

ВІДГУК

офіційного опонента

професора кафедри інформаційно-вимірювальних технологій,
Національного технічного університету України «Київський політехнічний
інститут імені Ігоря Сікорського»
доктора технічних наук, доцента Єременка Володимира Станіславовича
на дисертаційну роботу Короткого Тимофія Костянтиновича
“Ієрархічна інформаційна система моделювання і дослідження алгоритмів
потокowego СЕТ-шифрування”,
подану на здобуття ступеня доктора філософії
за спеціальністю 126 – “Інформаційні системи та технології” галузі знань 12 –
“Інформаційні технології” освітньо-наукової програми – “Інформаційні
системи та технології”

Актуальність теми дисертації

У сучасних умовах істотно зростає роль захищених інформаційних систем. Інформаційна безпека систем управління об'єктами критичної інфраструктури є одним з пріоритетних напрямків розвитку інформаційних технологій. Необхідно зазначити що задачі направлені на вдосконалення систем захисту інформації відносяться до наукоємних і їх вирішення потребує значних зусиль висококваліфікованих науковців. Для забезпечення ефективного використання науковців та підвищення продуктивності їх наукових досліджень доцільно застосовувати інформаційні системи і технології моделювання і дослідження процесів захисту інформації. Таким чином, тема дисертаційної роботи Короткого Тимофія Костянтиновича “Ієрархічна інформаційна система моделювання і дослідження алгоритмів потокowego СЕТ-шифрування” спрямована на вирішення важливої науково-практичної задачі підвищення продуктивності дослідження СЕТ-операцій при побудові перспективних стійких алгоритмів потокowego шифрування, є актуальною.

Зв'язок дисертації з науковими програмами, планами, темами

Результати дисертації пов'язані з науковими дослідженнями відповідно до Закону України «Про перспективні напрямки наукових досліджень» від 2006 року зі змінами від 2022 року. Отримані наукові результати включені в НДР Черкаського державного технологічного університету: «Дослідження шляхів розвитку потокowego шифрування на основі криптографічного кодування» (ДР № 0121U114389), і НДР «Інформаційна технологія психолінгвістичного аналізу тексту для стеганографічних систем» (ДР № 0123U102085).

Обґрунтованість наукових положень, висновків та рекомендацій

Наукові положення дисертації, сформульовані здобувачем є достатньо обґрунтованими. Це забезпечується логічною побудовою дослідження. Послідовним переходом від аналітики до удосконалення методів і технології. На основі яких будується чотирьохрівнева модель ієрархічної інформаційної системи моделювання і дослідження симетричних та несиметричних СЕТ-операцій. Висновки та рекомендації дисертації логічно витікають зі змісту проведеного дослідження, відповідають поставленій меті та задачам, а рекомендації щодо практичного використання результатів є достатньо аргументованими з позиції спеціальності 126 – Інформаційні системи та технології.

Достовірність одержаних наукових результатів

Достовірність основних наукових результатів дисертаційної роботи підтверджується наведеною в розділах 2, 3, 4 і 5 системою формальних методик і перетворень, що не містить принципових помилок, а також рядом прикладів. Отримані результати використані при створенні програмного макету ієрархічної інформаційної системи моделювання і дослідження алгоритмів потокового СЕТ-шифрування.

Наукова новизна отриманих результатів. На мою думку, наукова новизна дисертаційної роботи має достатньо коректне і чітке формулювання. До основних наукових результатів роботи відносяться:

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 двохрозрядних двооперандних СЕТ-операцій 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 двохоперандних двохранрядних 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 змодельовувати всі двохранрядні двохоперандні операції, які допускають перестановку операндів.

Рівень наукової новизни, представлений у роботі є достатнім для дисертації рівня доктора філософії за спеціальністю 126 – Інформаційні технології.

Значення результатів роботи для практики

Практичне значення результатів дисертаційної роботи полягає у створенні програмного макету ієрархічної інформаційної системи моделювання і дослідження алгоритмів потокового СЕТ-шифрування. Дана інформаційна система забезпечує синтез і аналіз 576 двохоперандних 2Сі-квантових СЕТ-операцій які допускають перестановку операндів. Розширює можливості дослідження генераторів послідовностей криптоперетворень, які можна будувати з використанням до 10623 2Сі-квантових і до $65 \cdot 10^{35}$ 3Сі-квантових несиметричних двохоперандних СЕТ-операцій.

Практична цінність роботи підтверджена актами впровадження, в навчальний процес Черкаського державного технологічного університету

Оцінка структури та змісту дисертації

Дисертаційна робота Короткого Т.К. складається зі вступу, п'яти розділів, висновків, списку використаних джерел і трьох додатків. Повний обсяг дисертації – 190 сторінок, з яких 158 сторінок основного тексту.

У *першому розділі* виконано аналіз сучасного стану та перспектив розвитку інформаційних систем і технологій проектування малоресурсних криптографічних систем. Акцентується увага на необхідність вдосконалення систем потокового СЕТ-шифрування.

Другий розділ присвячений удосконаленню технології побудови моделей некомутативних двохранрядних двохоперандних СЕТ-операції. Даний результат забезпечив зменшення складності процесів моделювання

некомутативних СЕТ-операцій за рахунок прямого переходу від побудованої моделі СЕТ-операції до моделі СЕТ-операції з переставленими операндами.

У *третьому розділі* удосконалено метод синтезу двохоперандних двохранрядних СЕТ-операцій, що забезпечило можливість додаткового синтезу несиметричних двохоперандних двохранрядних операцій подвійного циклу.

Четвертий розділ присвячено удосконаленню методу побудови двохранрядних двохоперандних операцій які допускають перестановку операндів на основі об'єднання двохранрядних однооперандних операцій криптографічного перетворення. Даний метод дозволяє синтезувати двохоперандні СЕТ-операції які допускають перестановку операндів для будь якої розрядності операндів.

П'ятий розділ присвячено дослідженню моделей генераторів псевдовипадкових послідовностей СЕТ-операцій, як основної складової системи моделювання потокових СЕТ-шифрів. Будується модель ієрархічної інформаційної системи моделювання і дослідження симетричних і несиметричних СЕТ-операцій. Наводяться особливості її реалізації.

Відповідність технічного та стильового оформлення встановленим вимогам

Дисертаційна робота відповідає вимогам наукового стилю та загальноприйнятим нормам української мови. Текст роботи написано зрозуміло, з коректним використанням технічної і наукової термінології. Робота оформлена з дотриманням до дисертаційних робіт затверджених наказом Міністерства освіти і науки України від 12.01.2017 р. № 40.

Повнота оприлюднення результатів роботи в публікаціях та ступінь апробації

Основні результати дисертації Короткого Т.К. достатньо повно викладені у 16 друкованих працях, зокрема: у 7 статтях у фахових виданнях України із яких 2 статті в фахових журналах категорії А, 3 статтях опублікованих за кордоном, із яких 1 стаття включена до науково-метричної бази SCOPUS (1 квартал), одноосібному розділі колективної монографії, і в матеріалах двох міжнародних науково-технічних конференцій.

Зауваження та дискусійні питання

1. На мою думку аналітичний огляд систем легкої криптографії необхідно було деталізувати і розширити, визначивши місце і значення малоресурсного постквантового СЕТ-шифрування.

2. Направленість наукового дослідження на автоматизацію побудови СЕТ-операцій які допускають перестановку операндів в структурі ієрархічної системи моделювання потокових криптоалгоритмів не виокремлена, що зменшую практичну цінність отриманих результатів. Адже перестановка

операндів забезпечує зміну алгоритму криптоперетворення, що приводить до збільшення криптостійкості шифрів випадкової підстановки.

3. В різних наукових публікаціях існують різні трактування комутативних і некомутативних перетворень, а також симетричних і несиметричних криптосистем та криптоалгоритмів. Автору було б доцільно навести дані визначення, а не обмежитися формальними взаємозв'язками між операціями і перетвореннями (ст..58, 59).

4. На мою думку, було б доцільно звернути увагу та дослідити і узагальнити властивості СЕТ-операцій подвійного і потрійного циклу. Група СЕТ-операцій з точністю до перестановки є групою СЕТ-операцій подвійного циклу (табл. 2.1), а для СЕТ-операцій потрійного циклу (табл.3.2), вона не є математичною групою, а лише підгрупою.

5. Розділи 3 і 4 перевантажені математичними перетвореннями СЕТ-операцій, які доцільно було б частково винести в додатки. Адже теоретичні і практичні висновки робляться на основі наведених узагальнених таблиць моделей СЕТ-операцій.

6. В процесі опису ієрархічної інформаційної системи автор представляє базу даних як базу моделей на заданому рівні ієрархії, а базу знань, як правила поєднання (перетворення) моделей в моделі вищого рівня. В процесі вирішення задачі моделювання на основі моделей операцій будуються таблиці підстановок, набори яких і будуть даними для побудови псевдовипадкових послідовностей на основі заданих алгоритмів (знань). Тому на мою думку використання термінів база даних і база знань не зовсім коректне.

7. В роботі присутні орфографічні і стилістичні помилки та неточності.

Дані зауваження не впливають на загальну оцінку роботи як позитивного внеску в розвиток науки. Вони можуть розглядатися як план подальших досліджень в теорії і практиці побудови легких криптографічних систем.

Висновок щодо відповідності дисертації вимогам, які висуваються до наукового ступеня доктора філософії

Оцінюючи роботу в цілому, вважаю, що в дисертації отримано нове рішення важливої науково-технічної задачі, спрямованої на 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 дисертаційна робота Короткого Тимофія Костянтиновича “Ієрархічна інформаційна система моделювання і дослідження алгоритмів потокового СЕТ-шифрування” відповідає вимогам Порядку присудження ступеня доктора філософії, затвердженого постановою Кабінету Міністрів України від 12.01.2022 р. № 44, а також Вимогам до оформлення дисертації, затвердженим наказом МОНУ від 12.01.2017 р. № 40, а здобувач заслуговує присудження ступеня доктора філософії за спеціальністю 126 – Інформаційні системи та технології.

Опонент:

професор кафедри інформаційно-
вимірювальних технологій

Національного технічного університету

України «Київський політехнічний
інститут імені Ігоря Сікорського»

доктор технічних наук, доцент

Володимир ЄРЕМЕНКО

