malware detection based on control flow graph analysis. *Radioelectronic and Computer Systems.* 2022. V. 1. P. 141–153. DOI: 10.32620/reks.2022.1.11.

19. Lysenko S., Savenko O., Bobrovnikova K., Kryshchuk A., Savenko B. Information technology for botnets detection based on their behaviour in the corporate area network. *Communications in Computer and Information Science.* 2017. V. 718. P. 166–181. DOI: 10.1007/978-3-319-59767-6_14.

20. Markoulidakis I., Rallis I., Georgoulas I., Kopsiaftis G., Doulamis A., Doulamis N. A Machine Learning Based Classification Method for Customer Experience Survey Analysis. *Technologies.* 2020. V. 8. Article no. 76. DOI: 10.3390/technologies8040076.

21. Lysenko S., Savenko O., Bobrovnikova, K. DDoS Botnet Detection Technique Based on the Use of the Semi-Supervised Fuzzy c-Means Clustering. *CEUR-WS.* 2018. V. 2104. P. 688-695.

References

1. Swamy S. N., Solomon R. K. An empirical study on system level aspects of Internet of Things (IoT). *IEEE Access* 8. 2020. P. 188082-188134.

2. Denysiuk D., Savenko O., Lysenko S., Savenko B., Kashtalian A. Method for Detecting Steganographic Changes in Images Using Machine Learning. In: *2023 13th International Conference on Dependable Systems, Services and Technologies (DESSERT)*, Athens, Greece. 2023. P. 1-6.
doi:10.1109/DESSERT61349.2023.10416453.

3. Letteri I., Antonio D. C., Giuseppe D. P. New optimization approaches in malware traffic analysis. In: *International Conference on Machine Learning, Optimization, and Data Science*. Cham: Springer International Publishing. 2021. P. 57-68.

4. Markowsky G., Savenko O., Lysenko S., Nicheporuk A. The technique for metamorphic viruses' detection based on its obfuscation features analysis. *CEUR-WS* 2104. 2018. P. 680-687.

5. Lysenko S., Savenko Ol., Bobrovnikova K. DDoS Botnet Detection Technique Based on the Use of the Semi-Supervised Fuzzy c-Means Clustering. *CEUR-WS* 2104. 2018. P. 688-695.

6. Savenko B., Lysenko S., Bobrovnikova K., Savenko O., Markowsky G.. Detection DNS Tunneling Botnets // *Proceedings of the 2021 IEEE 11th International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS), IDAACS'2021*, Cracow, Poland, September 22-25, 2021.

7. Xu X., Zheng Y., Liu X. Unsupervised Botnet Detection using Network Traffic Clustering Techniques. *Journal of Computer Networks and Communications.* 2021.

8. Ribeiro M., Vieira M. Deep Learning Clustering for Botnet Detection. *Cybersecurity and Privacy Journal.* 2020. V. 1. No. 1. P. 45-60.

9. Lysenko S., Bobrovnikova K., Shchuka R., Savenko O. A Cyberattacks Detection Technique Based on Evolutionary Algorithms. *11th International Conference on Dependable Systems. Services and Technologies (DESSERT).* 2020. V. 1. P. 127-132. DOI: 10.1109/DESSERT50317.2020.9125016

10. Zhu D. Efficient precision-adjustable architecture for softmax function in deep learning. *IEEE Transactions on Circuits and Systems II: Express Briefs.* 2020. V. 67. No. 12. P. 3382-3386.

11. Lerke A., Heßling H. On Strange Memory Effects in Long–term Forecasts using Regularised Recurrent Neural Networks. *IJC.* 2022. V. 21. No. 1. P. 19-24. https://doi.org/10.47839/ijc.21.1.2513

12. Savenko B., Kashtalian A. Method for Determining the Efficiency of a Distributed Anomaly Detection System. *CSIT.* 2022. V. 2. P. 14-22. https://doi.org/10.31891/csit-2022-2-2.

13. Sayed M. A., Anwar A. H., Kiekintveld C., Kamhoua C. Honeypot Allocation for Cyber Deception in Dynamic Tactical Networks: A Game Theoretic Approach. *14th International Conference on Decision and Game Theory for Security. GameSec 2023*. 2023. arXiv preprint. arXiv:2308.11817. DOI: 10.48550/arXiv.2308.11817.

14. Smirnov O.P., Poplavskyi S.Yu., Kovalchuk V.K., Lutyuk L.I. An improved method and means of cryptographic protection against vulnerabilities in hardware / Collection of scientific papers based on the materials of the XV All-Ukrainian scientific and practical conference "Actual problems of computer science APKN-2023". Khmelnytskyi, 2023, pp. 278-279. In Ukrainian. https://kn.khmnu.edu.ua/wp-content/uploads/sites/18/apkn-2023-corpuspaper.pdf

15. Anwar A. H., Kamhoua C., Leslie N. Honeypot allocation over attack graphs in cyber deception games. *International Conference on Computing, Networking and Communications (ICNC).* 2020. P. 502-506. IEEE. DOI: 10.1109/ICNC47757.2020.9049764.

16. Lysenko S., Savenko O., Bobrovnikova K., Kryshchuk A. Self-adaptive system for the corporate area network resilience in the presence of botnet cyberattacks. *Communications in Computer and Information Science.* 2018. V. 860. P. 385-401. DOI: 10.1007/978-3-319-92459-5_31.

17. Pomorova O., Savenko O., Lysenko S., Kryshchuk A., Bobrovnikova K. A Technique for the Botnet Detection Based on DNS-Traffic Analysis. In: Gaj, P., Kwiecień, A., Stera, P. (eds) *Computer Networks. CN 2015. Communications in Computer and Information Science.* 2015. V. 522. P. 127-138. DOI: 10.1007/978-3-319-19419-6_12.

18. Bobrovnikova K., Lysenko S., Savenko B., Gaj P., Savenko O. Technique for IoT malware detection based on control flow graph analysis. *Radioelectronic and Computer Systems.* 2022. V. 1. P. 141–153. DOI: 10.32620/reks.2022.1.11.

19. Lysenko S., Savenko O., Bobrovnikova K., Kryshchuk A., Savenko B. Information technology for botnets detection based on their behaviour in the corporate area network. *Communications in Computer and Information Science.* 2017. V. 718. P. 166–181. DOI: 10.1007/978-3-319-59767-6_14.

20. Markoulidakis I., Rallis I., Georgoulas I., Kopsiaftis G., Doulamis A., Doulamis N. A Machine Learning Based Classification Method for Customer Experience Survey Analysis. *Technologies.* 2020. V. 8. Article no. 76. DOI: 10.3390/technologies8040076.

21. Lysenko S., Savenko O., Bobrovnikova, K. DDoS Botnet Detection Technique Based on the Use of the Semi-Supervised Fuzzy c-Means Clustering. *CEUR-WS.* 2018. V. 2104. P. 688-695.