

ВІДГУК

офіційного опонента

на дисертаційну роботу Короткого Тимофія Костянтиновича на тему
«Ієрархічна інформаційна система моделювання і дослідження алгоритмів
потокowego СЕТ-шифрування», подану на здобуття наукового ступеня
доктора філософії за спеціальністю 126 – Інформаційні системи та технології
галузі знань 12 – Інформаційні технології

1. Актуальність теми дослідження та зв'язок з науковими програмами, планами та темами.

У сучасних умовах інформаційні системи і технології стали важливим інструментом науково-технічного прогресу, економіки та сталого розвитку суспільства. Вони використовуються в різних областях народного господарства, сприяють інтенсифікації впровадження наукових результатів як на рівні держави так і на рівні користувачів інформаційними послугами. В галузі кібербезпеки існує значна кількість інформаційних технологій направлених на оцінку якості систем захисту інформації включаючи криптографію. Проте технологіям підтримки процесів проектування систем захисту не приділялося достатньої уваги. В умовах військового стану інтенсифікації розробок малоресурсних постквантових систем потокowego шифрування стала однією з задач від вирішення якої залежить результат як інформаційного, так і науково-технічного протистояння. Таким чином, тема дисертаційної роботи «Ієрархічна інформаційна система моделювання і дослідження алгоритмів потокowego СЕТ-шифрування» є актуальною.

Крім того, актуальність і практичне значення даної наукової роботи підтверджується виконанням двох науково-дослідних робіт: «Дослідження шляхів розвитку потокowego шифрування на основі криптографічного кодування» (ДР № 0121U114389); «Інформаційна технологія психолінгвістичного аналізу тексту для стеганографічних систем» (ДР № 0123U102085), у яких автор брав участь як виконавець.

2. Ступінь обґрунтованості наукових положень, висновків і рекомендацій.

Наукові положення, висновки і рекомендації дисертаційної роботи Короткого Тимофія Костянтиновича є обґрунтовані, підтверджені коректним використанням основ теорії інформації, алгоритмів, ймовірності,

криптографії із застосуванням методів дискретної математики, математичної статистики та комп'ютерного моделювання.

Обґрунтованість і достовірність наукових положень, висновків і рекомендацій забезпечено комплексним характером досліджень, публікаціями у журналах включених до науково-метричної бази SCOPUS і в фахових виданнях категорії Б, обговоренням висунутих наукових положень та отриманих висновків на міжнародних та національних науково-технічних конференціях, проведенням обчислювальних експериментів. Отримані результати відповідають висунутим теоретичним положенням.

3. Наукова новизна результатів роботи.

На основі аналізу результатів дисертаційної роботи Короткого Т.К. можна зробити висновок, що найбільш суттєвими науковими результатами, які одержані в дисертації, є такі:

1) вперше побудована модель ієрархічної інформаційної системи моделювання і дослідження симетричних і несиметричних СЕТ-операцій, на основі методів синтезу СЕТ-операцій і груп СЕТ-операцій, шляхом вдосконалення моделей, методів і технології побудови комутативних і некомутативних СЕТ-операцій, а також генераторів псевдовипадкових наборів СЕТ-операцій, що дозволило встановлювати нові залежності між моделями синтезу симетричних і несиметричних операцій, які приводять до розширення взаємозв'язків між моделями ієрархічних рівнів інформаційної системи, реалізація якої забезпечить експериментальну підтримку для побудову перспективних стійких мало ресурсних алгоритмів потокового шифрування;

2) удосконалено технологію побудови удосконалених моделей некомутативних двохрандних двохрандних СЕТ-операції за результатами експерименту, на основі побудови удосконалених моделей СЕТ-операцій за результатами експерименту, шляхом встановлення взаємозв'язків між моделями до і після перестановки операндів, що забезпечило зменшення складності моделювання некомутативних СЕТ-операцій на основі реалізації прямого переходу від побудованої моделі СЕТ-операції до моделі СЕТ-операції з переставленими операндами;

3) удосконалено метод синтезу двохрандних двохрандних операцій криптографічного перетворення на основі метод синтезу симетричних операцій, шляхом застосування в якості першої базової операції несиметричної операції криптоперетворення та додаткової побудови

оберненої операції за результатами обчислювального експерименту, що забезпечили можливість додаткового синтезу несиметричних двохоперандних двохранрядних операцій подвійного циклу;

4) удосконалено метод побудови двохранрядних двохоперандних операцій, які допускають перестановку операндів, на основі об'єднання двохранрядних однооперандних операцій криптографічного перетворення, шляхом встановлення взаємозв'язків між прямими і оберненими операціями, що дозволило змодельовати всі двохранрядні двохоперандні операції, які допускають перестановку операндів.

4. Зміст дисертації та відповідність встановленим вимогам

Дисертаційна робота є завершеною науковою працею, яка містить вступ, п'ять розділів, висновки, список використаних джерел із 103 найменувань та 3 додатків на 10 сторінках. Дисертація має 190 сторінки, з яких 158 містять основний текст. У роботі є 13 рисунків і 15 таблиць. Побудова дисертації відповідає прийнятим для наукового дослідження вимогам.

У **вступі** обґрунтовано актуальність теми досліджень; показано зв'язок роботи з науковими програмами, планами, темами; сформульовано мету та основні задачі досліджень; подано наукову новизну і практичне значення отриманих результатів; визначено особистий внесок здобувача; наведено дані про апробацію, публікації та використання результатів дослідження.

У **першому розділі** проведено аналіз напрямків розвитку моделей і систем малоресурсної криптографії, включаючи СЕТ-шифрування. Проаналізовані інформаційні системи моделювання СЕТ-операцій та ієрархічна технологія дослідження симетричних СЕТ-операцій. На основі виявлених недоліків сформульована мета і завдання дослідження.

У **другому розділі** досліджуються некомутативні двохранрядні двохоперандні СЕТ-операції подвійного і потрійного циклу, які допускають перестановку операндів. Удосконалюється технологія побудови моделей некомутативних двохранрядних двохоперандних СЕТ-операцій.

Третій розділ присвячено побудові і дослідженню моделей несиметричних двохоперандних двохранрядних СЕТ-операцій. Удосконалюється метод синтезу двохоперандних двохранрядних СЕТ-операцій.

Четвертий розділ присвячено побудові і дослідженню моделей груп несиметричних двохоперандних двохранрядних СЕТ-операцій.

Удосконалюється метод побудови двохрозрядних двохоперандних операцій які допускають перестановку операндів на основі об'єднання двохрозрядних однооперандних операцій криптографічного перетворення.

П'ятий розділ присвячено інформаційній технології моделювання комутативних і некомутативних двохоперандних СЕТ-операцій для малоресурсних поточкових шифрів. Досліджуються моделі генераторів псевдо випадкових послідовностей СЕТ-операцій. Будується модель ієрархічної інформаційної системи моделювання і дослідження симетричних і несиметричних СЕТ-операцій.

У **висновках** стисло сформульовано основні наукові та практичні результати дисертаційної роботи.

У **додатках** містяться результати обчислювального експерименту, акти впровадження результатів дисертаційної роботи та список публікацій, в яких опубліковані основні наукові результати дисертації.

Таким чином, усі положення винесені на захист, висвітлені в тексті дисертації. Зміст дисертаційної роботи відповідає її назві. Дисертація написана науковою мовою та оформлена відповідно до існуючих нормативних документів.

5. Оформлення дисертації.

Дисертаційна робота оформлена у відповідності з чинними вимогами, що ставляться до такого виду робіт. Дисертація має завершену обґрунтовану структуру та форму представлення, що повною мірою розкриває досягнуту мету та виконані завдання дослідження.

6. Практичне значення результатів дисертаційної роботи.

Практичне значення результатів дисертаційної роботи полягає у розробці алгоритмічного забезпечення макету ієрархічної інформаційної системи моделювання і дослідження алгоритмів поточкового СЕТ-шифрування. Реалізація даного макету розширила можливості автоматизації процесів моделювання мало ресурсних поточкових СЕТ-шифрів, та теоретично зменшує час отримання необхідних результатів.

Практична цінність роботи підтверджується наявністю у здобувача двох актів впровадження у навчальний процес Черкаського державного технологічного університету.

7. Повнота викладу результатів в опублікованих працях, апробація роботи.

Основні результати дисертації достатньо повно **відображені** в 16 друкованій праці, з них, 3 статтях, які індексуються у науково-метричній базі Scopus, 5 статтях у фахових виданнях України, одноосібному розділі колективної монографії, 2 статтях опублікованих за кордоном, 4 тезах доповідей на міжнародних і вітчизняних конференціях та форумах. Опубліковані роботи в повній мірі охоплюють основні результати дисертаційних досліджень. Дисертація є завершеною кваліфікаційною роботою з науковими положеннями, які характеризуються внутрішньою єдністю. Аналіз сукупності наукових результатів, поданих у роботі Короткого Т.К, дає змогу зробити висновок про їх цілісність і засвідчує особистий внесок автора в науку щодо розроблення ієрархічна інформаційної системи моделювання і дослідження алгоритмів потокового СЕТ-шифрування

8 Відсутність (наявність) порушень принципів академічної доброчесності.

Ознайомившись із змістом дисертаційної роботи можна зробити висновок, що наукові положення дисертації і висновки мають авторське обґрунтування. Ознак порушення академічної доброчесності не встановлено.

9. Зауваження до дисертації та реферату.

Незважаючи на належний рівень виконаних наукових досліджень, до дисертаційної роботи виносяться такі зауваження:

1. В п.1.1. описуються відомі полегшені крипто примітиви та основні типів атак. Наведені матеріали в подальшому тексті дисертації не згадуються.

2. У першому розділі, зокрема, в пункті 1.2, крім аналізу підходів до синтезу симетричних та несиметричних СЕТ-операцій, доцільно було б детально і критично розглянути їх основні недоліки, виділивши ті з них, які дозволяє усунути дана робота.

3. Структури пристроїв реалізації сценаріїв потокового шифрування з використанням несиметричних двохоперандних СЕТ-операцій (рис. 2.1 і рис.2.2) доцільно було б доповнити структурами пристроїв реалізації розшифрування інформації. Подання процесу розшифрування інформації на рівні формального опису з введенням спеціальних визначень «комутативних»

і «некомутативних» СЕТ-операцій «подвійного і потрійного циклу» суттєво ускладнює сприйняття ідеї, на основі якої будувалося дисертаційне дослідження.

4. В підрозділі «5.3 Побудова інформаційної системи моделювання комутативних і некомутативних двооперандних сет-операцій для малоресурсних систем потокового шифрування» формальні моделі СЕТ-операцій (5.51) – (5.54) наведені посиланням на першоджерела без додаткових пояснень. Це суттєво ускладнює сприйняття алгоритмів функціонування інформаційної системи, які описано з формалізованою роботою блоків блок-схеми (рис.5.3 – рис.5.5).

5. Розділи 2-4 перенасичені викладками математичних перетворень, які знижують інформативність представленого матеріалу. Частину з цих можна було б винести в додатки.

Не зважаючи на вказані недоліки дисертаційна робота містить суттєві наукові результати, які є важливими для розвитку інформаційних систем і технологій, та заслуговує позитивної оцінки.

Вказані зауваження і недоліки не впливають на загальну позитивну оцінку виконаного дисертаційного дослідження та не зменшують її наукову новизну та практичну значущість і не знижують загального позитивного сприйняття проведеного обсягу досліджень.

10. Загальна оцінка роботи, її відповідність встановленим вимогам.

Дисертаційна робота Короткого Тимофія Костянтиновича на тему «Ієрархічна інформаційна система моделювання і дослідження алгоритмів потокового СЕТ-шифрування» є завершеною кваліфікаційною науковою роботою, яка містить нові науково обгрунтовані положення, які в сукупності вирішують актуальну науково-прикладну задачу підвищення продуктивності дослідження СЕТ-операцій при побудові перспективних стійких алгоритмів потокового шифрування на основі розширення можливостей ієрархічної інформаційної системи моделювання і дослідження СЕТ-операцій за рахунок встановлення нових і уточнення існуючих взаємозв'язків між моделями ієрархічних рівнів, які в сукупності забезпечать автоматизований синтез і аналіз симетричних та несиметричних однооперандних і багатооперандних СЕТ-операцій, а також генераторів їх псевдовипадкових послідовностей для потокового СЕТ-шифрування.

Вважаю, що за актуальністю, повнотою досліджень, науковою новизною, практичною цінністю одержаних результатів відповідає вимогам порядку присудження ступеня доктора філософії та скасування рішення разової спеціалізованої вченої ради закладу вищої освіти, наукової установи про присудження ступеня доктора філософії, затвердженого постановою Кабінету Міністрів України від 12.01.2022 р. № 44, та вимогам до оформлення дисертації, затвердженим наказом МОНУ від 12.01.2017 р. № 40, а її автор, Короткий Тимофій Костянтинович, заслуговує на присудження ступеня доктора філософії за спеціальністю 126 – Інформаційні системи та технології.

Офіційний опонент

декан факультету комп'ютерних
інформаційних технологій

Західноукраїнського національного університету,
доктор технічних наук, доцент

Ігор ЯКИМЕНКО

