ВІДГУК

на автореферат дисертаційної роботи

Сисоєнко Світлани Володимирівни

«Методи і моделі підвищення швидкості та стійкості матричного криптографічного перетворення інформації»,

поданої на здобуття наукового ступеня кандидата технічних наук за спеціальністю 05.13.05 – комп'ютерні системи та компоненти

Згідно поданого автореферату, дисертаційна робота присвячена вирішенню важливої науково-технічної задачі яка полягає в підвищенні швидкості та стійкості матричного криптографічного перетворення інформації шляхом впровадження ієрархічної структури групового перетворення та встановлення нових взаємозв'язків між прямими та оберненими операціями. Тема дисертаційної роботи є актуальною, оскільки сучасні методи обробки, передачі та шифрування інформації, в яких використовуються матричні криптоперетворення, сприяли появі загроз, пов'язаних з можливістю втрати, розкриття, модифікації даних, що належать кінцевим користувачам.

Судячи зі змісту автореферату, наукова новизна роботи полягає в наступному: вперше розроблено метод підвищення стійкості псевдовипадкових послідовностей, побудованих на основі застосування операцій матричного криптографічного перетворення, шляхом їх додавання за модулем, що забезпечило підвищення ймовірності вироджених результатів перетворення; удосконалено моделі побудови криптоперетворення на основі використання двохоперандних операцій шляхом впровадження ієрархічної структури групового перетворення та встановлення нових взаємозв'язків між прямими та оберненими операціями, що дозволяє підвищити стійкість результатів шифрування; вперше розроблено метод підвищення швидкості реалізації групового матричного криптографічного перетворення на основі запропонованої узагальненої математичної моделі групового матричного криптографічного перетворення шляхом зменшення складності побудови та реалізації оберненого перетворення, що забезпечило зменшення математичної складності та збільшення швидкості криптографічного перетворення.

Практичне значення дисертаційної роботи полягає у вдосконалені автором моделі та розробленні методів шифрування доведені здобувачем до структурних

і функціональних схем пристроїв, а також алгоритмів шифрування, які забезпечують підвищення стійкості та швидкості криптоперетворення.

До зауважень можна віднести наступне:

- в авторефераті не наведено пояснення яким чином забезпечується часткова реалізація додавання декількох псевдовипадкових послідовностей в методі підвищення швидкості групового матричного криптографічного перетворення;
- на мою думку підпис осі рис.3 «Складність обчислень» слід було б замінити на «Кількість операцій».

Дисертаційна робота на тему «Методи і моделі підвищення швидкості та стійкості матричного криптографічного перетворення інформації» є закінченим науковим дослідженням, має доведені наукову новизну та практичне значення. Дисертаційна робота відповідає вимогам порядку присудження наукових ступенів та паспорту спеціальності 05.13.05 – комп'ютерні системи та компоненти, а її автор, Сисоєнко Світлана Володимирівна, заслуговує присудження наукового ступеня кандидата технічних наук.

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 відділу кадрового