ВІДГУК
офіційного опонента

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

Актуальність теми дисертаційної роботи. Потокові шифри є критичним елементом систем криптографічного захисту інформації, до яких пред'являються вимоги щодо надвисокої швидкодії в умовах компактної реалізації. Сучасні тенденції розвитку інформаційно-телекомунікаційних систем передбачають застосування відкритих каналів звя'зку для побудови складних розподілених мереж, в тому числі для IoT та Fog Computing. Умови застосування пристроїв цих мереж передбачають жорсткі обмеження на енергосопоживання, і, як наслідок, обчислювальну складність перетворень, що можуть бути реалізовані. Водночас, безпечне функціонування таких пристроїв, що керують фізичними об'єктами, є надзвичайно критичним. Розробка нового покоління потокових шифрів і обґрунтування їхніх властивостей, насамперед криптографічної стійкості, є актуальною і необхідною задачею. Це додатково підкреслюється низкою міжнародних криптографічних конкурсів, де вирішувались задачі розробки перспективних потокових шифрів. Тема дисертації Сторожука А.Ю. присвячена аналізу властивостей і обґрунтуванню стійкості потокових шифрів, є актуальною як в теоретичному, так і прикладному аспекті, при обґрунтуванні властивостей перспективного національного стандарту України для потокового шифрування.

Ступінь обґрунтованості наукових положень, висновків та рекомендацій. Автором виконаний ґрунтовний аналіз наявних методів оцінювання та обґрунтування стійкості потокових шифрів на основі різних підходів. За результатами цього аналізу виділено переваги та недоліки відомих методів, обґрунтовано висновок про доцільність їх удосконалення та розроблення нових методів побудові статистичних атак, які узагальнюють раніше відомі атаки на основі алгебраїчно вироджених наближень булевих функцій, обґрунтування стійкості прототипу національного стандарту України щодо потокового шифрування відносно таких атак, а також розробка методів пошуку чи обґрунтування відсутності алгебраїчно вироджених наближень булевих функцій, що використовуються при побудові зазначених атак. Цей аналіз дозволив автору обґрунтовано сформулювати наукову-практичну задачу, мету роботи, виділити об'єкт та предмет дослідження.

Основні припущення, покладені в основу теоретичних досліджень, є коректними, а отримані результати не суперечать відомим результатам. Подальша перевірка теоретичних результатів продемонструвала високий ступінь їх адекватності в обраному класі задач. Застосувані методи досліджень дозволяють отримати цілком обґрунтовані оцінки ефективності розроблених автором оригінальних методів та моделей.

Достовірність отриманих результатів. Достовірність викладених в дисертації основних наукових положень, висновків і результатів, отриманих здобувачем, забезпечується коректними постановками розв'язуваних у роботі задач та подальшим їх теоретичним аналізом, висновки якого узгоджуються з одержаними практичними результатами.

Достовірність отриманих результатів підтверджується також узгодженістю теоретичних положень з даними, отриманими при обчислювальних експериментах, належною апробацією на міжнародних конференціях і семінарах, а також впровадженням результатів дисертаційної роботи.

Застосування всіх наукових положень і результатів роботи в реальних задачах ґрунтується на детальному аналізі суті кожного об'єкта дослідження, що забезпечує коректність висновків про практичну ефективність розроблених методів.

Наукова новизна результатів дисертації. Аналіз дисертаційної роботи дозволяє зробити висновок, що здобувачем у процесі досліджень отримані такі істотно нові наукові результати:

А) *вперше*:

1. запропоновано метод обчислення значень нижніх меж відносної відстані між зрівноваженою булевою функцією та множиною всіх k-вимірних функцій від n змінних; 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;

Б) *удосконалено*:

2. низку статистичних атак на синхронні потокові шифри, шляхом їхнього узагальнення та уніфікації, зокрема, атаку FKM та кубічну атаку; отримані аналітичні оцінки трудомісткості запропонованих атак свідчать про їх більш високу ефективність у порівнянні з аналогічними раніше відомими (на багато порядків);

3. відомий алгоритм, призначений для вирішення задачі побудови високоймовірних k-вимірних наближень булевих функцій; запропонований метод має суттєво меншу трудомісткість (у певних випадках в 1000 та більше разів);

В) *отримав подальший розвиток*:

4. метод пошуку алгебраїчно вироджених наближень булевих функцій, що базується на отриманих аналітичних умовах, та не має передумовою виконання будь-яких обмежень стосовно відстані, на якій треба відшукати наближення, і дозволяє знаходити наближення з більш широкого класу булевих функцій; за певних умов запропонований метод надає можливість переконуватися у відсутності зазначених наближень для обґрунтування практичної стійкості синхронних потокових шифрів відносно відомих статистичних атак.

Зв'язок з науковими програмами, планами, темами.

Дисертаційна робота виконана відповідно до планів науково-дослідної роботи Інституту спеціального зв'язку та захисту інформації Національного технічного університету України "Київський політехнічний інститут" та в рамках науково-дослідних робіт (НДР) "Севрюга" (№ держреєстрації 0113U005813) та "Мокрель" (№ держреєстрації 0115U004118) на замовлення Служби зовнішньої розвідки України.

Практичне значення результатів дисертаційної роботи.

Розроблені в дисертаційній роботі нові методи дозволили:

- розширити клас наближень булевих функцій, що можуть бути використані для побудови статистичних атак на синхронні потокові шифри;
- встановити обґрунтовані умови стійкості синхронних потокових шифрів відносно відомих та запропонованих статистичних атак;
- підвищити (у певних випадках – в 1000 та більше разів) трудомісткість найкращого з відомих алгоритмів побудови високоймовірних k-вимірних наближень булевих функцій;
- створити пакет прикладних програм для оцінювання та обґрунтування стійкості синхронних потокових шифрів відносно запропонованих статистичних атак;
- обґрунтувати практичну стійкість прототипу національного стандарту України щодо потокового шифрування відносно узагальненої статистичної атаки та вдосконалити обґрунтуваність експертних висновків про застосування в Україні перспективних алгоритмів потокового шифрування, призначених для захисту державних інформаційних ресурсів.

Наукові та практичні результати дисертаційної роботи реалізовані в Службі зовнішньої розвідки України (акти від 30.09.2016 р.), а також у науково-технічних розробках Приватного акціонерного товариства "Інститут інформаційних технологій" (акт від 25.07.2016 р.).

Повнота викладу основних результатів у наукових виданнях та апробація. Основні наукові результати дисертаційної роботи опубліковано в 14 наукових працях: з них 6 наукових статей у наукових фахових виданнях України (2 видання індексуються міжнародними наукометричними базами); 8 тез доповідей на наукових та науково-практичних конференціях.

Відповідність змісту автореферату основним положенням дисертації. Оформлення автореферату за своїм обсягом, структурою та змістом відповідає чинним вимогам. Зміст автореферату ідентичний змісту основних положень дисертації, автореферат адекватно відображає результати дисертації.

Відповідність дисертації встановленим вимогам. Рецензована дисертаційна робота є завершеним і цілісним дослідженням, матеріал її добре структуровано і характеризується логічним викладом, що узагальнює дослідження автора. Роботу написано коректною мовою з використанням сучасної науково-технічної термінології.

Оформлення дисертації відповідає вимогам п. 9, пп. 11-14 «Порядку присудження наукових ступенів». Стиль викладу матеріалів досліджень, наукових положень і рекомендацій забезпечує їх адекватне і належне сприйняття.

Зауваження по дисертаційній роботі.

1. Потоковий шифр SNOW 2.0 має байт-орієнтовану структуру, тому при обґрунтуванні його стійкості доцільно було б застосувати відповідний математичний апарат векторних булевих функцій. Крім SNOW 2.0, що є прототипом національного стандарту потокового шифрування, доцільно було б дослідити і наявну версію проекту потокового шифра.

2. Твердження про незалежність подій $\Omega_i^{(j)}(y)$ (стор. 46 дисертації) потребує більш розгорнутого доказу. Вимоги (2.3), (2.4) та (2.5) накладають відповідні обмеження на матриці, але небієктивність відображення φ ускладнює перевірку результатів. Теж саме стосується виразу параметру $N_{k,d}$ в доказі твердження 3.6 (стор. 83 дисертації).

3. У п. 2.1.2 дисертації (стор. 52 дисертації) описане проведення низки обчислювальних експериментів, зокрема із використанням випадкової матриці. Аналіз вихідного коду (додаток А дисертації, стор. 170) показав застосування стандартного класу Random() для генерації псевдовипадкових послідовностей. Документація компанії Microsoft для .NET Framework свідчить про реалізацію ГПВП на основі одного з алгоритмів Д.Кнута, який не є криптографічним. При проведенні обчислювальних експериментів в галузі досліджень дисертації доцільно використовувати криптографічний генератор псевдовипадкових послідовностей з національних або міжнародних стандартів.

4. В оглядовій частині дисертації наведена низка посилань на атаки типу “баланс час-дані-пам’ять” (trade-off) на шифр A5/1, але відсутнє посилання на атаку, яка реалізована Karsten Nohl; ця атака на основі шифртексту є практичною та із низкою параметрів дозволяє відновлювати ключ у реальному часі.

5. В дисертації і авторефераті наявні незначні стилистичні недоліки. Наприклад, множини матриць заданого розміру над скінченим полем мають різні позначення (стор. 43 і 112 дисертації). Крім того, присутні помилки друку (“Харьків”, рис. 1 автореферату; “гамии”, стор. 169, “программний”, стор.201, 228, 234 дисертації).

Вказані недоліки не впливають на високу оцінку виконаних досліджень.

Висновок по дисертаційній роботі. Дисертаційна робота Сторожука А.Ю. є завершеною науковою працею, в якій вирішено актуальну науково-практичну задачу підвищення ефективності використання національних інформаційних ресурсів за рахунок зменшення часу проведення експертних досліджень алгоритмів потокового шифрування, призначених для захисту інформації в спеціальних інформаційно-телекомунікаційних системах України. Виконані в дисертаційній роботі дослідження та отримані наукові результати відповідають паспорту спеціальності 21.05.01 – інформаційна безпека держави. Автореферат повністю відповідає змісту дисертації й описує суть одержаних результатів та висновків у дисертаційній роботі і оформлений згідно з чинними вимогами, що висуваються до кандидатських дисертацій.

Дисертація відповідає вимогам п. 9, 11, 12, 13, 14 «Порядку присудження наукових ступенів» (Постанова КМУ № 567, від 24 липня 2013 р.) щодо кандидатських дисертацій, а її автор Сторожук Артем Юрійович заслуговує на присудження йому наукового ступеня кандидата технічних наук за спеціальністю 21.05.01 – інформаційна безпека держави.

Офіційний опонент

Професор кафедри безпеки інформаційних технологій
Харківського національного університету радіоелектроніки,

доктор технічних наук, доцент Р.В. Олійников

Міністерство освіти і науки України Харківський національний університет радіоелектроніки № 02071197

Підпис Олійника
Засвідчую
Секретар
Учений
І.В. Магдалина