Голові спеціалізованої вченої ради
ДФ 64.051.020
Харківського національного
університету імені В. Н. Каразіна
61022, майдан Свободи, 4, м. Харків

ВІДГУК

опонента, завідувача кафедри комп'ютерних систем, мереж і кібербезпеки факультету радіоелектроніки, комп'ютерних систем та інфокомунікацій Національного аерокосмічного університету імені М. Є. Жуковського «Харківський авіаційний інститут», доктора технічних наук, професора Харченка Вячеслава Сергійовича на дисертаційну роботу Лисицького Костянтина Євгенійовича «Методи та засоби побудови блокових симетричних шифрів з підвищеною стійкістю та швидкодією», що подана на здобуття ступеня доктора філософії з галузі знань 12 – Інформаційні технології за спеціальністю 122 – Комп'ютерні науки.

1. Актуальність обраної теми. Безпечне функціонування критичних і бізнес-критичних систем забезпечується з використанням технологій блочного симетричного шифрування (БСШ), які лідирують при побудові засобів захисту інформації. Подальший розвиток й удосконалення алгоритмів БСШ здійснюється в умовах появи квантових комп'ютерів і суттєвого розширення можливостей виконання криптоаналітичних атак на шифри. Існуючі системи шифрування не здатні або обмежено здатні протистояти квантовим методам аналізу, що обумовило інтенсивні дослідження щодо оцінювання та подальшого нарощування їх стійкості.

Постквантові виклики вимагають для БСШ використання блоків шифрування і ключів з довжиною більше 256 бітів, що призводить до зниження швидкодії алгоритмів шифрування. Отже, зберігається суперечлива необхідність подальшого збільшення стійкості і швидкодії реалізації шифрів, орієнтованих на використання у пост-квантовий період. Це обумовлює актуальність теми дисертації, присвяченої вдосконалюванню методів проектування БСШ з підвищеною стійкістю та швидкодією для умов пост-квантової криптографії.

2. Ступінь обґрунтованості наукових положень, висновків і рекомендацій, сформульованих у дисертації. Дисертація Лисицького К. Є. містить вступ, п'ять розділів, висновки, список використаних джерел та п'ять додатків. Загальний обсяг роботи складає 220 сторінок.

У першому розділі дисертації проведений аналіз стану розвитку методів і технологій БСШ з урахуванням особливостей постквантового періоду. Він виконаний достатньо ретельно і надав можливість обґрунтувати і конкретизувати задачі досліджень.

Зауваження: огляд літератури, визначальним чином базується на аналізі результатів потужної наукової школи, які представляє дисертант, що є природнім. Однак, на наш погляд, доцільно було б зробити посилання і більш детально проаналізувати публікації інших науковців. Посилання на англомовні джерела обмежуються 2016 р., хоча є кілька публікацій останніх років, які слід було б взяти до уваги (наприклад, https://www.researchgate.net/publication/276854796_New_Approach_in_Symmetric_Block_Cipher_Security_Using_a_New_Cubical_Technique, https://www.researchgate.net/publication/287224352_Design_and_Analysis_of_New_Symmetric_Block_Cipher_Algorithm, https://core.ac.uk/download/pdf/231159887.pdf). Крім того, структурування розділу не виглядає бездоганним, оскільки не досить зрозуміло, чому особливості сучасного етапу розвитку криптографії (п.1.4) аналізуються після того, як проведено аналіз методів і засобів БСШ (пп.1.2,1.3).

У другому розділі дисертації обґрунтовується методологія оцінки стійкості блокових симетричних шифрів до атак диференціального та лінійного криптоаналізу. Цікавими і важливими є визначені автором умови приходу ітеративних шифрів до стаціонарного стану випадкової підстановки, розподіли максимумів повних диференціалів і зміщень лінійних оболонок, зокрема, для 128-бітних шифрів. Експериментально підтверджено, що криптографічні перетворення, властиві SPN конструкціям шифрів є збалансованими і якість перетворень практично не залежить від ключів шифрування.

Зауваження: зазначимо, що результати цього розділу фактично виходять за рамки задачі (як вона сформульована), оскільки запропонований автором підхід надає змогу отримати точні значення показників стійкості шифрів. Отже йдеться про підвищення точності оцінок стійкості. З іншого боку, цей результат можна розглядати як підсилення результатів, які стосуються підвищення стійкості, бо підвищення точності оцінювання безпосередньо впливає на забезпечення необхідної стійкості шифрів. Автору доцільно було б чіткіше протрасувати цей зв'язок.

У третьому розділі розвивається підхід, сформований у попередньому розділі, і узагальнюються результати, присвячені формуванню моделі випадкової підстановки, яка безпосередньо впливає на обґрунтування методів оцінювання показників доказової стійкості БСШ до атак диференціального і лінійного криптоаналізу. Доводиться низка відповідних тверджень і теорем. Запропоновано використовувати як S-блоки шифрів випадкові підстановки з виходу генератора випадкових підстановок, які проходять перевірку на відповідність критеріям відбору.

Зауваження: розділ побудований у дещо незвичний спосіб як огляд наукових результатів, опублікованих у відповідних працях. Навіть нумерація тверджень і теорем не є

наскрізною. Це дещо ускладнює розуміння рамок нових наукових положень власне дисертаційного дослідження.

Четвертий розділ уточнює за допомогою обчислювальних експериментів значення динамічних показників приходу ряду сучасних шифрів до стану випадкової підстановки, які можуть стати важливими при порівняльній оцінці їх ефективності. Досліджено відповідні властивості шифрів Rijndael, IDEA NXT, Мухомор, Білоруський шифр, Калина-2, Camelia. Автор на підставі теоретичних і експериментальних досліджень обґрунтовує і розробляє оригінальний метод оцінювання ефективності БСШ.

Зауваження: цей розділ також побудований у оглядовому стилі, хоча структурується дещо у інший спосіб. П. 4.1 має назву «Стислий огляд попередніх результатів досліджень», далі уточняється методика і реалізуються експериментальні дослідження. Такий варіант подання результатів має право на використання, але не вистачає загальної «дорожньої карти» досліджень з фіксацією і описом зв'язків наукових результатів. Крім того, результати активізації S-блоків за диференціальними показниками слід доповнити аналогічними результатами за лінійними показниками.

У п'ятому розділі запропоновано удосконалені методи проєктування БСШ з суттєво поліпшеними динамічними показниками приходу до стану випадкової підстановки, орієнтованих на використання у постквантовій криптографії. Автору вдалося побудувати шифри зі зменшеною кількістю циклових перетворень без втрати стійкості, що забезпечує підвищення продуктивності алгоритмів шифрування. Крім того, запропоновано просту схему розгортання ключів, яка не прив'язана до процедури шифрування, що забезпечує відсутність самоподібності циклових підключів при їх формуванні.

Зауваження: розділ є ключовим і насичений низкою результатів, які визначають задачу і мету досліджень. Доцільно було б запропонувати загальну послідовність використання і взаємозв'язки всіх запропонованих моделей і методів.

В цілому слід зазначити, що наукові основні результати і висновки всебічно обґрунтовані. Їх достовірність підтверджується коректністю використання сучасних методів досліджень (теорії ймовірностей, математичної статистики, системного аналізу, методів статистичних випробувань і прикладної криптографії), строгим доведенням сформульованих тверджень і теорем, великим обсягом експериментальних досліджень і збігом їх результатів з аналітичними моделями, а також практичним впровадженням результатів.

3. Наукова новизна результатів досліджень полягає у наступному:

1. Удосконалено метод оцінювання показників доказової стійкості блокових симетричних шифрів до атак диференціального і лінійного криптоаналізу, який на відміну від відомих будується на основі використання теоретичних значень максимумів законів розподілу переходів XOR таблиць (повних диференціалів) і змішень таблиць ЛАТ (лінійних

корпусів) шифруючих перетворень, які розглядаються як випадкові підстановки, що забезпечує підвищення точності оцінювання.

2. Вперше запропоновано методи проєктування SPN блокових симетричних шифрів з поліпшеними динамічними показниками приходу до стану випадкової підстановки, які надають змогу збільшити мінімальну кількість S-блоків, що активізуються на перших циклах шифруючих перетворень, зокрема:

- метод використання в першому циклі SPN шифру збільшеного числа S-блоків на основі реалізації двошарової його конструкції;

- метод побудування першого циклу шифру за допомогою шару керованих укрупнених S-блоків, що з'єднані шляхом послідовного їх включення з додаванням чергового сегменту даних до входу кожного S-блоку циклової функції зі складанням виходу останнього укрупненого S-блоку з виходами інших,

- метод побудування всієї конструкції шифру з використанням принципів послідовного включення укрупнених S-блоків в ланцюжок з додаванням чергового сегменту даних до входу кожного укрупненого S-блоку циклової функції зі складанням виходу останнього укрупненого S-блоку з виходами інших.

Крім того, обґрунтовано можливість побудування шифрів з використанням випадкових S-блоків з підвищеними показниками стійкості й швидкодії для умов застосування квантових комп'ютерів.

3. Вперше запропоновано метод визначення кількості циклів приходу шифру до показників випадкової підстановки на основі врахування мінімальної кількості тільки тих активних S-блоків, що припадають на перші цикли перетворень, беруть участь у формуванні граничних значень диференціальної та лінійної ймовірностей і забезпечують підвищення точності оцінювання криптостійкості.

4. Вперше визначено й експериментально підтверджено закони розподілу максимумів (екстремальні розподіли) переходів XOR таблиць і зміщень таблиць лінійних апроксимацій шифрів, що дозволило підтвердити гіпотезу стосовно досить малого діапазону зміни максимумів повних диференціалів і максимумів зміщень лінійних корпусів сучасних шифрів та їх практичну незалежність від ключового матеріалу.

5. Набула подальшого розвитку модель випадкової підстановки, яка визначається значеннями максимумів таблиць диференціальних різниць і зміщень таблиць лінійних апроксимацій підстановок, близькими до значень максимумів екстремальних законів розподілу переходів XOR таблиць і зміщень таблиць лінійних апроксимацій випадкових підстановок, що забезпечує використання як випадкових підстановок в шифрах безпосередньо підстановок, породжених випадковим генератором підстановок.

Зауваження. Формулювання наукової новизни опонентом в цілому співпадає з авторським, викладеним у вступі, за виключенням деяких стилістичних відмінностей і корективів, а також внаслідок об'єднання деяких результатів. Зазначимо, що автором формулювання нових наукових положень зроблено достатньо розгорнуто і в кількох розділах дисертації.

В цілому слід зробити висновок про високий науковий рівень дисертації, великий обсяг нових наукових результатів, які є суттєвим внеском в розвиток теорії і методів розроблення блочних симетричних шифрів.

4. Повнота викладу результатів у наукових публікаціях, що відповідають темі дисертації. Нові наукові результати достатньо повно викладено у 11 статтях, серед яких 2 статті у фахових наукових журналах, які входять до переліку МОН України, 2 статті в науковому закордонному виданні, 2 статті – виданнях, включених до наукометричних баз Scopus і Web of Science. Загальна кількість основних публікацій – 15. В дисертації автор посилається на інші власні (додаткові) публікації, що сприяє більш повному і поглибленому поясненню результатів виконаних досліджень.

5. Практичне значення результатів полягає у тому, що запропоновані методи розроблення БСШ реалізовано в системах криптографічного захисту при виконанні державних НДР (ЗАТ «Інститут інформаційних технологій», Харківського національного університету імені В. Н. Каразіна, Харківського національного університету радіоелектроніки і навчальному процесі кафедри БІСТ ХНУ імені В. Н. Каразіна, що підтверджено відповідним чином оформленими актами.

6. Оцінка академічної доброчесності. Після вивчення тексту дисертації та ознайомлення із науковими працями можна зробити висновок, що робота виконана самостійно та не містить ознак порушення академічної доброчесності.

7. Зауваження та недоліки. Більшу частину зауважень надано в пп. 2,3. Крім того, слід зазначити наступне:

- є певні відмінності у формулюванні мети досліджень у вступі («удосконалення методів побудови блокових симетричних шифрів з підвищеною криптостійкістю і швидкодією в умовах можливого застосування квантових методів криптоаналізу») і першому розділі («підвищення (забезпечення) потрібної стійкості блокових симетричних шифрів при суттєвих обмеженнях на складність їх практичної реалізації в умовах можливого застосування квантових комп'ютерів»);

- більш системно слід було б надати методику (етапи, математичний апарат) досліджень, зв'язок результатів та їх впровадження;

- кращою могла б бути критеріальна частина дисертації та більш детальними розрахунки стосовно підвищення швидкодії;

- є певні вади оформлення, мовні та стилістичні некоректності.

Зауваження не впливають на кінцевий позитивний висновок щодо оцінки наукового рівня і практичної цінності дисертаційного дослідження.

8. Висновки. Дисертаційна робота Лисицького К. Є. «Методи та засоби побудови блокових симетричних шифрів з підвищеною стійкістю та швидкодією» є завершеним науковим дослідженням, виконаним за актуальною тематикою, має наукову і практичну значимість. Тема і зміст роботи відповідають спеціальності 122 – Комп'ютерні науки. Вимоги «Тимчасового порядку присудження ступеня доктора філософії», затвердженого постановою Кабінету міністрів України від 06.03.2019 р. № 167 (зі змінами) дотримано. Дисертація оформлена у відповідності із наказом Міністерства освіти і науки України від 12.01.2017 р. № 40 «Про затвердження вимог до оформлення дисертацій».

Вважаю, що Лисицький Костянтин Євгенійович заслуговує на присудження ступеня доктора філософії з галузі знань 12 – Інформаційні технології за спеціальністю 122 – комп'ютерні науки.

28.08.2021 р.

Опонент
завідувач кафедри комп'ютерних систем, мереж і кібербезпеки факультету радіоелектроніки, комп'ютерних систем та інфокомунікацій Національного аерокосмічного університету ім. М. Є. Жуковського «Харківський авіаційний інститут»
Лауреат Державної премії України у галузі науки і техніки,
заслужений винахідник України,
доктор технічних наук, професор — Вячеслав ХАРЧЕНКО

Підпис професора Харченка Вячеслава Сергійовича засвідчую.
Вчений секретар Національного аерокосмічного університету ім. М. Є. Жуковського «Харківський авіаційний інститут» кандидат філософських наук, доцент — Світлана ЧМИХУН