Голові спеціалізованої вченої ради
ДФ 64.051.019
Харківського національного
університету імені В. Н. Каразіна
61022, м. Харків, майдан Свободи, 4

ВІДГУК

офіційного опонента, доцента кафедри математичних методів захисту інформації Фізико-технічного інституту Національного технічного університету України «Київський політехнічний інститут імені Ігоря Сікорського», кандидата технічних наук Яковлєва Сергія Володимировича на дисертацію **Родінко Марії Юріївни** **«Методи побудови та дослідження властивостей малоресурсних блокових шифрів та їх компонентів»,** подану на здобуття ступеня доктора філософії з галузі знань 12 – Інформаційні технології за спеціальністю 122 – Комп'ютерні науки

Актуальність обраної теми дисертації.

Широкого розвитку та поширення набув так званий «Інтернет речей» – велика сукупність комунікаційно пов'язаних між собою малопотужних пристроїв різної функціональності, які можуть виконувати як вузькі специфічні задачі (наприклад, системи захищеного зв'язку або системи автономної сигналізації), так і складні комплексні задачі (наприклад, «розумні дома»). У сфері використання Інтернету речей через особливості застосування актуальними залишаються питання захисту конфіденційності оброблюваних даних та їх цілісності, які традиційно вирішуються криптографічними механізмами захисту інформації. Однак відомі підходи до синтезу криптографічних механізмів, зокрема, блокових шифрів та геш-функцій, виявились слабко придатними для створення захищених криптографічних засобів в межах Інтернету речей, оскільки класичні алгоритми, такі як блоковий шифр AES, вимагають порівняно значних ресурсів для імплементації та витрачають багато потужності при виконанні, що є критичним для функціонування малопотужних пристроїв.

Через окреслені причини виник новий напрям у криптографії – *легка криптографія* (lightweight cryptography), задачею якої є розробка спрощених криптографічних механізмів, придатних для ефективної реалізації у малопотужних пристроях. Однак зробити це можна лише за рахунок зниження криптографічної стійкості таких алгоритмів. Більш того, деякі напрочуд ефективні з точки зору

реалізації підходи, які використовуються у легкій криптографії, зокрема, так званий ARX-дизайн (тобто використання у алгоритмі лише простих операцій, доступних на рівні інструкцій процесора), взагалі мають дуже слабке теоретичне підгрунтя для доведення стійкості від різних класів атак. Відповідно, баланс між ефективністю реалізації та криптографічною стійкістю для легких криптографічних механізмів часто обгрунтовується ad hoc, за допомогою експериментальних розрахунків та експертної думки розробників і аналітиків.

Отже, **актуальність обраної теми** визначається:

1) відсутністю та необхідністю створення сучасної науково-теоретичної бази для дослідження та розробки легких криптографічних алгоритмів та їх складових елементів, яка базується на сучасному математичному апараті та дозволяє аналізувати та науково обґрунтовувати криптографічні властивості цих засобів;

2) відсутністю та необхідністю створення системи вимог до легких криптографічних алгоритмів та умов безпечного функціонування;

3) потребами держави та бізнесу у вітчизняних засобах криптографічного захисту інформації нового покоління, криптографічні, функціональні та технічні характеристики яких задовольняють сучасним комплексним вимогам до малопотужних надійних засобів криптографічного захисту інформації.

Оцінка змісту дисертації, її завершеності у цілому.

Дисертація складається із вступу, п'яти розділів, висновків, списку використаних джерел та п'яти додатків.

У **вступі** обгрунтовується актуальність теми дисертаційної роботи, формулюються мета і завдання досліджень, зазначаються предмет, об'єкт і методи досліджень, наукова новизна отриманих результатів, відомості про їх апробацію, практичне впровадження та публікації.

У першому розділі наведено загальні відомості про блокові шифри та їх моделі та конструкції, описано відомі методи генерування складових блокових шифрів (лінійних перетворень, таблиць підстановок та схем розгортання ключів), а також наведено ряд відомих атак та методів оцінювання стійкості блокових шифрів до наведених атак. Наприкінці розділу окреслено особливості побудови малоресурсних блокових шифрів.

У другому розділі наведено удосконалений метод генерування таблиць підстановок (S-блоків) із встановленими значеннями криптографічних параметрів, які відповідають високому рівню криптографічної стійкості до певних класів атак. Удосконалення методу полягає у пришвидшенні його роботи при збереженні якості одержуваних таблиць, що досягається врахуванням залежності критеріїв, які

використовуються, між собою. У розділі описано теоретичну ідею методу та наведено дані експериментальних розрахунків, які дозволяють пришвидшити генерування байтових S-блоків певного типу у п'ять разів.

Третій розділ присвячено аналізу так званих неін'єктивних схем розгортання раундових ключів. У розділі аналізується математична модель, в якій схема розгортання моделюється випадковим відображенням, та показується, що якість роботи такої схеми, оцінена у потужності множини генерованих послідовностей раундових ключів, асимптотично не поступається якості модельних ін'єктивних схем розгортання.

У четвертому розділі наведено специфікацію малоресурсного шифру «Кипарис», запропонованого здобувачкою, та проведено первинний аналіз його стійкості до відомих криптоаналітичних атак. Описано вимоги, які висувались при розробці даного шифру, загальну конструкцію та усі складові елементи (раундове перетворення, схему розгортання ключів), а також параметри використання. За основу обрано конструкцію схеми Фейстеля та ARX-дизайн, які дозволили створити дуже швидкий шифр, придатний для реалізації у малопотужних пристроях. Також у розділі описано математичну модель для оцінки стійкості до диференціального аналізу та наведено результати експериментальної оцінки стійкості шифру «Кипарис» до диференціального аналізу у припущенні марковської поведінки диференціальних імовірностей; стійкість визначалась наявністю високоімовірних диференціалів та диференціальних характеристик, які знаходились безпосереднім пошуком, алгоритм якого також наведено у розділі. Здобувачкою показано, імовірність знайдених диференціалів настільни низька, що з цього можна стверджувати про наявність у шифру «Кипарис» практичної стійкості до диференціального криптоаналізу.

У п'ятому розділі проведено дослідження швидкості роботи шифру «Кипарис» та його статистичних властивостей. Показано, що швидкість реалізацій шифру «Кипарис» на платформах Windows та Android складає 1-3,5 Гбіт/сек, в залежності від особливослей платформи, архітектури та реалізації, що не поступається та часто перевершує відомі світові аналоги. Статистичні якості та лавинні ефекти шифру «Кипарис» виявились цілком прийнятними.

У **висновках** викладено найбільш важливі наукові й практичні результати, отримані у дисертаційній роботі, які дають повний розв'язок сформульованих завдань дослідження.

У **додатках** містяться повний перелік наукових робіт здобувачки, у яких викладено результати дисертаційного дослідження; повні результати тестування статистичних властивостей шифру «Кипарис» тестами NIST STS; вихідні коди реалізації шифру «Кипарис», які використовувались для дослідженя швидкості роботи та статистичних властивостей; вихідні коди програми пошуку

диференціальних характеристик шифру «Кипарис»; відповідні акти впровадження результатів дисертаційного дослідження.

Основні наукові положення дисертації викладені у 21 науковій роботі, зокрема, у одному розділі монографії, опублікованому у співавторстві, шести статтях, опублікованих у фахових виданнях України та виданнях, які включено до міжнародних наукометричних баз, двох статтях, які додатково висвітлюють результати здобувачки, та дванадцяти доповідях на всеукраїнських та міжнародних наукових та науково-практичних конференціїях. Практична значимість одержаних результатів підтверджується наявністю двох патентів та трьох актів впровадження.

Достовірність отриманих у дисертаційній роботі результатів забезпечується коректністю постановок задач та використаних припущень і обмежень, а також використанням сучасного математичного апарату та програмного забезпечення. Всі результати, отримані у дисертації, мають математичне обґрунтування та підтверджуються відповідними експериментальними обчисленнями.

В цілому, зміст та оформлення дисертації відповідають вимогам до кваліфікаційних наукових робіт. Вона є завершеною кваліфікаційною науковою працею, що виконана здобувачем особисто у вигляді спеціально підготовленого рукопису, містить висунуті автором для прилюдного захисту нові наукові положення та практичні результати, характеризується єдністю змісту і свідчить про особистий науковий внесок здобувача.

Оцінка обґрунтованості наукових положень дисертації, їх наукової новизни та достовірності.

Здобувачкою вперше одержані такі наукові результати:

1) удосконалено метод градієнтного спуску для генерування нелінійних таблиць заміни, що відрізняється від відомого обґрунтованим порядком застосування критеріїв при перевірці підстановок на відповідність криптографічним показникам, що дозволяє суттєво знизити час генерації S-блоків із визначеними криптографічними властивостями;

2) отримав подальший розвиток математичний метод оцінки колізійних властивостей неін'єктивних схем розгортання ключів блокових шифрів, що відрізняється застосуванням удосконаленої математичної моделі та більш ефективного математичного апарату та дозволяє отримати уточнену оцінку ймовірності колізії двох послідовностей раундових ключів;

3) запропоновано два методи пошуку одноpаундових диференціальних характеристик для визначеного класу ARX-шифрів, що дозволяють з низькою обчислювальною складністю отримувати оцінки практичної стійкості раундової функції блокового шифру визначеного класу до диференціального криптоаналізу;

4) отримали подальший розвиток методи пошуку багатораундових диференціальних характеристик для визначеного класу ARX-шифрів, що відрізняються вдосконаленим механізмом відбору вхідних різниць та формуванням початкової множини одноpаундових диференціальних характеристик, що дозволяє отримати оцінку практичної стійкості немодифікованого та неспрощеного блокового шифру визначеного класу до диференційного криптоаналізу.

Для усіх зазначених наукових результатів у тексті дисертації наведено теоретичне обгрунтування та експериментальні підтвердження. Окремо хочу підкреслити ретельність, з якою здобувачка описала усі модельні припущення для оцінювання практичної стійкості ARX-шифрів до диференціального криптоаналізу: наразі формальна теорія диференціального криптоаналізу ARX-криптосистем не розроблена, і така акуратність лише підкреслює якість та достовірність одержаних наукових результатів за даним напрямом.

До винесених на захист наукових результатів є такі **зауваження.**

1. Хоча в загальній постановці удосконалення методу градієнтного спуску для генерування S-блоків описано теоретично, через мінімізацію певної функції оцінки ефективності, практичне застосування методу вимагає експериментального обчислення багатьох параметрів, що викликано початковим орієнтуванням на конкретний метод. Аналітичні значення або оцінки значень даних параметрів невідомі через те, що обраний для удосконалення метод оперує не з усіма можливими S-блоками, а з достатньо малою їх підмножиною, на якій поведінка криптографічних параметрів є невідомою (а її визначення саме по собі становить цікаву наукову задачу). Через це оцінювана ефективність удосконаленого методу стає залежною від якості оцінювання відповідних параметрів, а сценарій використання вимагає спочатку повного перебору порядку застосування критеріїв. У той же час здобувачка використовує терміни «оптимальний S-блок» та «оптимальний метод генерації», що, на мою думку, недоречно в даному контексті: з математичної точки зору оптимальність прив'язана до сукупності критеріїв, які необхідно зазначати, та повинна бути строго формально доведена. Втім, не можна сперечатись, що зроблені здобувачкою вдосконалення дійсно суттєво пришвидшують пошук необхідних S-блоків, що несе значний практичний зиск. Було б цікаво подивитись, як запропоновані вдосконалення впливають на інші методи генерування криптографічно надійних S-блоків.

2. Розглянуті властивості неін'єктивних схем розгортання раундових ключів навіть за формулюванням схожі на властивості криптографічних геш-функцій, зокрема, на колізії геш-функцій; математичний апарат, який застосовується, також відповідає математичному апарату, який застосовується для оцінки появи других прообразів та колізій геш-функцій. На мою думку, вдале поєднання відомих результатів загального аналізу властивостей криптографічних геш-функцій із моделями та методами, які застосовує здобувачка для аналізу схем розгортання ключів, дозволило б суттєво посилити одержані наукові результати.

3. Розроблений легкий шифр «Кипарис» у тексті дисертації називається «постквантовим». Однак визначення стійкості того чи іншого криптографічного алгоритму до атак у квантовій моделі обчислень наразі становить складну задачу, а багато алгоритмів вважаються постквантово стійкими, виходячи з достатньо загальних міркувань. Оскільки в тексті дисертації не наводиться відповідного аналізу, на мою думку, треба користуватись таким означенням з обережністю.

4. На стор. 105-106 тексту дисертації здобувачка зазначає, що знайдені нею одноразундові диференціали для раундової функції шифру «Кипарис» не комбінувались у дворaундові. З теоретичної точки зору два одноразундових диференціали зі спільними частинами (вихідна різниця першого співпадає із вхідною різницею другого) завжди повинні комбінуватись у дворaундовий диференціал із ненульовою імовірністю появи. Оскільки диференціали для шифру «Кипарис» шукались експериментально, а у тексті дисертації наводяться не всі деталі реалізації, цікаво, які саме обмеження практичного пошуку не дозволили зкомбінувати одноразундові диференціали та чи не можна тут покращити метод пошуку та підсилити одержані результати.

5. На стор. 106-107 зазначається, що для пошуку багатораундових диференціалів для тривіалізації диференціалу другого раунду шифрування покладається вимога $\Delta Y = F(\Delta X)$, де ΔX та ΔY – ліва та права частини вхідної різниці, F – внутрішнє раундове перетворення шифру. Однак дана вимога дуже сильно обмежує множину доступних диференціалів, оскільки проходження вхідної різниці ΔX у вихідну $F(\Delta X)$ на функції F є випадковою подією із (зазвичай) не дуже високою імовірністю. На мою думку, розгляд інших можливих класів багатораундових диференціалів дозволить суттєво посилити одержані результати щодо практичної стійкості шифру «Кипарис» до диференціального криптоаналізу.

Виконання положень академічної доброчесності.

Винесені на захист наукові результати відображені у відповідних наукових публікаціях та апробовані на наукових та науково-практичних конференціях. Для тих наукових праць, в яких здобувачка не була єдиним автором, у дисертації чітко зазначено її особистий вклад як співавтора. Результати, одержані іншими

науковцями, включено у текст дисертації із належним оформленням та відповідними посиланнями. З огляду на зазначене, вважаю, що робота не містить ознак порушення академічної доброчесності.

ВИСНОВОК

Вважаю, що дисертація «Методи побудови та дослідження властивостей малоресурсних блокових шифрів та їх компонентів» за актуальністю обраної теми, змістом роботи, ступенем обґрунтованості наукових положень, висновків і рекомендацій, що сформульовані в роботі, їх достовірністю та новизною, повнотою їх викладу в опублікованих працях відповідає спеціальності 122 – Комп'ютерні науки та задовольняє вимогам наказу Міністерства освіти і науки України від 12.01.2017 р. № 40 «Про затвердження вимог до оформлення дисертацій» та «Тимчасового порядку присудження ступеня доктора філософії» (постанова Кабінету Міністрів України від 06.03.2019 р. № 167 зі змінами), а її автор, Родінко Марія Юріївна, заслуговує на присудження ступеня доктора філософії з галузі знань 12 – Інформаційні технології за спеціальністю 122 – Комп'ютерні науки.

Доцент кафедри математичних методів
захисту інформації
Фізико-технічного інституту
Національного технічного
університету України
«Київський політехнічний інститут
імені Ігоря Сікорського»,
кандидат технічних наук

Сергій ЯКОВЛЄВ

Підпис Сергія ЯКОВЛЄВА
засвідчую
Відділ кадрів
архівної
справи
№ 6