В.о. ученого секретаря спеціалізованої вченої ради
Д 26.062.17 д.т.н., проф. В.П. Кваснікову
Національний авіаційний університет
проспект Космонавта Комарова, 1
м. Київ, 03058, Україна

ВІДГУК

офіційного опонента д.т.н., доцента Терейковського Ігора Анатолійовича
на дисертацію Коркішко Лесі Мирославівни
«Методи та засоби маскованої арифметики для пристроїв систем захисту інформації»,
представлену на здобуття наукового ступеня кандидата технічних наук за спеціальністю 05.13.21 – «Системи захисту інформації»

Актуальність теми. Стрімкий розвиток новітніх інформаційних технологій та розповсюдження сучасних комп'ютерних систем та мереж, окрім надання якісних інформаційних послуг, зумовлюють і суттєве збільшення ризиків та можливих загроз інформаційній безпеці, загострюють існуючі протиріччя між необхідністю оброблення та передачі великих обсягів інформації у зазначені терміни та підвищення вимог до їх безпеки. Конфіденційність інформації, як правило, забезпечується методами симетричної та асиметричної криптографії. Сучасні алгоритми криптографічних перетворень є добре дослідженими та стійкими до багатьох методів математичного криптографічного аналізу. Разом з тим, недоліки у реалізаціях таких алгоритмів у реальних пристроях систем захисту інформації створюють передумови для успішного визначення ключів, з використанням атак, що використовують комбінування методів математичного аналізу алгоритмів, відомостей про їх реалізацію та результатів спостереження за роботою криптографічних пристроїв. Серед таких каналів спостереження одним із найбільш небезпечних є канал спостереження за енергоспоживанням пристрою при обробці даних з використанням ключової інформації. Для ускладнення проведення таких атак передбачають рандомізоване виконання алгоритмів шифрування (перемішування порядку виконання елементарних операцій, випадкова зміна шляху виконання алгоритму), спотворення справжньої залежності характеристик споживаної потужності (введення шуму чи збільшення його рівня), вирівнювання споживаної потужності при обробці різних даних (фільтрування, спеціальні логічні елементи, тощо). Таким рішенням притаманні недоліки в частині їх високої вартості та низької технологічності виготовлення, підвищеного енергоспоживання, зменшеної продуктивності обробки даних, складності програмної реалізації. Альтернативний шлях захисту від таких атак полягає у введенні невизначеності у рівень споживаної потужності пристрою шляхом рандомізування проміжних значень, які виникають у процесі обчислень криптографічного перетворення. При цьому дані обробляються у так званому «маскованому представленні», яке містить хоча б одну випадкову маску та результат виконання деякої операції маскування над початковими даними та усіма масками. З огляду на те, що збільшення кількості масок у маскованому представленні призводить до зменшення залежності споживаної потужності

від ключових даних та значного ускладнення атак на основі аналізу енергоспоживання, розробка методів та засобів виконання базових операцій, характерних для криптографічних перетворень шифрування, над даними у МП є актуальним напрямком наукових досліджень.

Тому можна вважати, що розробка і дослідження нових ефективних методів та засобів маскованої арифметики для пристроїв систем захисту інформації є *актуальною науково-практичною задачею*, що має теоретичне і практичне значення.

Актуальність дисертаційної роботи також підтверджується тим, що тематика дисертаційної роботи Коркішко Л.М. та одержані автором результати безпосередньо пов'язані з науково-дослідними роботами: 1) держбюджетна НДР Тернопільського національного економічного університету «Методи та засоби реалізації алгоритмів захисту інформації стійких до атак на реалізацію» (д. р. № 0105U008181), 2) держбюджетна НДР Тернопільського національного економічного університету «Паралельні методи та засоби реалізації алгоритмів захисту інформації в комп'ютерних мережах з використанням математичного апарату еліптичних кривих» (д. р. № 0109U000035), у яких здобувач брав участь у якості виконавця.

Метою дисертаційної роботи є підвищення ефективності захисту даних і ключів криптографічних алгоритмів від їх несанкціонованої реконструкції за допомогою інженерно-криптографічних атак на основі аналізу зміни споживаної потужності при реалізації цих алгоритмів у криптографічних операційних блоках термінальних обчислювальних пристроях комп'ютерних систем за рахунок побудови їх структур на основі операцій над даними у маскованому представленні із довільною кількістю масок.

Оцінка обґрунтованості та достовірності наукових положень, висновків та рекомендацій.

Викладені наукові положення, висновки є повністю обґрунтованими, а достовірність теоретичних положень підтверджується експериментальними даними та результатами верифікації методів маскованої арифметики. Отримані, під час експериментів, дані відповідають теоретичним висновкам роботи і повністю підтверджують їх.

У **вступі** автором представлена загальна характеристика роботи, обґрунтована актуальність наукової теми, сформульовані мета і задачі дослідження, відображено наукову новизну та практичну цінність отриманих результатів і висновків, наведено дані щодо їх апробації та впровадження.

У **першому розділі** проведено аналіз сучасних методів захисту від атак на основі аналізу споживаної потужності пристрою від параметрів та даних криптографічного перетворення. Споживана потужність пристрою залежить від енергоспоживання базових напівпровідникових структур (логічних елементів), з яких побудований пристрій, від хемінгової ваги/відстані оброблюваних даних та керуючих сигналів (чи їх послідовності). У результаті аналізу відомих методів захисту від таких атак встановлено, що ці методи не є досконалими і мають певні обмеження щодо практичного застосування для розв'язання завдання побудови криптографічних пристроїв. Встановлено, що перспективний метод захисту від атак на основі аналізу залежності споживаної потужності пристрою повинен дозволяти будувати як програмні, так і апаратні засоби шифрування вартості, не залежати від кількості даних, які обробляються, дозволяти реалізацію на існуючій технологічній базі із стандартними бібліотеками елементів інтегральних схем чи наборах команд процесора. Обґрунтовано, що таким вимогам відповідає

обробка даних у маскованому представленні із багатьма масками, що полягає у введенні невизначеності у рівень споживаної потужності пристрою шляхом рандомізування проміжних значень, які виникають у процесі обчислень криптографічного перетворення.

У **другому розділі** дисертації розроблено методи виконання базових операцій алгоритмів криптографічних перетворень над даними у маскованому представленні. Запропоновано методи виконання таких операцій над даними у маскованому представленні із довільною кількістю масок: диз'юнкції, кон'юнкції, обчислення оберненого елемента у полі $GF(2^N)$ із довільною кількістю масок, операцій табличного перетворення, перетворення маскованого представлення даних на основі суматора маскованих даних за модулем 2^N із одною маскою. Реалізацію розроблених методів здійснюють у такі етапи: спочатку для підвищення стійкості до атаки на основі аналізу споживаної потужності заданого порядку спочатку обирають кількість масок, рівну, чи більшу заданому порядку атаки на основі аналізу споживаної потужності. Далі генерують задану кількість випадкових незалежних масок, однакової розрядності до даних. Переводять дані із немаскованого представлення у масковане представлення. Після цього дані у маскованому представленні обробляють згідно з розробленими методами, використовуючи, за необхідності додатково згенеровані маски. Якщо обробку даних необхідно продовжити, то дані у маскованому представленні використовують у подальших обчисленнях. За необхідності остаточний результат обчислень переводять із маскованого представленні у звичайне представлення. Використані додаткові маски повторно не використовують.

У **третьому розділі** дисертаційної роботи автором розроблено структури криптографічних операційних блоків обробки даних у маскованому представленні. Також автором досліджено характеристики структур цих блоків. У результаті порівняння розроблених структур криптографічних операційних блоків на основі розроблених у другому розділі методів із відомими структурами встановлено, що розроблені структури придатні як для програмної, так і для апаратної реалізації. За рахунок використання існуючих стандартних бібліотек елементів напівзамовлених інтегральних схем досягається низька вартість, низьке енергоспоживання та висока технологічність апаратної реалізації та отримання нових якостей – повного маскування результату, використанні нової маски результату, підтримки різнотипного маскування, адаптування до довільної кількості масок.

У **четвертому розділі** роботи здобувач проводить верифікацію та дослідження розроблених методів на основі дослідженні поведінкових програмних Verilog-моделей структур обчислювальних блоків виконання операцій над даними у маскованому представленні. Такі моделі використано для подальшого створення та дослідження ядер апаратно-орієнтованих процесорів симетричного блокового шифрування даних у маскованому представленні для систем захисту інформації. У роботі розроблено програмні поведінкові Verilog-моделі процесорів шифрування даних за алгоритмами mCrypton та ГОСТ28147-89 із даними у масковане представленні із використанням логічного маскування та однією маскою, виконання базових операції яких можна здійснюється за допомогою розроблених у третьому розділі структур операційних блоків.

Розроблено систему моделювання, яка дозволяє контролювати входи моделей процесорів та отримувати від симулятора інформацію про хемінгову вагу усіх міжз'єднань із файлу активності складових елементів моделі. Цей

файл разом із інформацією про паразитні зв'язки, використано для аналізу споживаної потужності у динаміці. Порівняно стійкість розроблених моделей процесорів до атаки на основі аналізу споживаної потужності з використанням аналізу кореляційних коефіцієнтів без використання маскованого представлення даних та з його використанням.

У **додатках** вміщено акти впровадження результатів дисертаційної роботи, опис атак на основі аналізу споживаної потужності на основі кореляційних коефіцієнтів, використаних для реалізації практичної частини дисертаційного дослідження.

Наукова новизна отриманих результатів полягає передусім у тому, що: вперше запропоновано метод виконання операції диз'юнкції над даними у маскованому представленні, масштабований до кількості масок даних у їх маскованому представленні; вперше запропоновано метод перетворення маскованого представлення даних, що дозволяє перетворювати масковане представлення даних із арифметичним маскуванням у дані із логічним маскуванням та навпаки; отримав подальший розвиток метод виконання операції кон'юнкції над даними у маскованому представленні, що є масштабований до кількості масок даних у їх маскованому представленні; отримав подальший розвиток метод інвертування даних у маскованому представленні у полях виду $GF(2^N)$, що дозволяє обробляти дані із довільною кількістю масок; удосконалено метод табличних перетворень даних у маскованому представленні, що дозволяє виконувати табличні перетворення над вхідними даними як із логічною, так і з арифметичною масками.

Основні положення дисертації опубліковано у 21 науковій праці, у тому числі 2 розділи у закордонних монографіях, 10 статей у наукових журналах та збірниках наукових праць, які входять до переліку фахових наукових видань МОН України (серед них 2 статті у виданнях, що входять до міжнародних наукометричних баз даних), а також 9 тез доповідей і матеріалів конференцій.

Результати дисертаційного дослідження *достатньо апробовані* на науково-технічних конференціях і семінарах різного рівня, зокрема, на International Workshop on Information Security Applications (WISA), Південна Корея, 2004, міжнародній конференції "Комп'ютерні науки та інформаційні технології" (CSIT), м. Львів, 2006, міжнародній конференції "Комп'ютерні науки та інженерія" (CSE), м. Львів, 2006, 2007, Науковій конференції Тернопільського державного технічного університету ім. І.Пулюя, м. Тернопіль, 2007, International Science Conference "Internet in the information society" (IIS), м. Домрова Гурніца, Польща, 2007, International Workshop on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS), м. Дортмунд, Німеччина, 2007, м. Варшава, Польща, 2015, International Conference Advanced Computer Systems and Networks: Design and Application (ACSN), м. Львів, International conference on modern problems of telecommunication, computer science and engineering training (TCSET), Львів-Славське, 2008.

Варто також зауважити, що основні положення дисертації та зміст автореферату повністю ідентичні.

Цінність для практики становлять: отримані в дисертаційній роботі результати можуть бути використані для розширення варіантів побудови криптографічних операційних блоків апаратних або програмних систем захисту інформації; створені програмні Verilog-моделі структур криптографічних ОБ виконання операцій кон'юнкції та диз'юнкції, додавання

за модулем 2^N, пошуку інвертованого елемента у полі $GF(2^N)$ для даних у маскованому представленні із довільною кількістю логічних масок, орієнтованих на подальше використання при створенні та дослідженні ядер спеціалізованих апаратно-орієнтованих криптографічних процесорів, що підтверджується актом про їх використання у науково-дослідних роботах Тернопільського національного економічного університету (акт від 18.06.2015); створені програмні Verilog-моделі ядер спеціалізованих апаратно-орієнтованих процесорів симетричного блокового шифрування, які обробляють дані із одною логічною маскою та володіють підвищеною стійкістю до атак на основі аналізу споживаної потужності, що підтверджується актом про впровадження у діяльність Інституту передових технологій Самсунг Електронікс (Республіка Корея) (акт від 11.01.2011); розроблені алгоритми оцінки характеристик складності криптографічних блоків для виконання операцій кон'юнкції, диз'юнкції, додавання за модулем 2^N, табличних операцій, перетворення МП даних, пошуку інвертованого елемента у полі $GF(2^N)$ впроваджені у начальний процес підготовки фахівців у галузі інформаційної безпеки, що підтверджується актами про впровадження у навчальний процес Університету в Бєльсько-Бялій (Польща) (акт від 30.06.2015), Тернопільського національного економічного університету (акт від 18.06.2015), Тернопільського національного технічного університету імені І. Пулюя (акт від 21.06.2016).

Зауваження:

1. Відсутність структурної схеми розробленого методу виконання операції інвертування даних дещо ускладнює сприйняття отриманих результатів.
2. На сторінці 13 підрозділу 1.1 в одних дужках забагато посилань на літературні джерела.
3. Сформульовані в тексті дисертації обмеження на використання запропонованого автором методу перетворення маскованого представлення даних не досить чітко визначають сферу його застосування.
4. Автору варто було б більш докладно обґрунтувати застосування розроблених ним програмних Verilog-моделей ядер спеціалізованих апаратно-орієнтованих процесорів симетричного блокового шифрування.
5. В тексті дисертації не досить чітко визначені обмеження на використання запропонованого автором методу табличних перетворень даних у маскованому представленні.

Висновки:

Принагідно висловлені зауваження не занижують вартості дисертаційного дослідження та не впливають на його позитивну оцінку. Оцінюючи опоновану дисертаційну роботу загалом, вважаю, що вона є закінченою кваліфікаційною роботою, у ній розв'язана важлива науково-практична задача підвищення ефективності захисту даних і ключів криптографічних алгоритмів від їх несанкціонованої реконструкції за допомогою інженерно-криптографічних атак на основі аналізу зміни споживаної потужності при реалізації цих алгоритмів у криптографічних операційних блоках термінальних обчислювальних пристроях комп'ютерних систем.

Вважаю, що представлена дисертаційна робота «Методи та засоби маскованої арифметики для пристроїв систем захисту інформації» відповідає усім вимогам «Порядку присудження наукових ступенів і присвоєння вченого звання старшого наукового співробітника», затвердженого Постановою КМУ від 24 липня 2013 року № 567, а її автор Коркішко Леся Мирославівна заслуговує присудження наукового ступеня кандидата технічних наук за науковою спеціальністю 05.13.21 – «Системи захисту інформації».

ОФІЦІЙНИЙ ОПОНЕНТ

Доктор технічних наук, професор
кафедри системного програмування і
спеціалізованих комп'ютерних
систем факультету прикладної математики
Національного технічного університету
України «Київський політехнічний інститут
імені Ігоря Сікорського»

Терейковський І. А.

Відділ кадрів і архівної справи № 6

Підпис гр.
ЗАСВІДЧУЮ
Відділ кадрів та діловодства
підпис пр-ще