Голові спеціалізованої вченої ради К 73.052.04
Черкаського державного технологічного університету

18006, м. Черкаси, бульвар Шевченка, 460

ВІДГУК

на автореферат дисертації Козловської Світлани Григорівни
на тему «Методи синтезу груп симетричних операцій для потокового шифрування», яка представлена на здобуття наукового ступеня кандидата технічних наук за спеціальністю 05.13.05 – комп'ютерні системи і компоненти

Актуальність теми. На сьогоднішній день один із найперспективніших напрямів розвитку комп'ютерної криптографії поєднує методи криптології та комп'ютерної інженерії і полягає в розширенні спектра операцій криптографічного перетворення, забезпечуючи на їх основі вдосконалення існуючих та побудову нових криптографічних алгоритмів. Особливої уваги заслуговують при цьому дослідження, що спрямовані на розробку спеціалізованих операцій криптографічного перетворення на основі булевих функцій. Основною областю застосування таких операцій, як відомо, є блокові шифри. Їх розвиток в свою чергу пов'язаний з вирішенням задач генерації високоякісних псевдовипадкових послідовностей та побудови нових логічних операцій потокового шифрування. Саме тому дисертаційна робота Козловської Світлани Григорівни, метою якої є підвищення якості систем потокового шифрування конфіденційної інформації за рахунок збільшення стійкості та варіативності перетворення на основі додаткового використання груп двохоперандних двохрозрядних операцій, синтезованих на основі додавання за модулем два та чотири, є надзвичайно актуальною.

Оцінка змісту автореферату. Виходячи з представлених матеріалів, автор здійснив логічну побудову дисертаційної роботи, як послідовну композицію:

теоретичної основи у вигляді розробленого методу побудови та дослідження двохоперандних операцій криптоперетворення, розроблених методів груп симетричних двохрозрядних двохоперандних операцій потокового шифрування та методу підвищення стійкості та надійності потокового шифрування

та практичної складової власних досліджень у вигляді моделей та варіантів функціональних схем спеціалізованих дискретних пристроїв, які реалізують криптографічне перетворення інформації на основі застосування синтезованих груп операцій потокового шифрування та забезпечують підвищення варіативності й стійкості до лінійного крипто аналізу.

Така структура представлення результатів досліджень в авторефераті демонструє наявність комплексного підходу до вирішення наукової задачі і сформульованих в її рамках наукових завдань. Представлені в авторефераті відомості, на наш погляд, повністю характеризують зміст дисертаційної роботи і дозволяють судити про новизну і практичну значущість результатів. Приведений список наукових робіт свідчить про достатню міру апробації результатів досліджень.

Характеристика новизни. Як можна судити із змісту автореферату, найбільш цінними науковими результатами, отриманими автором, є:

1) *вперше розроблений* **метод побудови та дослідження двохоперандних**

операцій криптоперетворення на основі відомих таблиць істинності, який на відміну від існуючих за рахунок впровадження нових перестановочних схем побудови таблиць істинності наборів двохоперандних операцій криптоперетворення забезпечує встановлення нових взаємозв'язків між операндами й результатами, а також дозволяє застосовувати одноопераднді операції у потоковому шифруванні;

2) *вперше розроблені* **методи синтезу груп симетричних двохрозрядних двохоперандних операцій потокового шифрування,** які на відміну від існуючих за рахунок застосування результатів реалізації методу побудови та дослідження двохоперандних операцій, а також табличного представлення класифікації групи одноопераднді двохрозрядних операцій криптографічного перетворення та встановлення нових раніше невідомих взаємозв'язків між одноопераднді та двохоперандними операціями, забезпечують синтез математичних груп симетричних двохоперандних операцій на основі додавання за модулем два та додавання за модулем чотири;

3) **метод синтезу підвищення стійкості та надійності потокового шифрування,** *що набув подальшого розвитку* за рахунок додаткового застосування синтезованих груп симетричних двохоперандних операцій криптографічного перетворення інформації та забезпечив, як наслідок, підвищення стійкості та варіативності потокового шифрування.

Зауваження:

- зі змісту автореферату не зрозуміло, як саме перевірено коректність отриманих результатів побудованих узагальнених перестановочних схеми та перестановочних схем побудови таблиць істинності (ст.11, 12);
- в тексті автореферату наявні окремі граматичні та стилістичні помилки.

Зазначені недоліки суттєво не впливають на загальне позитивне враження від роботи, не зменшують її якості, а також наукової та практичної цінності. Вони не є визначальними і можуть бути враховані як деякі напрямки подальших досліджень.

Висновок. Судячи зі змісту автореферату дисертаційна робота С.Г.Козловської «Методи синтезу груп симетричних операцій для потокового шифрування» виконана на високому науково-технічному рівні та відповідає вимогам п.п. 9 і 11 постанови Кабінету Міністрів України №567 від 24.07.2013 р. про "Порядок присудження наукових ступенів" (із змінами), а здобувач – Козловська Світлана Григорівна, заслуговує на присудження наукового ступеня кандидата технічних наук за спеціальністю 05.13.05 – комп'ютерні системи і компоненти.

Завідувач кафедри інформаційної та кібернетичної безпеки Київського університету імені Бориса Грінченка
доктор технічних наук, професор В. Л. Бурячок

КИЇВСЬКИЙ УНІВЕРСИТЕТ ІМЕНІ БОРИСА ГРІНЧЕНКА
Ідентифікаційний код 02136554
ВЛАСНОРУЧНИЙ ПІДПИС
Бурячка В.Л. ЗАСВІДЧУЮ
(ПІБ)
фахівець ВК комбатокіб
24.06.2019