Голові спеціалізованої вченої ради К 73.052.04
Черкаського державного технологічного університету

18006, м. Черкаси, бульвар Шевченка, 460

ВІДГУК

на автореферат дисертації Нестеренко Оксани Борисівни
на тему «Методи та засоби синтезу операцій потокового шифрування за критерієм строгого стійкого кодування», яка представлена на здобуття наукового ступеня кандидата технічних наук за спеціальністю 05.13.05 – комп'ютерні системи і компоненти

Актуальність теми. Один із найперспективніших напрямів розвитку комп'ютерної криптографії полягає в поєднанні досягнень комп'ютерної інженерії та криптології. Це забезпечує, як відомо, розширення спектру операцій криптографічного перетворення та побудову на їх основі нових криптографічних алгоритмів. Особливої уваги заслуговують при цьому дослідження, що спрямовані на розробку спеціалізованих операцій для потокового шифрування на основі булевих функцій із заданими характеристиками. Не зважаючи на значні досягнення в даній галузі як вітчизняних, так і зарубіжних вчених багато відповідних задач залишається на даний час невирішеними. В першу чергу це стосується задач, спрямованих на підвищення невизначеності результатів шифрування, особливо в криптосистемах, алгоритми яких використовують псевдовипадкові послідовності. Саме тому дисертаційна робота Нестеренко Оксани Борисівни, метою якої є підвищення невизначеності результатів потокового шифрування за рахунок використання нових операцій криптоперетворення, синтезованих за критерієм строгого стійкого кодування 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 синтезу операцій за критерієм строгого стійкого кодування, методу синтезу операцій за критерієм строгого стійкого кодування мінімальної складності на основі використання операцій перестановки і гамування та методів синтезу програмних і апаратних криптографічних засобів комп'ютерної техніки на основі використання нової групи операцій, побудованих за критерієм строгого стійкого кодування

та практичної складової власних досліджень у вигляді апаратно-програмного комплексу, який реалізує операції потокового шифрування та гарантовано забезпечує зміну кожного біта інформації з імовірністю одна друга.

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 синтезу операцій за критерієм**

строгого стійкого кодування, який на відміну від існуючих для реалізації таких операцій та побудови таблиць істинності дискретних моделей використовує таблиці мінімальних відстаней Хеммінга й забезпечує максимальну невизначеність результатів перетворення та збільшення варіативності криптоалгоритмів;

2) *вперше розроблений* **метод синтезу операцій за критерієм строгого стійкого кодування мінімальної складності на основі використання операцій перестановки і гамування,** який на відміну від існуючих за рахунок встановлення обмежень та залежностей між операціями перетворення і таблицями мінімальних відстаней за Хеммінгом, забезпечує максимальну невизначеність результатів перетворення при практично мінімальній складності схемотехнічної та програмної реалізації;

3) **методи синтезу програмних і апаратних криптографічних засобів комп'ютерної техніки,** *що набули подальшого розвитку* за рахунок використання операцій, побудованих за критерієм строгого стійкого кодування та застосування методів синтезу моделей операцій з новими властивостями які, як наслідок, забезпечили спрощення процесу синтезу програмних і апаратних криптографічних засобів і дозволили реалізувати синтез аналогічних засобів мінімальної складності без побудови таблиць істинності та мінімізації.

Зауваження.

- зі змісту автореферату не зрозуміло, як саме перевірено коректність результатів обчислювального експерименту в результаті якого було отримано 42 чотирьохрозрядні операції, які відповідають критерію строгого стійкого кодування (ст.10);
- 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 О.Б.Нестеренко «Методи та засоби синтезу операцій потокового шифрування за критерієм строгого стійкого кодування» 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 – Нестеренко Оксана Борисівна, 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
вчений секретар
24.06.2019