ВІДГУК

офіційного опонента к.т.н. **Хохлачової Юлії Євгеніївни**

на дисертацію Коркішко Лесі Мирославівни «Методи та засоби маскованої арифметики для пристроїв систем захисту інформації», представлену на здобуття наукового ступеня кандидата технічних наук за науковою спеціальністю 05.13.21 – «Системи захисту інформації»

Актуальність

Інтенсивний розвиток інформаційних та комунікаційних технологій позитивно впливає на усі галузі діяльності людини, суспільства та держави, проте часто породжує множини неконтрольованих внутрішніх та зовнішніх загроз, які негативно відбиваються на характеристиках безпеки інформації. Одними з базових характеристик безпеки є конфіденційність даних. Для отримання конфіденційності повідомлень, наприклад за допомогою криптографічних перетворень симетричного блокового шифрування, засобами відправника проводять криптографічне перетворення даних – зашифрування – із використанням конфіденційного ключа. Засобами відправника виконується криптографічне перетворення – розшифрування – із використанням такого ж ключа. Конфіденційність даних, які передаються від відправника до отримувача ґрунтується на нерозголошенні ключа шифрування. Якщо ключ шифрування стає відомим порушнику, то властивість конфіденційності даних порушується, оскільки порушник може використати відомий йому ключ для перетворення розшифрування та отримати доступ до розшифрованого повідомлення. Загроза витоку ключа стає більш реалістичною, коли порушник володіє доступом або може спостерігати за роботою засобів шифрування. У цьому випадку порушник може скористатися інформацією із побічних каналів витоку інформації із засобів шифрування та провести на них так звані «інженерно-криптографічні» атаки з метою виявлення ключа шифрування. Одним із перспективних методів зниження загрози проведення таких успішних атак з використанням інформації про споживану потужність засобів шифрування є організація обчислень криптографічних перетворень з використанням маскованого представлення даних.

Дисертаційна робота Коркішко Лесі Мирославівни присвячена **актуальним питанням** побудови і дослідження методів та засобів виконання складових операцій криптографічних перетворень над даним у маскованому представленні. Актуальність дисертаційної роботи також підтверджується науково-дослідними та госпрозрахунковими роботами, з якими вона пов'язана:

1) «Методи та засоби реалізації алгоритмів захисту інформації стійких до атак на реалізацію» (№ 0105U008181);

2) «Паралельні методи та засоби реалізації алгоритмів захисту інформації в комп'ютерних мережах з використанням математичного апарату еліптичних кривих» (№ 0109U000035).

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.

Ідентичність змісту автореферату й основних положень дисертації

У авторефераті дисертації з необхідною повнотою відображено загальну характеристику, основний зміст та висновки дисертації. Структура дисертації відповідає вимогам, які ставляться до кандидатських дисертацій. Дисертаційна робота складається зі вступу, чотирьох розділів, загальних висновків, додатків, списку використаних джерел і має 144 сторінки основного тексту, 39 рисунків, 9 таблиць, 11 сторінок додатків. Список використаних джерел містить 126 найменувань і займає 16 сторінок. Загальний обсяг роботи 176 сторінок.

Результати дисертації викладено послідовно та структуровано, відповідно до поставлених задач дослідження.

У *вступі* автором представлена загальна характеристика роботи, обґрунтована актуальність, сформульовані мета і задачі досліджень, відображені наукова новизна і практична цінність отриманих результатів, наведено дані про їх апробації та впровадження.

У першому розділі виконаний аналіз сучасних методів захисту від атак на основі аналізу споживаної потужності від параметрів та даних криптографічного перетворення. Встановлено, що перспективний метод захисту від атак на основі аналізу залежності споживаної потужності пристрою повинен дозволяти будувати як програмні, так і апаратні засоби шифрування, не залежати від кількості даних, які обробляються, дозволяти реалізацію на існуючій технологічній базі із стандартними бібліотеками елементів інтегральних схем чи наборах команд процесора. Таким вимогам відповідає обробка даних у маскованому представленні, що полягає у введенні невизначеності у рівень споживаної потужності пристрою шляхом рандомізування проміжних значень, які виникають у процесі обчислень криптографічного перетворення.

У другому розділі розроблено методи виконання базових операцій алгоритмів криптографічних перетворень над даними у маскованому представленні. Перелік операцій над даними у маскованому представленні охоплює: операцію диз'юнкції, операцію кон'юнкції, операцію табличного перетворення даних, операцію інвертування у полі $GF(2^N)$, операцію перетворення типу маскованого представлення даних на основі суматора даних у маскованому представленні.

У третьому розділі розроблено структури та досліджено характеристики складності криптографічних операційних блоків обробки даних у

маскованому представленні. Проведено порівняння розроблених та відомих структур операційних блоків.

Четвертий розділ присвячений розробці програмних моделей поведінкових Verilog-моделей структур операційних 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 маскованому представленні із використанням логічного маскування однією маскою, виконання базових операцій яких здійснено за допомогою розроблених у третьому розділі структур операційних блоків.

Варто також зауважити, що для основних положень дисертації та змісту автореферату характерна повна ідентичність.

Наукове та практичне значення результатів дисертаційної роботи

Наукова новизна отриманих результатів дисертаційної роботи, на мою думку, перш за все, полягає у такому:

1) вперше запропоновано метод виконання операції диз'юнкції над даними у маскованому представленні, що, за рахунок обчислення функції корекції маски результату з використанням виключно даних у маскованому представленні та їх масок, дозволяє використати таку операцію для побудови структур криптографічних операційних блоків виконання операції диз'юнкції, масштабованих до кількості масок даних у їх маскованому представленні;

2) вперше запропоновано метод перетворення маскованого представлення даних, що, за рахунок використання операції додавання за модулем 2^N над даними у маскованому представленні, побудованої на основі маскованих логічних операцій, дозволяє перетворювати масковане представлення даних із арифметичним маскуванням у дані із логічним маскуванням та навпаки, а також використати таке перетворення для створення структур криптографічних операційних блоків, які використовують масковане представлення даних як з логічною, так і з арифметичною маскою;

3) отримав подальший розвиток метод виконання операції кон'юнкції над даними у маскованому представленні, що, за рахунок введення у функцію корекції маски результату обчислень з урахуванням усіх масок вхідних та вихідних даних, дозволяє використати таку операцію для побудови структур криптографічних операційних блоків виконання операції кон'юнкції, масштабованих до кількості масок даних у їх маскованому представленні;

4) отримав подальший розвиток метод інвертування даних у маскованому представленні у полях виду $GF(2^N)$, що, за рахунок введення у функцію корекції маски результату обчислень з урахуванням усіх масок вхідних та вихідних даних, дозволяє обробляти дані із довільною кількістю масок, а також використати таке перетворення для побудови структур

криптографічних операційних блоків інвертування даних у полях виду $GF(2^N)$, які використовують табличні методи виконання операцій у цих полях;

5) удосконалено метод табличних перетворень даних у маскованому представленні, що, за рахунок введення додаткового проміжного маскування із узгодженим типом маски вхідних даних, дозволяє виконувати табличні перетворення над вхідними даними як із логічною, так і з арифметичною масками та отримувати результат із заданим типом маскування, а також дозволяє використати таку операцію для побудови структур криптографічних операційних блоків табличної заміни засобів шифрування даних у маскованому представленні.

Практичне значення результатів дисертації полягає у наступному:

1) створені програмні Verilog-моделі структур криптографічних операційних блоків 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 спеціалізованих апаратно-орієнтованих криптографічних процесорів, що підтверджується актом про їх використання у науково-дослідних роботах Тернопільського національного економічного університету (акт від 18.06.2015);

2) 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);

3) розроблені алгоритми оцінки характеристик складності криптографічних блоків для виконання операцій кон'юнкції, диз'юнкції, додавання за модулем 2^N, табличних операцій, перетворення маскованого представлення 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).

Результати дисертаційної роботи впроваджено в науково-дослідних роботах Тернопільського національного економічного університету, Інституту передових технологій Самсунг Електронікс (Республіка Корея), в навчальному процесі Університету в Бєльсько-Бялій (Польща), Тернопільського національного економічного університету, Тернопільського національного технічного університету імені І. Пулюя, що підтверджено відповідними актами впровадження.

Оцінка висновків здобувача щодо значущості його праці для науки й практики.

Дисертаційна робота полягає у побудові та дослідженні методів та засобів виконання складових операцій криптографічних перетворень над даними у маскованому просторі. Крім того розроблено методи виконання базових операцій для криптографічних операційних блоків, які оперують даними у маскованому представленні: логічних (кон'юнкції, диз'юнкції) із довільною кількістю масок, арифметичних (обчислення зворотного елемента за модулем 2N, додавання за модулем 2N), табличних операцій, операцій перетворення маскованого представлення даних; розроблено структури криптографічних операційних блоків, масштабованих до кількості масок та досліджено їх характеристики складності при їх апаратній реалізації; розроблено та експериментально досліджено програмні моделі ядер спеціалізованих апаратно-орієнтованих процесорів симетричного блокового шифрування даних у маскованому представленні

У вступі, висновках по розділах, особливо у третьому та четвертому розділах дисертації здобувачем наведені данні щодо можливості застосування результатів дисертації, що дає підставу зробити висновки про її важливість для науки й практики при створенні та організації пристроїв систем захисту інформації.

Повнота викладу результатів дисертаційної роботи в опублікованих працях та їх апробація

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, а також 9 тез доповідей і матеріалів конференцій.

Дисертація Коркішко Л.М. має достатній рівень апробації на наукових конференціях і семінарах. Наведений перелік публікацій, їх зміст та обсяг відповідають темі дисертації, у повному обсязі відображають отримані положення, наукові результати та висновки, свідчать про їх новизну.

Можливі шляхи використання результатів дисертаційних досліджень.

Отримані в дисертаційній роботі нові теоретичні положення доцільно використовувати в наукових дослідженнях і навчальному процесі науково-педагогічним колективом Тернопільського національного економічного університету та інших навчально-наукових організацій, пов'язаних із питаннями дослідження сучасних інформаційних технологій та систем, а також методів, засобів та принципів захисту інформації.

Ідентичність змісту автореферату й основним положенням дисертації.

Автореферат відповідає змісту та основним положенням дисертації.

Відповідність теми та змісту дисертації паспорту спеціальності, за якою вона подана на захист.

Тема дисертації та її зміст відповідають формулі й галузі досліджень паспорта спеціальності 05.13.21 – "Системи захисту інформації", оформлена відповідно до вимог значних стандартів.

Недоліки та зауваження по роботі

1. У підрозділі 2.2 автор наводить методи для виконання табличних перетворень над даними у маскованому представленні. Однак, незрозуміло, чому автор не пропонує використовувати ці ж табличні перетворення для виконання логічних та арифметичних операцій над даними у маскованому представленні, зокрема для виконання операцій арифметичного додавання за модулем 2^N.
2. У третьому розділі дисертації (стор. 77, п. 3.1.3) для реалізації суматора даних у маскованому представленні обрана схема суматора із послідовним переносом. Автором не наведено варіанти схем для інших структур суматорів, наприклад, із паралельним переносом, із прискореним переносом, тощо.
3. У третьому та четвертому розділах, зокрема на стор. 70, 71, 73, 74, 83, 85, 111, використовується вирази «апаратне відображення потокового графу алгоритму» та «апаратне відображення згортки потокового графу алгоритму», однак автором не наведено пояснення цих виразів.

У тексті дисертації використано різні позначення для обробки даних у $GF(2^N)$. Так, на стор. 38, 39, 47 – 50, тощо, використано термін «інвертування», а на стор. 12, 28, 30, 46, 63 – 65, 80 – 88, тощо – термін «обернення» чи «знаходження оберненого елемента». Крім цього, на стор. 116, 117, 199, 139 використано термін

«маскований суматор», що відрізняється від введеного на стор. 59 означення «суматор даних у маскованому представленні». Вживання таких різних термінів ускладнює розуміння викладу дисертації.

5. У четвертому розділі на стор. 120 при наведенні підходів до реалізації процесорів, які обробляють дані у маскованому представленні, автором не уточнено спосіб зберігання ключа у маскованому представленні та відповідної йому маски. Доцільно було б описати етапи завантаження ключа, його маскування, зберігання маски, оновлення маски при роботі процесора.

6. У висновках до другого розділу у першому абзаці (стор. 66) є описка «Зокрема, запропоновано метод виконання операції диз'юнкції, розвинуто методи виконання операції *диз'юнкції* та інвертування…». Замість цього необхідно написати «…розвинуто методи виконання операції *кон'юнкції* та інвертування…».

7. В тексті дисертації та авторефераті присутні незначні стилістичні та орфографічні помилки.

Висновки

Зазначені недоліки не є суттєвими та критичними і не впливають на загальну позитивну оцінку роботи здобувача. У цілому дисертаційна робота Коркішко Лесі Мирославівни «Методи та засоби маскованої арифметики для пристроїв систем захисту інформації» є закінченою науковою працею, яка містить нові науково обґрунтовані теоретичні та експериментальні результати, що у сукупності є суттєвими для забезпечення конфіденційності даних, які обробляються в інформаційно-комунікаційних системах.

Матеріал дисертації викладено послідовно, стиль викладання доказовий, чіткий і лаконічний. Висновки до кожного розділу і дисертації в цілому тісно пов'язані з їх змістом і відображають суть виконаних досліджень. Публікації автора повністю висвітлюють наукові положення і результати дисертації.

Вважаю, що дисертаційна робота «Методи та засоби маскованої арифметики для пристроїв систем захисту інформації» повністю відповідає вимогам «Порядку присудження наукових ступенів», затвердженого Постановою КМ України від 24.07.2013 р. № 567 (із змінами, внесеними згідно з Постановами КМ України № 656 від 19.08.2015 р., № 1159 від 30.12.2015 р. № 567 від 27.07.2016 р.), а її автор Коркішко Леся Мирославівна заслуговує присудження наукового ступеня кандидата технічних наук за науковою спеціальністю 05.13.21 – «Системи захисту інформації».

Офіційний опонент

доцент кафедри безпеки інформаційних технологій
Національного авіаційного університету, к.т.н. Ю.Є. Хохлачова

Підпис Хохлачової Ю. Є.
засвідчую
Вчений секретар
Національного авіаційного університету
Г. Єчеба