ВІДГУК ОФІЦІЙНОГО ОПОНЕНТА

на дисертацію Сторожука Артема Юрійовича
«Методи оцінювання та обґрунтування стійкості потокових шифрів відносно статистичних атак на основі алгебраїчно вироджених наближень булевих функцій»,
прийнятої до захисту на здобуття наукового ступеня кандидата технічних наук за спеціальністю 21.05.01 – інформаційна безпека держави

Актуальність. Проблема захисту інформації набуває великого значення у процесі розвитку суспільства. Одним із способів її вирішення є використання криптографічних методів захисту інформації. Важливою складовою забезпечення безпеки інформації в сучасних спеціальних інформаційно-телекомунікаційних системах є синхронні потокові шифри. Найважливішою вимогою до таких шифрів є умова їх практичної стійкості відносно усіх відомих методів криптоаналізу. Якщо дана вимога не буде виконуватись, то інші характеристики шифру втрачають своє значення. Разом з тим, отримання науково обґрунтованих оцінок стійкості потокових шифрів навіть відносно добре вивчених методів криптоаналізу є складною науковою проблемою. Фактично, висновок про стійкість будь-якого потокового шифру ґрунтується на неможливості провести на нього окремі атаки, відомі криптоаналітикам, а також на припущенні про те, що майбутні атаки не призведуть до помітних покращень відомих криптоаналітичних методів. Тому, робота Сторожука А.Ю., що пов'язана із розробкою нових та удосконаленням існуючих методів оцінювання і обґрунтування стійкості потокових шифрів відносно статистичних атак на основі алгебраїчно вироджених наближень булевих функцій є безумовно актуальною.

Зв'язок роботи з науковими програмами, планами та темами.

Дисертаційне дослідження проводилося відповідно до планів науково-дослідної роботи Інституту спеціального зв'язку та захисту інформації Національного технічного університету України «Київський політехнічний інститут імені Ігоря Сікорського» та в межах науково-дослідних робіт «Севрюга» (номер держреєстрації 01113U005813) та «Мокрель» (номер держреєстрації 0115U004118) на замовлення Служби зовнішньої розвідки України.

Оцінка змісту дисертації, її завершеності у цілому.

Робота складається із вступу, чотирьох розділів, висновків, списку використаних джерел та чотирьох додатків. Загальний обсяг дисертації – 267 сторінок, з них 146 сторінок основного тексту, які включають 29 рисунків і 19 таблиць.

У вступі розкрито стан наукової задачі та її значимість, обґрунтовано необхідність проведення дослідження та актуальність теми роботи, її зв'язок з науковими програмами, сформульовано мету і завдання дослідження, наукову новизну і практичне значення, зазначено особистий внесок здобувача. С відомості про апробацію отриманих результатів та про наявні публікації.

Перший розділ роботи присвячено аналізу сучасного стану і напрямами розвитку методів криптографічного захисту інформації з використанням синхронних потокових шифрів. У розділі детально показана роль та значення потокових шифрів у забезпеченні захисту інформації в сучасних інформаційно-телекомунікаційних системах, розглянуто особливості побудови та функціонування сучасних синхронних потокових шифрів, наведено основні відомі методи оцінювання та обґрунтування стійкості потокових шифрів відносно сучасних атак. У результаті доведена актуальність даної роботи та визначено основні напрями та задачі дисертаційного дослідження.

У **другому розділі** викладено дві статистичні атаки на синхронні потокові шифри, які узагальнюють низку раніше відомих атак, надаючи криптоаналітику більше можливостей для вибору як функцій-оракулів, так і їх наближень.

Перша атака спрямована на відновлення ключів генераторів гами з лінійним законом реініціалізації початкового стану і узагальнює деякі з відомих подібних атак (Daemen et al. (1993); Golić, Morgari (2003), Armknecht et al. (2004)).

Друга атака є узагальненням більш потужної атаки FKM (статистична атака Фішера-Хазаі-Майєра), а також кубічної атаки і базується на наближенні булевих функцій, що реалізуються алгоритмами шифрування в цілому, алгебраїчно виродженими функціями. Також, у розділі наведено приклад ефективного застосування узагальненої статистичної атаки до редукованої версії шифру Grain-128, при якій трудомісткість атаки в 2^{27} разів менша ніж трудомісткість раніше відомої атаки.

У **третьому розділі** викладено метод побудови списку всіх k-вимірних функцій степеня не вище d, що знаходяться на відносній відстані не більше $2^{-d}(1-\varepsilon)$, $\varepsilon \in (0,1)$ від булевої функції n змінних, $d \le k < n$. Зазначений метод суттєво покращує аналогічний раніше відомий алгоритм Гопалана, а саме, має меншу трудомісткість у порівнянні з останнім (у певних випадках в 1000 та більше разів). Зменшення трудомісткості досягається шляхом застосування більш точної оцінки кількості шуканих наближень вхідної функції, а також більш економної організації обчислень, яка базується на детальному аналізі структури цих наближень. Показано, що цей метод може бути застосований на практиці при аналізі кореляційних властивостей функцій ускладнення синхронних потокових шифрів при малих значеннях k і d, якщо кількість «відносно великих» за модулем коефіцієнтів Уолша-Адамара функції f не перевищує 20.

Іншим науковим результатом розділу є метод обґрунтування відсутності високоймовірних наближень булевих функцій, який базується на ймовірнісному алгоритмі обчислення значень нижніх меж відносної відстані між зрівноваженою булевою функцією та множиною всіх k-вимірних функцій від n змінних. На відміну від відомих алгоритмів розв'язання цієї задачі, складність запропонованого алгоритму залежить лінійно від n та поліноміально від величин, обернених до точності та імовірності помилки алгоритму. Показано, що при малих значеннях k запропонований метод може бути ефективно використаний на практиці для обґрунтування стійкості функцій ускладнення синхронних потокових шифрів відносно узагальненої статистичної атаки.

У **четвертому розділі** викладено метод пошуку алгебраїчно вироджених наближень булевих функцій, заданих за допомогою оракулів, який відрізняється за сутністю від відомих та базується на отриманих аналітичних умовах, яким задовольняють шукані наближення. Крім того, за певних умов запропонований метод надає можливість переконуватися у відсутності зазначених наближень, що дозволяє використовувати його для обґрунтування практичної стійкості синхронних потокових шифрів відносно узагальненої статистичної атаки.

Також, у розділі вирішено важливу прикладну задачу оцінювання практичної стійкості шифру SNOW-2.0, що є прототипом майбутнього національного стандарту потокового шифрування України, відносно узагальненої статистичної атаки.

У загальних **висновках** викладено найбільш важливі наукові та практичні результати, отримані у дисертаційній роботі, які дають розв'язок сформульованих задач дисертаційного дослідження.

Список літератури є інформативним, достатньо повно охоплює предметну галузь, відображає опрацювання здобувачем значної кількості іноземних джерел.

В цілому викладення отриманих наукових і практичних результатів є послідовним, логічним та обґрунтованим, експериментальна частина не суперечить теоретичній, а дисертаційне дослідження має завершений характер.

Вміст автореферату достатньо повно розкриває основні положення дисертації та відповідає вимогам до оформлення.

Повнота викладу в опублікованих працях.

Матеріали дисертаційної роботи достатньо повно опубліковані в шести статтях в журналах, що входять до переліку наукових фахових видань України (два з них включені до міжнародних наукометричних баз), а також у восьми матеріалах конференцій. Обсяг друкованих робіт та їх кількість відповідають вимогам щодо публікації основного змісту дисертації на здобуття наукового ступеня кандидата технічних наук. Проведено апробацію і обговорення результатів дослідження на восьми міжнародних наукових та науково-практичних конференціях.

Найбільш суттєві наукові результати дисертації:

1. Удосконалено низку статистичних атак на синхронні потокові шифри, шляхом їхнього узагальнення та уніфікації (зокрема, атаку FKM та кубічну атаку). Розроблені атаки базуються на алгебраїчно вироджених наближеннях булевих функцій. Отримані аналітичні оцінки трудомісткості запропонованих атак, свідчать про їх більш високу ефективність у порівнянні з раніше відомими.

2. Удосконалено раніше відомий алгоритм Н. Гопалана призначений для вирішення задачі побудови високоймовірних k-вимірних наближень булевих функцій. Запропонований метод розв'язання вказаної задачі має суттєво меншу трудомісткість у порівнянні з зазначеним алгоритмом. Зменшення трудомісткості досягається шляхом застосування більш точної оцінки кількості шуканих наближень вхідної функції та більш економної організації обчислень.

3. Розроблено метод обчислення значень нижніх меж відносної відстані між зрівноваженою булевою функцією та множиною всіх k-вимірних функцій від n змінних. Сутність методу полягає у статистичному оцінюванні відносної відстані за допомогою спеціально розробленого ймовірнісного алгоритму, складність якого залежить лінійно від n та поліноміально від величин, обернених до точності та ймовірності помилки алгоритму.

4. Розвинуто метод пошуку алгебраїчно вироджених наближень булевих функцій. Запропонований автором метод відрізняється за сутністю від відомих та базується на отриманих аналітичних умовах, яким задовольняють шукані наближення. Крім того, за певних умов запропонований метод дає можливість переконуватися у відсутності зазначених наближень, що дозволяє його використовувати для обґрунтування практичної стійкості синхронних потокових шифрів відносно відомих статистичних атак.

Ступінь обґрунтованості та достовірності наукових положень, висновків і рекомендацій, сформульованих у дисертації.

Високий ступінь достовірності та обґрунтованості наукових результатів роботи визначаються коректним використанням методів теорії булевих функцій, лінійної алгебри, теорії ймовірностей, методів математичної статистики, експериментальною перевіркою та підтвердженням теоретичних міркувань і тверджень. Достовірність та обґрунтованість підтверджені всебічною апробацією на багатьох наукових та науково-практичних конференціях, наявністю рецензованих спеціалістами публікацій у фахових виданнях, впровадженням розроблених методів у держбюджетних науково-дослідних роботах.

Практичне значення отриманих результатів та можливі шляхи їх використання.

Практичне значення дисертації полягає в наданні можливості проведення оцінки стійкості сучасних програмно-орієнтованих синхронних потокових шифрів за допомогою розроблених автором прикладних програм (вихідні коди програм наведено у додатках). Вказані програми доцільно використовувати при проведенні експертних досліджень алгоритмів потокового шифрування, що використовуються в засобах криптографічного захисту інформації.

Крім того, отримані у дисертаційній роботі результати дозволяють:

– розширити клас наближень булевих функцій, що можуть бути використані для побудови статистичних атак на синхронні потокові шифри;

– встановити науково обґрунтовані умови стійкості синхронних потокових шифрів відносно відомих та запропонованих статистичних атак;

– підвищити трудомісткість найкращого з відомих алгоритмів побудови високоймовірних k-вимірних наближень булевих функцій;

– обґрунтувати практичну стійкість шифру SNOW 2.0 відносно узагальненої статистичної атаки.

Практична цінність роботи підтверджена впровадженням її результатів у науково-дослідних роботах «Севрюга» (акт від 30.09.16 р.) та «Мокрель» (акт від 30.09.16 р.), а також в науково-технічних розробках ЗАО «Інститут інформаційних

технологій» (акт від 25.07.16 р.).

Дискусійні положення, недоліки, зауваження та побажання.

1. Другий розділ присвячений удосконаленню і дослідженню двох статистичних атак на синхронні потокові шифри. У розділі зазначається, що під ефективністю даних атак розуміється трудомісткість їх виконання та необхідний обсяг матеріалу для успішної реалізації атаки з заданою надійністю. Проте, при дослідженні другої статистичної атаки кількісно оцінюється тільки трудомісткість її виконання, а необхідний обсяг матеріалу не розраховується, що не дає у повній мірі оцінити ефективність даної атаки.

2. Також, у другому розділі роботи наводиться приклад практичного застосування узагальненої статистичної атаки на редуковану версію шифру Grain-128. На мою думку, було б доцільно дослідити можливість її застосування до більшого числа синхронних потокових шифрів (наприклад, до відомого шифру Trivium) та навести порівняльні оцінки ефективності даної атаки.

3. У третьому розділі запропоновано метод побудови списку всіх k-вимірних функцій степеня не вище d, що знаходяться на відносній відстані не більше $2^{-d}(1-\varepsilon)$, $\varepsilon \in (0,1)$ від булевої функції n змінних, $d \le k < n$. У табл. 3.1 роботи наведено порівняння ефективностей роботи даного методу із алгоритмом Гопалана для низки значень n, m_k (кількості "відносно великих" за модулем коефіцієнтів Уолша-Адамара функції f), ε, k і d, що показало суттєво меншу трудомісткість розробленого методу при малих k, d і $m_k \le 20$. Цікаво було б побачити, як би змінювалась трудомісткість даних методів при різних ε ($\varepsilon \ne 0{,}125$) та інших значень параметрів k ($k = \overline{4,10}$), d ($d = \overline{2,10}$), n ($n = \overline{10,30}$) і m_k ($m_k = \overline{5,30}$).

4. По тексту дисертації є незначні орфографічні помилки. Деякі рисунки та таблиці наводяться з недостатніми поясненнями, що ускладнює сприйняття відображених результатів.

Загальні висновки.

Представлена на рецензію дисертаційна робота Сторожука А.Ю. «Методи оцінювання та обґрунтування стійкості потокових шифрів відносно статистичних атак на основі алгебраїчно вироджених наближень булевих функцій» є завершеною, самостійно підготованою кваліфікаційною працею, в якій на підставі теоретичних та експериментальних досліджень надано нове вирішення важливої наукової задачі, щодо розробки методів побудови науково обґрунтованих оцінок стійкості потокових шифрів відносно статистичних атак, що базуються на алгебраїчно вироджених наближеннях булевих функцій.

Дисертаційна робота містить не захищені раніше наукові положення та нові результати, спрямовані на розвиток та вдосконалення криптографічних методів захисту. Сформульовані наукові положення, висновки та рекомендації є достовірними та обґрунтованими. Матеріал дисертації викладено логічно і послідовно, стиль викладання чіткий і зрозумілий. Висновки до розділів та до дисертації в цілому тісно пов'язані з їх змістом і відображають основну суть роботи. Зміст автореферату повністю відповідає тексту дисертації, а основні

наукові положення, які в них містяться, є ідентичними. Наукові положення та висновки досить повно відображені в фахових виданнях. Матеріали дисертації достатньою мірою апробовані на міжнародних конференціях.

Дисертаційна робота відповідає профілю спеціалізованої вченої ради Д 26.062.17 та паспорту спеціальності 21.05.01 – інформаційна безпека держави.

Таким чином, за своєю актуальністю, ступенем достовірності та обґрунтованості наукових положень, висновків, новизною, практичним значенням і повнотою викладу в опублікованих працях дисертаційна робота «Методи оцінювання та обґрунтування стійкості потокових шифрів відносно статистичних атак на основі алгебраїчно вироджених наближень булевих функцій» відповідає вимогам до кандидатських дисертацій, а її автор, Сторожук Артем Юрійович, заслуговує на присудження наукового ступеня кандидата технічних наук зі спеціальності 21.05.01 – інформаційна безпека держави.

ОФІЦІЙНИЙ ОПОНЕНТ
Кандидат технічних наук,
доцент кафедри
безпеки інформаційних технологій
Навчально-наукового інституту
інформаційно-діагностичних систем
Національного авіаційного університету **В.М. Кінзерявий**

Особистий підпис Кінзерявого В.М. засвідчую.
Вчений секретар
Національного авіаційного університету **Г.Г. Єнчева**