Голові спеціалізованої
вченої ради Д 64.051.29
61022, м. Харків, майдан Свободи, 4

ВІДГУК

на автореферат дисертації Полуяненко Миколи Олександровича на тему «Моделі та методи синтезу регістрів зсуву з нелінійними зворотними зв'язками для схем потокового симетричного шифрування», поданої на здобуття наукового ступеня кандидата технічних наук за спеціальністю 05.13.21 – системи захисту інформації

Актуальність теми. Одним із способів вирішення завдань захисту державних інформаційних ресурсів та інформації з обмеженим доступом є криптографічний захист. Базовим елементом систем потокового криптоперетворення є генератори псевдовипадкових послідовностей (ПВП), серед яких найбільш перспективними вважаються генератори ПВП, побудовані на основі регістрів з нелінійним зворотним зв'язком. Вони, як відомо, з одного боку забезпечують ефективність апаратної реалізації, а, з іншого, – дозволяють протистояти алгебраїчним атакам.

Проте постійне вдосконалення обчислювальних технологій та поява нових математичних методів криптоаналізу висувають нові вимоги до криптографічної безпеки систем генерації ПВП. При цьому особливо гостро постають два основних питання: обґрунтування критеріїв до структури генератора ПВП та синтезу самих генераторів, що відповідають обраним критеріям. Це, а також нездатність багатьох з нелінійних регістрів, що застосовуються в потокових шифрах, генерувати послідовність максимального періоду та їх невідповідність низці інших критеріїв криптографічної стійкості висуває вимоги щодо застосовування додаткових вузлів ускладнення, що не є можливим при адаптуванні алгоритмів у системах з обмеженим середовищем. На теперішний час відсутній добре розроблений алгоритм синтезу потокових шифрів на основі нелінійних регістрів зсуву, що значно уповільнює їх потенційний розвиток. Саме тому дисертаційна робота М.О. Полуяненка, що присвячена розробці та теоретичному обґрунтуванню методу синтезу регістрів зсуву з нелінійними зворотними зв'язками для їхнього застосування в схемах потокового симетричного шифрування 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 регістрів зсуву з нелінійними зворотними зв'язками (РЗНЗЗ) , які формують послідовність максимального періоду та удосконаленої моделі оцінки криптографічної стійкості схем потокового симетричного шифрування, яка полягає в розробці системи критеріїв і показників стійкості псевдовипадкової послідовності, що, в свою чергу, дозволило йому скоротити обчислювальну складність формування нелінійних регістрів зсуву та переборного пошуку регістрів із встановленими конструктивними характеристиками

та практичної складової власних досліджень у вигляді апаратно-програмного комплексу, який реалізує метод синтезу РЗНЗЗ, а також систему критеріїв та

показників стійкості псевдовипадкової послідовності, що сформовано регістрами зсуву з нелінійними зворотними зв'язками.

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 регістрів зсуву з нелінійними зворотними зв'язками**, що формують послідовність максимального періоду, який відрізняється від наявних методів переборного пошуку зменшеною обчислювальною складністю та дозволяє провести пошук нелінійних регістрів зсуву великих розмірів із встановленими конструктивними характеристиками;

2. **модель оцінки криптографічної стійкості схем потокового симетричного шифрування, яка набула подальшого розвитку** й полягає в розробці системи критеріїв і показників стійкості псевдовипадкової послідовності, що сформовано регістрами зсуву з нелінійними зворотними зв'язками.

Зауваження. Аналіз змісту автореферату дозволив виявити такі недоліки:

– відсутність пояснення терміну «квадратична складність суми послідовності», який згадується в авторефераті на стор.14 п.3, але не є загальноприйнятим;

– наявність окремих граматичних і стилістичних помилок.

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 М.О. Полуяненка «Моделі та методи синтезу регістрів зсуву з нелінійними зворотними зв'язками для схем потокового симетричного шифрування» відповідає вимогам щодо кандидатських дисертацій згідно відповідних пунктів «Порядку присудження наукових ступенів», затвердженого Постановою Кабінету Міністрів України від 24.07.2013 р. № 567 (із змінами), а здобувач – Полуяненко Микола Олександрович, заслуговує на присудження йому наукового ступеня кандидата технічних наук за спеціальністю 05.13.21 – системи захисту інформації.

Професор кафедри інформаційних технологій
і математичних дисциплін Факультету інформаційних
технологій та управління Київського університету імені
Бориса Грінченка
доктор технічних наук, професор В.Л. Бурячок

КИЇВСЬКИЙ УНІВЕРСИТЕТ ІМЕНІ БОРИСА ГРІНЧЕНКА
Ідентифікаційний код 02136554
УКРАЇНА

КИЇВСЬКИЙ УНІВЕРСИТЕТ
ІМЕНІ БОРИСА ГРІНЧЕНКА
Ідентифікаційний код 02136554
ВЛАСНОРУЧНИЙ ПІДПИС
Бурячка В.Л. ЗАСВІДЧУЮ
(ПІБ)
(посада)
(підпис)