МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ

СТОРОЖУК Артем Юрійович

УДК 621.391:519.2:510.5

МЕТОДИ ОЦІНЮВАННЯ ТА ОБҐРУНТУВАННЯ СТІЙКОСТІ ПОТОКОВИХ ШИФРІВ ВІДНОСНО СТАТИСТИЧНИХ АТАК НА ОСНОВІ АЛГЕБРАЇЧНО ВИРОДЖЕНИХ НАБЛИЖЕНЬ БУЛЕВИХ ФУНКЦІЙ

21.05.01 – «Інформаційна безпека держави»

А в т о р е ф е р а т
дисертації на здобуття наукового ступеня
кандидата технічних наук

Київ – 2016

Дисертацією є рукопис.

Робота виконана в Інституті спеціального зв'язку та захисту інформації Національного технічного університету України «Київський політехнічний інститут імені Ігоря Сікорського», м. Київ.

Науковий керівник: кандидат технічних наук, доцент
Конюшок Сергій Миколайович,
Інститут спеціального зв'язку та захисту інформації
Національного технічного університету України
«Київський політехнічний інститут імені Ігоря Сікорського»,
заступник начальника інституту з навчальної та наукової роботи.

Офіційні опоненти: доктор технічних наук, доцент
Олійников Роман Васильович,
Харківський національний університет радіоелектроніки,
професор кафедри безпеки інформаційних систем і технологій;

кандидат технічних наук
Кінзерявий Василь Миколайович,
Національний авіаційний університет,
доцент кафедри безпеки інформаційних технологій.

Захист відбудеться 16 березня 2017 р. о $13^{\underline{00}}$ годині на засіданні спеціалізованої вченої ради Д 26.062.17 при Національному авіаційному університеті за адресою: 03680, м. Київ, просп. Космонавта Комарова, 1 (аудиторія 11-111).

З дисертацією можна ознайомитись у бібліотеці Національного авіаційного університету за адресою: 03680, м. Київ, просп. Космонавта Комарова, 1.

Автореферат розісланий 14 лютого 2017 р.

Учений секретар спеціалізованої
вченої ради Д 26.062.17
к.т.н., доцент С.О. Гнатюк

ЗАГАЛЬНА ХАРАКТЕРИСТИКА РОБОТИ

Актуальність теми. Найважливішою задачею забезпечення інформаційної безпеки держави є створення та підтримання умов, які гарантують безпечну обробку, зберігання та передачу державних інформаційних ресурсів. Для її вирішення разом з технічними та організаційними застосовують криптографічні методи, які базуються на спеціальних математичних перетвореннях інформації, що захищається. На сьогодні без криптографічних методів та засобів неможливо вирішення таких задач інформаційної безпеки як забезпечення конфіденційності, цілісності, автентичності, невідстежуваності (анонімності), неможливості відмови від авторства та ін. Тому рівень розвитку криптографічних методів, які використовуються для захисту державних інформаційних ресурсів, суттєво впливає на інформаційну безпеку держави в цілому, її економічну незалежність та суверенітет.

Важливою складовою забезпечення безпеки інформації в сучасних спеціальних інформаційно-телекомунікаційних системах (СІТС) є синхронні потокові шифри (СПШ). Це обумовлено надвисокою швидкістю потокового шифрування (зокрема, програмні реалізації слово-орієнтованих потокових шифрів є в 5 – 10 разів швидше у порівнянні з відповідними реалізаціями блокових шифрів). На сьогодні лише потоковий шифр може забезпечити прийнятну швидкість шифрування на канальному, мережевому та транспортному рівнях. Програмно-орієнтовані потокові шифри знаходять застосування у вбудованих додатках систем з обмеженою кількістю обчислювальних ресурсів, зокрема у бездротовій телефонії (шифр SOBER) та в системах платного телебачення (шифр Panama). Окремо варто відзначити алгоритм потокового шифрування A5/1, який є невід'ємною частиною стандарту мобільного зв'язку GSM.

Значний інтерес до потокових шифрів спостерігається у європейському науковому криптографічному співтоваристві. Про це свідчить проведення міжнародних конкурсів NESSIE (2000 – 2003 рр.) та eSTREAM (2004 –2008 рр.), спрямованих на створення стійких потокових шифрів, придатних до широкого застосування. Через відсутність на сьогодні національного стандарту потокового шифрування в Україні вирішення цієї задачі є дуже актуальним і для нашої держави.

Найважливішою вимогою до потокових шифрів є умова їх практичної стійкості відносно всіх відомих криптоаналітичних атак. Якщо ця вимога не виконується, то інші характеристики шифру втрачають своє значення. Разом з тим, отримання науково обґрунтованих оцінок стійкості потокових шифрів (навіть відносно конкретних, 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. У зв'язку з цим особливої гостроти набуває проблема обґрунтування стійкості потокових шифрів, призначених для захисту інформації в СІТС України.

Аналіз доступних наукових публікацій показує, що найбільш потужними та широко розповсюдженими на практиці є атаки на синхронні потокові шифри на основі підібраних векторів ініціалізації (BI). До них належать зокрема кубічна атака, атака Фішера-Хазаі-Маєра (FKM), а також їх різноманітні модифікації та вдосконалення. Як показує детальний аналіз цих атак, всі вони будуються на основі наближень булевих функцій, пов'язаних з алгоритмами шифрування, функціями менш складної структури. Обґрунтування практичної стійкості потокового шифру відносно будь-якої з цих атак зводиться до встановлення факту відсутності зазначених наближень.

Не дивлячись на помітний прогрес у розробці конкретних атак, слід констатувати, що низка важливих окремих наукових задач залишається невирішеною. По-перше, це відносна вузькість класів функцій-наближень, які використовуються (афінні; функції від малого числа змінних). По-друге, це відсутність (за виключенням окремих спеціальних випадків) ефективних алгоритмів пошуку наближень булевих функцій із зазначених класів. І нарешті, це відсутність методів, які б дозволяли за достатньо загальних умов обґрунтовувати стійкість синхронних потокових шифрів відносно вищезазначених атак.

Наведені факти свідчать про певне протиріччя між потребами в обґрунтовано стійких та практичних алгоритмах потокового шифрування, що необхідні для забезпечення безпеки державних інформаційних ресурсів, з одного боку, та відсутністю методів обґрунтування стійкості цих алгоритмів відносно широкого кола сучасних атак, з іншого. Зазначене протиріччя породжує *наукову задачу*, *яка полягає в розробці методів побудови науково обґрунтованих оцінок стійкості потокових шифрів відносно статистичних атак, що базуються на алгебраїчно вироджених наближеннях булевих функцій,* розв'язанню якої присвячено дану дисертаційну роботу.

Зв'язок роботи з науковими програмами, планами, темами. Робота над дисертацією проводилася 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.

Мета і завдання дослідження. *Метою дисертаційної роботи є* 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.

Для досягнення поставленої мети в дисертаційній роботі сформульовано та вирішено такі взаємопов'язані *окремі задачі досліджень*:

1. Проаналізувати сучасні методи оцінювання та обґрунтування стійкості синхронних потокових шифрів відносно відомих статистичних атак на основі підібраних векторів ініціалізації.
2. Розробити статистичну атаку на фільтрувальний генератор гами з лінійним законом реініціалізації початкового стану (ПС) та функцією ускладнення, що є близькою до алгебраїчно виродженої.
3. Розробити статистичну атаку на СПШ, яка узагальнює аналогічні раніше відомі атаки та має більшу ефективність у порівнянні з ними.
4. Розробити метод побудови списку усіх високоймовірних k-вимірних наближень булевих функцій, що використовуються у складі СПШ.
5. Розробити метод оцінювання відносної відстані між зрівноваженою булевою функцією, заданою за допомогою оракула, та множиною k-вимірних функцій.
6. Розробити метод пошуку алгебраїчно вироджених наближень булевих функцій для оцінювання стійкості СПШ відносно узагальненої статистичної атаки.
7. Створити пакет прикладних програм для оцінювання та обґрунтування стійкості синхронних потокових шифрів відносно запропонованих статистичних атак.
8. Оцінити практичну стійкість шифру SNOW 2.0 відносно узагальненої статистичної атаки.

Об'єктом дослідження в дисертаційній роботі є криптографічні перетворення, що реалізуються синхронними потоковими шифрами, призначеними для захисту інформації в інформаційно-телекомунікаційних системах України.

Предметом дослідження є методи оцінювання та обґрунтування стійкості синхронних потокових шифрів відносно статистичних атак на основі алгебраїчно вироджених наближень булевих функцій.

Методи дослідження. Основу дисертаційних досліджень складають теоретичні дослідження (математичні методи оцінювання та обґрунтування стійкості синхронних потокових шифрів). Для розв'язання окремих задач 2 – 6 застосовувалися методи теорії булевих функцій, гармонічного аналізу, лінійної алгебри і теорії ймовірностей; для розв'язання окремих задач 4, 5, 8 використовувалися також методи математичної статистики. Чисельні розрахунки на ПК виконувалися з використанням платформи .NET Framework 4.0,

а також пакету прикладних програм Maple 15. Обробка статистичних даних у процесі дослідження проводилася відповідно до положень математичної статистики.

Наукова новизна одержаних результатів. Підсумком розв'язання перелічених вище наукових задач є такі нові наукові результати, що виносяться на захист:

1. Вдосконалено 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 аналогічними, раніше відомими. Зокрема, застосування однієї з цих атак до редукованої версії шифру Grain-128 дозволяє зменшити обчислювальну складність відновлення ключа шифру майже в 2^{27} разів у порівнянні з атакою FKM.

2. Вдосконалено раніше відомий алгоритм П. 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, 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.

3. Вперше запропоновано 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. 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.

4. Отримав подальший розвиток метод пошуку алгебраїчно вироджених наближень булевих функцій. Запропонований метод відрізняється за сутністю від відомих та базується на отриманих аналітичних умовах, яким задовольняють шукані наближення. На відміну від раніше відомих, запропонований метод не має передумовою виконання будь-яких обмежень стосовно відстані, на якій треба відшукати наближення, а також дозволяє знаходити наближення з більш широкого класу булевих функцій. Крім того, за певних умов запропонований метод надає можливість переконуватися у відсутності зазначених наближень, що до-

зволяє використовувати його для обґрунтування практичної стійкості СПШ відносно відомих статистичних атак.

Практичне значення одержаних результатів. Загальне практичне значення дисертації полягає в наданні можливості проведення оцінювання стійкості сучасних програмно-орієнтованих синхронних потокових шифрів за допомогою спеціально розроблених прикладних програм (додатки А, Б, В, Д). Вказані програми доцільно використовувати при проведенні експертних досліджень алгоритмів потокового шифрування, що використовуються в засобах криптографічного захисту інформації, яка відноситься до державних інформаційних ресурсів.

Крім того, наведені в 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 (у певних випадках в 1000 та більше разів) трудомісткість найкращого з відомих алгоритмів побудови високоймовірних k -вимірних наближень булевих функцій;

– обґрунтувати практичну стійкість шифру SNOW 2.0, що є прототипом майбутнього національного стандарту потокового шифрування, відносно узагальненої статистичної атаки;

– підвищити обґрунтованість експертних висновків про застосування в Україні перспективних алгоритмів потокового шифрування, призначених для захисту державних інформаційних ресурсів.

Наукові та практичні результати дисертаційної роботи реалізовано: в Службі зовнішньої розвідки України – в результаті виконання НДР “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.).

Особистий внесок здобувача. У статті [1] і тезах доповідей [7-10, 12] автором запропоновано та реалізовано статистичну атаку на фільтрувальний генератор гами з лінійним законом реініціалізації початкового стану; в статті [5] і тезах доповідей [11, 13] автором запропоновано узагальнену статистичну атаку на синхронні потокові шифри; в статті [4] автором запропоновано та реалізовано швидкі алгоритми побудови списку k-вимірних наближень булевих функцій; в статті [2] – швидкий імовірнісний алгоритм оцінювання відстані між зрівноваженою булевою функцією та множиною k-вимірних функцій; в статті [6] і тезах доповіді [14] розроблено та реалізовано алгоритми пошуку k-вимірних наближень булевих функцій та обчислення статистичних оцінок відносної відстані між вхідною функцією та множиною k-вимірних функцій.

Апробація результатів дисертації. Результати дисертаційних досліджень доповідалися та обговорювалися *на 8 міжнародних наукових та нау-*

ково-практичних конференціях: Міжнародному конгресі з інформатики “Информационные системы и технологии “CSISIT’ 2013” (Білорусь, м. Мінськ, 2013 рік), XLI – XLII Міжнародних наукових конференціях “Питання оптимізації обчислень” (м. Кацивелі, 2013 р., смт. Чинадієво, 2015 р.), Міжнародній науковій конференції “Probability, reliability and stochastic optimization” (м. Київ, 2015 р.), XV – XVIII Міжнародних науково-практичних конференціях “Безпека інформації в інформаційно-телекомунікаційних системах” (м. Київ, 2012, 2013, 2015, 2016 рр.).

Публікації. 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.

Структура і обсяг роботи. Дисертація складається із вступу, чотирьох розділів, висновків, списку використаних джерел та чотирьох додатків. Повний обсяг роботи – 267 сторінок, з яких 121 сторінку займають додатки, рисунки, таблиці та список використаних джерел, що включає 163 найменування.

ОСНОВНИЙ ЗМІСТ РОБОТИ

У вступі подано загальну характеристику роботи згідно з чинними вимогами до дисертацій.

У першому розділі проаналізовано сучасний стан і напрями розвитку методів криптографічного захисту інформації з використанням синхронних потокових шифрів. Зазначено, що СПШ є на сьогодні важливою складовою забезпечення конфіденційності інформації у спеціальних інформаційно-телекомунікаційних системах, зокрема у бездротових сенсорних мережах, радіомережах, розподілених центрах обробки даних та ін. (рис. 1).

Широке використання потокових шифрів для захисту інформації в СІТС призводить до суттєвого підвищення вимог до їх стійкості (спроможності протистояти усім відомим криптоаналітичним атакам). На основі проведеного аналізу доступних наукових публікацій показано, що найбільш потужними атаками на СПШ є атаки на основі підібраних ВІ, до яких належать атака FKM, кубічна атака та їх різноманітні модифікації і вдосконалення.

Атака FKM будується на основі статистичного наближення булевої функції F, що визначається потоковим шифром, іншою функцією g, яка залежить лише від деяких розрядів ключа. Це дозволяє спочатку відновити зазначені розряди методом максимуму правдоподібності, а потім знайти решту ключа шляхом повного перебору. Авторами атаки зазначено способи вибору функцій F та g для низки конкретних СПШ, але не дано теоретичного обґрунтування ефективності цих способів у загальному випадку. Крім

того, залишається відкритим питання, чи можна підвищити ефективність цієї атаки, вибираючи наближення функції F з більш широкого класу булевих функцій. Зазначені факти свідчать про необхідність уніфікації та узагальнення низки відомих атак на СПШ на основі підібраних ВІ, визначення загальних умов їх застосовності та отримання аналітичних оцінок параметрів, що характеризують їх ефективність.

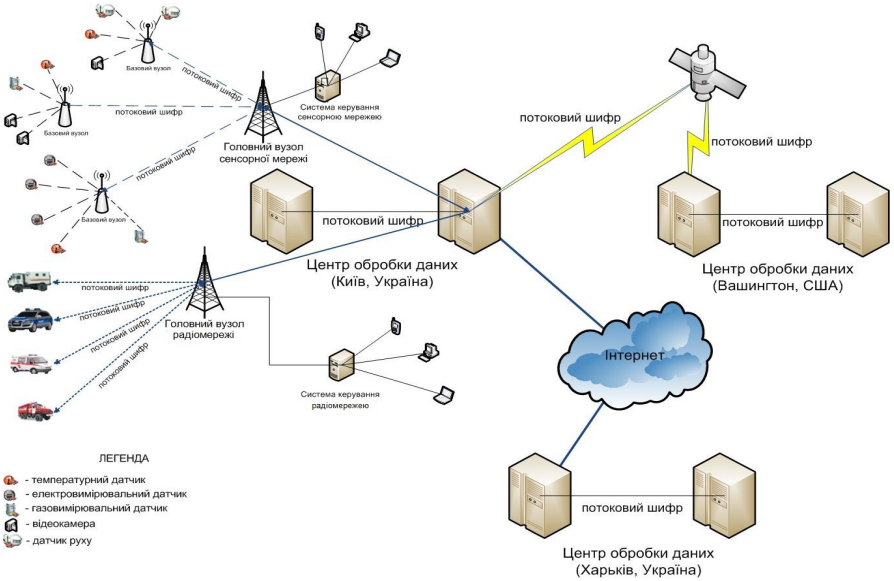

Рис. 1. Типова архітектура розподіленої СІТС

У другому розділі викладено дві статистичні атаки на СПШ. Перша з них є застосовною до генераторів гами з лінійним законом реініціалізації ПС та узагальнює деякі з відомих подібних атак (Daemen et al. (1993); Golić, Morgari (2003), Armknecht et al. (2004)). Друга запропонована атака узагальнює кубічну атаку та атаку FKM і, в принципі, може бути застосована до будь-якого СПШ, який описується за допомогою булевої функції $F : V_{l_0} \times V_{l_1} \to \{0,1\}$, один з аргументів якої є секретним, а інший – загальнодоступним параметром (тут і далі для будь-якого натурального m використовується позначення $V_m = \{0,1\}^m$). Саме ця атака описується далі.

Розглянемо СПШ, який складається з генератора гами та алгоритму формування його ПС за ключем та вектором ініціалізації. Генератор гами являє собою скінченний автономний автомат з множиною станів V_N, функцією

переходів $h: V_N \to V_N$ та функцією виходів $f: V_N \to \{0,1\}$, а алгоритм формування ПС задається відображенням $H: V_{l_0} \times V_{l_1} \to V_N$, де l_0 – довжина ключа, l_1 – довжина ВІ. Знак гами в i-му такті, який відповідає ключу $k \in V_{l_0}$ та ВІ $c \in V_{l_1}$, визначається за формулою $\gamma_i(k,c) = f(h^i(H(k,c)))$, де h^i є i-м степенем відображення h відносно операції композиції, $i = 0, 1, \ldots$.

Для проведення атаки противник вибирає функції-оракули $F: V_{l_0} \times V_{l_1} \to \{0,1\}$, $\varphi: V_{s+l_1} \to \{0,1\}$ та матрицю $M_0 \in \mathbf{F}_2^{l_0 \times s}$ рангу $s < l_0$, які задовольняють таким умовам:

а) існує ефективний алгоритм обчислення значень $F_k(c) = F(k,c)$, $c \in V_{l_1}$, яким би не був невідомий фіксований ключ $k \in V_{l_0}$;

б) справедлива нерівність $\mathbf{P}_{k,c}\{F(k,c) = \varphi(kM_0, c)\} \geq 1 - \vartheta$, де k та c є незалежними випадковими векторами, перший з яких розподілений рівномірно на множині V_{l_0}, а другий – відповідно до деякого (не обов'язково рівномірного) закону $\mathbf{P}_c$ на множині V_{l_1}, $\vartheta \in (0, 1/2)$.

Атака складається з двох етапів, на першому з яких за допомогою методу максимальної правдоподібності відновлюється вектор kM_0; на другому етапі, шляхом перебору знаходиться невідомий ключ $k \in V_{l_0}$.

Назвемо ключ k ε-*слабким* (*відносно описаної атаки*), $\varepsilon \in (0,1)$, якщо $\mathbf{P}_c\{F_k(c) = \varphi(kM_0, c)\} \geq 1/2(1+\varepsilon)$ та припустимо, що, поряд з умовами а), б) виконується наступна умова:

в) для будь-якого ε-слабкого ключа $k \in V_{l_0}$ та довільного вектора $y \in V_s \setminus \{kM_0\}$ справедлива нерівність $\mathbf{P}_c\{F_k(c) = \varphi(y,c)\} = 1/2$.

У розділі доведено низку тверджень, які узагальнюють та уточнюють окремі результати, відомі для атаки FKM. Зокрема, показано, що за умов а), б), в) при $\vartheta = 1/2 - 2^{-\mu}$, $\varepsilon = (2^{\mu} - 1)^{-1}$, де $\mu > 1$, та $r = \left\lceil 2^{2\mu+3} \ln(2^s \delta^{-1}) \right\rceil$, де $\delta \in (0,1)$, існує не менше ніж $2^{l_0 - \mu}$ ε-слабких ключів СПШ, кожен з яких може бути відновлений за допомогою запропонованої атаки зі складністю: $T(l_0, s, r) = O\left(2^s r(T_F + T_\varphi) + s(l_0 - s)2^{l_0 - s} T_{\mathcal{A}}\right)$ операцій, де $T_{\mathcal{A}}$ – часова складність алгоритму $\mathcal{A}$, T_F та T_φ – часові складності обчислення значень F та φ відповідно.

У табл. 1 наведено результати розрахунків трудомісткості атаки на реду-

ковану версію шифру Grain-128 ($l_0 = 128$, $l_1 = 96$, $T_F = 128$, $T_\varphi = T_F(l_0 + l_1)^2$, $T_{\mathcal{A}} = 3 \cdot 128$), де в ролі оракула F використовується функція F_{FKM} від $l_0 + l_1 = 224$ змінних, запропонована розробниками атаки FKM. Зауважимо, що трудомісткість останньої атаки складає 2^{124} операцій, що лише в 16 разів менше трудомісткості повного перебору ключів. У той же час, використовуючи (побудоване за допомогою розробленого дисертантом алгоритму) наближення функції F_{FKM} з більш широкого класу алгебраїчно вироджених функцій з параметрами $s = 52$, $\vartheta = 0{,}1702$, можна побудувати на цю версію шифру узагальнену статистичну атаку зі складністю 2^{97}, що в 2^{27} разів менше трудомісткості атаки FKM.

Таблиця 1

Оцінки трудомісткості узагальненої статистичної атаки

ϑ	s	$T(l_0, s, r)$
0,49	30	2^{119}
	50	2^{99}
	70	2^{108}
0,20	30	2^{119}
	50	2^{99}
	70	2^{98}
0,01	30	2^{119}
	50	2^{99}
	70	2^{97}

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).

Позначимо B_n множину булевих функцій від n змінних, $F_{n \times k}$ – множину матриць розміру $n \times k$ над полем $F = \mathbf{GF}(2)$. Функція $g \in B_n$ називається *k-вимірною*, якщо вона може бути представлена у вигляді $g(x) = \varphi(xA)$, $x \in V_n$, де $\varphi \in B_k$, $A \in F_{n \times k}$. Позначимо $B_{n,k}$ множину k-вимірних функцій

від n змінних, $\overline{B}_{n,k} = B_{n,k} \setminus B_{n,k-1}$. Потрібно розробити метод, який для заданих $f \in B_n$, $d, k \in \mathbf{N}$, де $d \le k < n$, будує множину

$$B_{n,k,d}(f;\varepsilon) = \{g \in B_{n,k} : d(f,g) \le 2^{-d}(1-\varepsilon), \deg g \le d\}. \qquad (1)$$

Сутність методу, що пропонується, полягає в ефективному переборі певних пар (φ, A), для яких функція $g(x) = \varphi(xA)$, $x \in V_n$ належить множині (1). При цьому використовується декілька наукових рішень, які є результатом дослідження будови множини (1) і дозволяють суттєво оптимізувати зазначений перебір.

По-перше, використовується розбиття множини (1) на такі підмножини: $\{g \in B_{n,d-1} : d(f,g) \le 2^{-d}(1-\varepsilon)\} \cup \overline{B}_{n,d,d}(f;\varepsilon) \cup \left(\bigcup_{i=d+1}^{k} \overline{B}_{n,i,d}(f;\varepsilon) \right)$. Це дозволяє застосувати для побудови кожної з підмножин окремий алгоритм, базуючись на особливих властивостях саме цієї підмножини. По-друге, з метою уникнення повторень при переборі використовується розбиття множини матриць у виразах шуканих наближень на класи еквівалентності з перебором тільки так званих незвідних представників класів. По-третє, встановлено, що стовпці матриць у виразах шуканих наближень достатньо вибирати лише з множини $S_f(\mu_{0,k}) = \{\alpha \in V_n : |\hat{f}(\alpha)| \ge \mu_{0,k}\}$, де $\hat{f}(\alpha) = 2^{-n} \sum_{x \in V_n} (-1)^{f(x) \oplus \alpha x}$, $\alpha \in V_n$, $\mu_{0,k} = \max\{2^{1-k}\varepsilon, \frac{4}{3\sqrt{3}} 2^{-k/2-d/2} \varepsilon^{3/2}\}$. Це дозволяє суттєво зменшити складність перебору.

Показано, що трудомісткість запропонованого методу складає не більше ніж $T^{(\varepsilon)}_{n.k.d}(m_k) = O\left(2^n(n^2+nd) + 2^{n+d} nd \binom{m_k}{d} + 2^n n \sum_{i=d+1}^{k} i \binom{m_k}{i} N_{i,d} \right)$ операцій, де $m_k = |S_f(\mu_{0,k})|$, $N_{i,d} = \sum_{l=0}^{i} (-1)^l \binom{i}{l} 2^{\sum_{j=0}^{d} \binom{i-l}{j}}$, $i \in \overline{d+1,k}$, в той час як трудомісткість алгоритму Гопалана є не менше ніж $\widetilde{T}^{(\varepsilon)}_{n.k.d} = 2^n (m_k)^k nk\, 2^{\sum_{i=0}^{d} \binom{k}{i}}$.

Результати чисельних розрахунків (табл. 2), а також практичного застосування запропонованого методу свідчать про те, що він є більш ефективним у порівнянні з алгоритмом Гопалана (в певних випадках в 1000 та більше разів) і може бути ефективно застосованим на практиці при малих значеннях k і d, якщо кількість m_k "відносно великих" за модулем коефіцієнтів Уолша-

Адамара функції f не перевищує 20. У випадку $d = k$ трудомісткість методу помітно зменшується, що робить можливим його застосування при більших значеннях k (наприклад, $k = 10$), в той час як алгоритм Гопалана стає практично незастосовним.

Таблиця 2

Результати порівняння ефективності запропонованого методу та алгоритму Гопалана ($\varepsilon = 0{,}125$)

Параметри					Трудомісткість запропонованого методу	Трудомісткість алгоритму Гопалана
n	k	d	$\log(\mu_{0,k})^{-2}$	m_k		
15	4	2	12,00	5	2^{35}	2^{42}
				20	2^{44}	2^{50}
		3	12,00	5	2^{39}	2^{46}
				20	2^{49}	2^{54}
		4	12,00	5	2^{28}	2^{47}
				20	2^{38}	2^{55}
	5	2	18,00	6	2^{40}	2^{51}
				20	2^{51}	2^{59}
		4	18,00	6	2^{55}	2^{66}
				20	2^{67}	2^{74}
		5	18,00	6	2^{29}	2^{67}
				20	2^{41}	2^{75}

Другим науковим результатом розділу є метод статистичного оцінювання відносної відстані між зрівноваженою булевою функцією $f \in B_n$ та множиною всіх k-вимірних функцій від n змінних. Цей метод запропоновано вперше та може бути застосовано для обґрунтування стійкості СПШ, коли потрібно не шукати алгебраїчно вироджені наближення, а навпаки, переконатися в їх відсутності.

Нехай зрівноважена функція f задана за допомогою оракула. Треба розробити метод обчислення значень нижніх меж відносної відстані $d(f, B_{n,k})$ з точністю ε та достовірністю $1-\delta$, де $\varepsilon, \delta \in (0,1)$. При цьому потрібно, щоб для будь-якого фіксованого k трудомісткість методу лінійно залежала від n та поліноміально від ε^{-1} та δ^{-1}.

Сутність методу полягає у звуженні функції f на підпростір, що визначається випадковою рівноймовірною булевою $t \times n$-матрицею X, та обчисленні відносної відстані $\Delta(f, B_{n,k})$ між функцією $f_X(u) = f(uX)$, $u \in V_t$ та множиною $B_{n,k}$. При цьому для обчислення останнього параметра достатньо перебирати лише так звані спеціальні ступеневі матриці, що суттєво зменшує складність обчислень (без втрати точності).

Доведено, що при $t = k + \lceil \log(\varepsilon^{-2}\delta^{-1}) \rceil$ виконується нерівність $\mathbf{P}_X\{d(f, B_{n,k}) \geq \Delta(f, B_{n,k})\} \geq 1 - \delta$. При цьому трудомісткість методу не перевищує $T_{n,k}(\varepsilon, \delta) = O\left(2^k (k + \varepsilon^{-2}\delta^{-1})(n\varepsilon^{-2}\delta^{-1} + k^2 \max\{2^{k^2}, \varepsilon^{-2k}\delta^{-k}\})\right)$ операцій.

У табл. 3 показано результати застосування запропонованого методу до функції ускладнення G СПШ Achterbahn-80. Обчислення проведені на ПК з процесором Intel Core i7 (1,6 ГГц) та обсягом оперативної пам'яті 4 Гб RAM (DDR3) на базі Windows 7 (використовувався пакет прикладних програм Maple 13.0). Середній час роботи комп'ютерної програми складає 652 с.

Таблиця 3

Статистичні нижні оцінки параметра $d(G, B_{n,2})$

($n = 11$, $\varepsilon = 1/8$, $\delta = 0{,}25$, $t = 10$)

Номер експерименту	$\theta(X)$	$\Delta(G, B_{n,2})$	Номер експерименту	$\theta(X)$	$\Delta(G, B_{n,2})$
1	0,2517	0,3316	6	0,2512	0,3119
2	0,1881	0,3434	7	0,2498	0,3126
3	0,1881	0,3434	8	0,1891	0,3429
4	0,1266	0,3742	9	0,1891	0,3429
5	0,1881	0,3434	10	0,2507	0,3121

Зауважимо, що точне значення відносної відстані $d(G, B_{n,2})$ дорівнює 0,4375, а час його обчислення складає 3020 секунд, що приблизно в 5 разів перевищує середній час оцінювання цього параметра з точністю $\varepsilon = 1/8$ та надійністю $1 - \delta \geq 0{,}75$. У цілому, отримані результати показують, що при малих значеннях k запропонований метод може бути ефективно використаний на практиці для обґрунтування стійкості функцій ускладнення СПШ відносно статистичних атак, наведених у другому розділі.

У четвертому розділі викладено метод пошуку алгебраїчно вироджених наближень булевих функцій, заданих за допомогою оракулів, який відрізня-

ється за сутністю від відомих та базується на отриманих аналітичних умовах, яким задовольняють шукані наближення. Крім того, вирішено важливу прикладну задачу оцінювання практичної стійкості шифру SNOW-2.0, що є прототипом майбутнього національного стандарту потокового шифрування України, відносно узагальненої статистичної атаки.

За означенням функція $g(k,c)=\varphi(kM_0,c)$, $k\in V_{l_0}$, $c\in V_{l_1}$, називається θ-*допустимим наближенням* функції $F=F(k,c)$, $k\in V_{l_0}$, $c\in V_{l_1}$, якщо $\varphi\in B_{s+l_1}$, $M_0\in \mathbf{F}_2^{l_0\times s}$, $\operatorname{rank}(M_0)=s$ і $d(F,g)\le 1/2\cdot(1-\theta)$. Запропонований метод пошуку (обґрунтування відсутності) θ-допустимих наближень функції F складається з двох етапів, на першому з яких здійснюється пошук певних підпросторів, що є допустимими для вхідної функції-оракула (при цьому відсутність зазначених підпросторів свідчить про відсутність відповідних наближень). На другому етапі за допомогою спеціально розробленого алгоритму за знайденим підпростором будується булева функція від меншої кількості змінних, яка (поряд з базисом знайденого підпростору) задає наближення вхідної функції.

Наукову основу методу складає наступне твердження.

Нехай функція $g(k,c)=\varphi(kM_0,c)$, $k\in V_{l_0}$, $c\in V_{l_1}$ є θ-допустимим наближенням функції F. Позначимо $\mathcal{D}(F,w(\theta,\mu))=\{\alpha\in H_0^{\perp}: wt(D_\alpha F)\le w(\theta,\mu)\}$, де $H_0=\{(0,c): c\in V_{l_1}\}$, $D_\alpha F(x)=F(x\oplus\alpha)\oplus F(x)$, $x\in V_n$, $w(\theta,\mu)=\min\{-\theta, 1/2\cdot(1-\theta^2)+\mu\}$, а μ є довільним числом з властивістю $\sum_{\beta\in V_n}\hat{F}(\beta)^4\le\mu^2<1$. Тоді існує множина $D\subseteq\mathcal{D}(F,w(\theta,\mu))$ потужності $|D|\ge 3/4\cdot 2^{l_0-s}$ така, що стовпці матриці $M=\begin{pmatrix} M_0 & 0\\ 0 & I_{l_1}\end{pmatrix}$ належать підпростору, дуальному до D.

Зазначене твердження встановлює аналітичні умови, яким задовольняють шукані наближення функції F, що дозволяє суттєво скоротити час їх пошуку в порівнянні з методом повного перебору. Зокрема, застосування розробленого методу до функції F_{FKM}, яка використовується для побудови узагальненої статистичної атаки на редуковану версію шифру Grain-128, дозволяє отримати θ-допустиме наближення цієї функції при $s=52$, $\theta=0{,}57$ за 53 години на стандартному комп'ютері (саме це наближення дозволяє побудувати атаку, складність якої в 2^{27} разів менше складності атаки FKM).

Застосування розробленого методу до низки функцій $F_{\mathrm{SNOW\text{-}2.0}}$ для побудови узагальненої статистичної атаки на шифр SNOW-2.0 (рис. 2) дає не-

гативний результат. При $s \le 20$, $\theta = 0{,}6$ з достовірністю не менше ніж 0,99 жодна з зазначених функцій не має наближень, які знаходяться від неї на відносній відстані не більше ніж $1/2 \cdot (1-\theta) = 0{,}2$ та мають вигляд $\varphi(kM_0, c)$, $(k, c) \in V_{128} \times V_{128}$, де $\varphi : V_{148} \to \{0, 1\}$, $M_0 \in \mathbf{F}_2^{128\times 20}$ (при цьому час виконання комп'ютерної програми складає приблизно 187 годин).

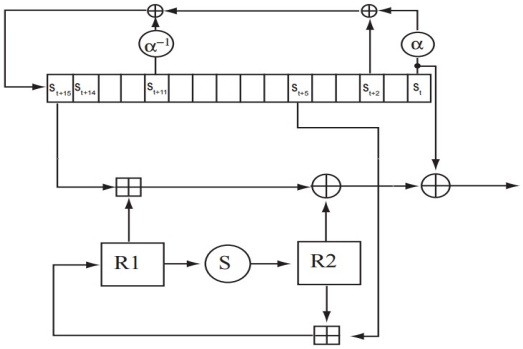

Рис. 2. Схема генератора гами шифру SNOW-2.0

Це свідчить про практичну стійкість шифру відносно узагальненої статистичної атаки.

У висновках викладено найбільш важливі наукові та практичні результати дисертаційного дослідження, сформульовано вирішену наукову задачу, розкрито методи її розв'язання, наукове та практичне значення роботи, обґрунтованість та достовірність отриманих результатів, подано висновки та рекомендації щодо їхнього подальшого використання.

ВИСНОВКИ

У дисертаційній роботі вирішено важливу й актуальну *наукову задачу* розробки методу побудови науково обґрунтованих оцінок стійкості потокових шифрів відносно статистичних атак, що базуються на алгебраїчно вироджених наближеннях булевих функцій.

1. Проведено детальний аналіз доступних наукових публікацій присвячених сучасним методам оцінювання та обґрунтування стійкості СПШ відносно відомих статистичних атак на основі підібраних векторів ініціалізації. Всі вказані атаки базуються на наближеннях булевих функцій, пов'язаних з алгоритмами шифрування, функціями менш складної структури. Обґрунтування практичної стійкості потокового шифру відносно будь-якої з таких атак зводиться до встановлення факту відсутності зазначених наближень.

2. Розроблено статистичну атаку на генератори гами з лінійним законом реініціалізації початкового стану за певних умов дозволяє відновлювати ключі довжиною 128 біт зі складністю не більше 2^{38} елементарних операцій, використовуючи не більше 2^{15} відрізків гами довжиною не більше 117 знаків кожен разом з відповідними векторами ініціалізації.

3. Розроблено статистичну атаку на синхронні потокові шифри, яка узагальнює атаку FKM, кубічну атаку і базується на наближеннях булевих функцій, що реалізуються алгоритмами шифрування, алгебраїчно виродженими функціями. Трудомісткість цієї атаки залежить лінійно від складності обчислення значення функції-наближення та алгоритму опробування ключів, що використовується. Для випадку редукованої версії шифру Grain-128 трудомісткість узагальненої статистичної атаки не перевищує 2^{97}, що є в 2^{27} разів менше ніж трудомісткість раніше відомої атаки.

4. Розроблено метод побудови списку всіх k-вимірних функцій степеня не вище d, що знаходяться на відносній відстані не більше $2^{-d}(1-\varepsilon)$ від булевої функції n змінних, який суттєво покращує аналогічний раніше відомий алгоритм Гопалана (має меншу трудомісткість у порівнянні з останнім, у певних випадках в 1000 та більше разів). Зазначений 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. Зокрема, при $k \le 4$ цей метод дозволяє за декілька секунд побудувати список усіх високоймовірних k-вимірних наближень функції Карле-Фенга від $n = 5$ змінних.

5. Для обґрунтування відсутності високоймовірних k-вимірних наближень зрівноважених булевих функцій можна використовувати запропонований метод обчислення значень нижніх меж відносної відстані між заданою булевою функцією та множиною всіх k-вимірних функцій від n змінних. Застосування цього методу дозволяє знизити трудомісткість процедури оцінювання стійкості функції ускладнення шифру Achterbahn-80 приблизно в 5 разів (з 3020 секунд до 652 секунд на звичайному ПК), що свідчить про скорочення часу проведення експертних досліджень алгоритмів потокового шифрування, призначених для захисту державних інформаційних ресурсів.

6. Для знаходження (чи обґрунтування відсутності) певних алгебраїчно вироджених наближень булевих функцій, заданих за допомогою оракулів, можна використовувати метод, викладений в розділі 4. Метод складається з двох етапів, на першому з яких здійснюється пошук певних підпросторів, що є допустимими для вхідної функції-оракула (при цьому відсутність зазначених просторів свідчить про відсутність відповідних наближень). На другому етапі за знайденим

підпростором будується булева функція від меншої кількості змінних, яка (разом з базисом знайденого підпростору) задає наближення вхідної функції. Для розв'язання окремих задач на кожному етапі методу запропоновано поліноміальні ймовірнісні алгоритми, які можуть бути застосовані на практиці до функцій-оракулів від декількох десятків чи сотень змінних.

7. Для проведення процедури обґрунтування стійкості перспективних програмно-орієнтованих потокових шифрів доцільно використовувати спеціально створені прикладні програми (див. додатки А, Б, В, Д), які реалізують методи обґрунтування стійкості, наведені в 3 та 4 розділах дисертації. Виконання вказаних програм можливе на стандартному комп'ютері за доступний для огляду час (від декількох секунд до декількох діб).

8. Застосування розробленого методу пошуку алгебраїчно вироджених наближень булевих функцій (див. розділ 4 дисертації) до низки функцій $F_{\text{SNOW-2.0}}$ для побудови узагальненої статистичної атаки на шифр SNOW-2.0 (прототип майбутнього національного стандарту потокового шифрування України) дає негативний результат. Зокрема, при $s \le 20$, $\theta = 0{,}6$ з достовірністю не менше ніж $0{,}99$ жодна з зазначених функцій не має наближень, які знаходяться від неї на відносній відстані не більше ніж $1/2 \cdot (1-\theta) = 0{,}2$ та мають вигляд $\varphi(kM_0, c)$, $(k,c) \in V_{128} \times V_{128}$, де $\varphi : V_{148} \to \{0,1\}$, $M_0 \in \mathbf{F}_2^{128\times 20}$. Це свідчить про практичну стійкість шифру відносно узагальненої статистичної атаки.

СПИСОК ОПУБЛІКОВАНИХ ПРАЦЬ ЗА ТЕМОЮ ДИСЕРТАЦІЇ

1. Алексейчук А.Н. Статистическая атака на генератор гаммы с линейным законом реинициализации начального состояния и функцией усложнения, близкой к алгебраически вырожденной / А.Н. Алексейчук, С.Н. Конюшок, А.Ю. Сторожук // Радиотехника. – 2014. – Вып. 176. – С. 13-21.

2. Олексійчук А.М. Швидкий імовірнісний алгоритм оцінювання відстані між зрівноваженою булевою функцією та множиною *k*-вимірних функцій / А.М. Олексійчук, С.М. Конюшок, А.Ю. Сторожук // Прикладная радиоэлектроника. – 2014. – Т.13. – №3. – С.186-191.

3. Сторожук А.Ю. Дослідження теоретичного обсягу матеріалу при моделюванні статистичної атаки на генератор гами з лінійним законом реініціалізації та функцією ускладнення, що є близькою до алгебраїчно виродженої. // А.Ю. Сторожук // Спеціальні телекомунікаційні системи та захист інформації. Збірник наукових праць. – 2014. – Вип. 2 (26). – С. 12-17.

4. Олексійчук А.М. Швидкі алгоритми побудови k-вимірних наближень наближень булевих функцій // А.М. Олексійчук, С.М. Конюшок, А.Ю. Сторожук // Захист інформації. – 2015. – Т. 17. – № 1. – С. 43-52.

5. Алексейчук А.Н. Обобщенная статистическая атака на синхронные поточные шифры // А.Н. Алексейчук, С.Н. Конюшок, А.Ю. Сторожук // Захист інформації. – 2015. – Т. 17. – № 3. – С. 54-65.

6. Олексійчук А.М. Метод пошуку алгебраїчно вироджених наближень булевих функцій для побудови статистичних атак на синхронні потокові шифри / А.М. Олексійчук, С.М. Конюшок, А.Ю. Сторожук // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. – 2016. – Вип. 1 (31) 2016. – С. 65-79.

7. Конюшок С.Н. Криптографически безопасные генераторы псевдослучайных последовательностей, встроенные в операционные системы Windows и Linux / С. Н. Конюшок, А. Ю. Сторожук // Тези доповідей XV ювілейної міжнародної науково-практичної конференції ["Безопасность информации в информационно-телекоммуникационных системах"] (Київ, 22-25 травня 2012 р.). – К.: ООО "ИП ЭДЕЛЬВЕЙС", НИЦ "ТЕЗИС" НТУУ "КПИ", 2012. – С. 46.

8. Сторожук А.Ю. Модифицированная атака на фильтрующий генератор гаммы с линейным законом реинициализации и функцией усложнения близкой к алгебраически вырожденной / А.Ю. Сторожук, С.Н. Конюшок // Тези доповідей XVI міжнародної науково-практичної конференції ["Безопасность информации в информационно-телекоммуникационных системах"] (Київ, 21-24 травня 2013 р.). – К.: ООО "ИП ЭДЕЛЬВЕЙС", НИЦ "ТЕЗИС" НТУУ "КПИ", 2013. – С. 40-41.

9. Сторожук А.Ю. Статистическая атака на генератор гаммы с линейным законом реинициализации начального состояния и функции усложнения, близкой к алгебраически вырожденной / А.Ю. Сторожук, С.Н. Конюшок, С.Ж. Піскун // Праці міжнародної наукової конференції ["Питання оптимізації обчислень (ПОО-XL)"] (АР Крим, Велика Ялта, смт. Кацівелі, 30 вересня – 4 жовтня 2013 р.). – К.: Інститут кібернетики імені В.М. Глушкова НАН України, 2013. – С. 256-257.

10. Алексейчук А.Н. Статистическая атака на генератор гаммы с линейным законом реинициализации начального состояния и функцией усложнения, близкой к алгебраически вырожденной / А.Н. Алексейчук, С.Н. Конюшок, А.Ю. Сторожук // Материалы междунар. науч. конгресса ["Международный конгресс по информатике: информационные системы и технологии"] (Білорусь, Мінськ, 4-7 листопада 2013 р.). – К.: Минск: БГУ, 2013. – С. 24-27.

11. Alekseychuk A.N. Algebraic degenerate approximations of Boolean functions for key recovery attacks on stream ciphers / A.N. Alekseychuk, S.N. Konushok, A.Y. Storozhuk // International conference "Probability, reliability and stochastic optimization". Conference materials, Kyiv: Taras Shevchenko national university of Kyiv. – С. 27.

12. Конюшок С.М. Дослідження теоретичного значення обсягу матеріалу при моделюванні статистичної атаки на генератор гами з лінійним законом

реініціалізації та функцією ускладнення, що є близькою до алгебраїчно виродженої / С.М. Конюшок, А.Ю. Сторожук // Тези доповідей XVII міжнародної науково-практичної конференції ["Безпека інформації в інформаційно-телекомунікаційних системах"] (Київ, 26-28 травня 2015 р.). – К.: Державна служба спеціального зв'язку та захисту інформації України, 2015. – С. 25-26.

13. Алексейчук А.Н. Усовершенствованный метод построения статистических атак на синхронные поточные шифры / А.Н. Алексейчук, С.Н. Конюшок, А.Ю. Сторожук. // Праці міжнародної наукової конференції ["Питання оптимізації обчислень (ПОО-XLII)"] (Закарпатська обл., Мукачівський район, смт. Чинадієво, 21-25 вересня 2015 р.). – К.: Інститут кібернетики імені В.М. Глушкова НАН України, 2015. – С. 136-137.

14. Олексійчук А.М. Метод пошуку алгебраїчно вироджених наближень булевих функцій для побудови статистичних атак на синхронні потокові шифри / А.М. Олексійчук, С.М. Конюшок, А.Ю. Сторожук. // Матеріали XVIII міжнародної науково-практичної конференції (випуск 18) ["Безпека інформації в інформаційно-телекомунікаційних системах"] (Київ, 25-26 травня 2016 р.). – К.: Державна служба спеціального зв'язку та захисту інформації України, 2015. – С. 38.

АНОТАЦІЯ

Сторожук А.Ю. Методи оцінювання та обґрунтування стійкості потокових шифрів відносно статистичних атак на основі алгебраїчно вироджених наближень булевих функцій. – Рукопис.

Дисертація на здобуття наукового ступеня кандидата технічних наук за спеціальністю 21.05.01 – Інформаційна безпека держави. – Національний авіаційний університет, Київ, 2016.

У дисертації розв'язано актуальну наукову задачу розробки методів побудови науково обґрунтованих оцінок стійкості синхронних потокових шифрів (СПШ) відносно статистичних атак на основі алгебраїчно вироджених наближень булевих функцій. Отримані нові результати дозволяють на практиці оцінювати і обґрунтовувати стійкість сучасних СПШ, що, зрештою, надає можливість суттєво скоротити час проведення експертних досліджень алгоритмів потокового шифрування, призначених для захисту державних інформаційних ресурсів України. Головним прикладним результатом роботи є наукове обґрунтування практичної стійкості шифру SNOW-2.0 (прототип майбутнього стандарту потокового шифрування України) відносно статистичних атак на основі алгебраїчно вироджених наближень булевих функцій.

Ключові слова: безпека державних інформаційних ресурсів, криптографічний захист інформації, синхронний потоковий шифр, статистична атака, алгебраїчно вироджене наближення булевої функції.

АННОТАЦИЯ

Сторожук А.Ю. Методы оценивания и обоснования стойкости поточных шифров относительно статистических атак на основе алгебраически вырожденных приближений булевых функций. – Рукопись.

Диссертация на соискание научной степени кандидата технических наук по специальности 21.05.01 – Информационная безопасность государства. – Национальный авиационный университет, Киев, 2016.

В диссертации решена актуальная научная задача разработки методов построения научно обоснованных оценок стойкости синхронных поточных шифров (СПШ) относительно статистических атак на основе алгебраически вырожденных приближений булевых функций.

В первом разделе проанализированы современное состояние и направления развития методов криптографической защиты информации с использованием СПШ в специальных информационно-телекоммуникационных системах Украины, проведен анализ методов оценки и обоснования стойкости СПШ относительно известных атак. На основе проведенного анализа доступных научных публикаций показано, что наиболее мощными атаками на СПШ являются атаки на основе подобранных векторов инициализации (ВИ), к которым относятся атака FKM, кубическая атака и различные их модификации.

Во втором разделе описаны статистические атаки на СПШ, обобщающие ранее известные атаки (в частности атаку FKM и кубическую атаку). Полученные аналитические оценки трудоемкости предложенных атак свидетельствуют об их более высокой эффективности по сравнению с аналогичными ранее известными. В частности применение одной из этих атак к редуцированной версии шифра Grain-128 позволяет уменьшить вычислительную сложность восстановления ключа примерно в 2^{27} раз по сравнению с атакой FKM.

В третьем разделе описано два метода решения задачи построения и/или обоснования отсутствия высоковероятных k-мерных приближений булевых функций, используемых в СПШ. Первый метод предназначен для построения списка всех k-мерных функций степени не выше d, находящихся на относительном расстоянии не более $2^{-d}(1-\varepsilon)$ от булевой функции n переменных, заданной вектором значений, $1 \le d \le k < n$, $\varepsilon \in (0,1)$ и является более эффективным по сравнению с ранее известным алгоритмом Гопалана (в 1000 и более раз). Второй метод предложен впервые и предназначен для вычисления значений нижних границ относительного расстояния между уравновешенной булевой функцией и множеством k-мерных функций. Показано, что применение разработанных методов на практике позволяет в ряде случаев заметно сократить время проведения исследований алгоритмов поточ-

ного шифрования, предназначенных для защиты государственных информационных ресурсов.

В четвертом разделе изложен метод нахождения (обоснования отсутствия) определенных алгебраически вырожденных приближений булевых функций, заданных при помощи оракулов, который отличается, по сути, от известных и позволяет охватить более широкий класс приближений.

Применение разработанного метода к шифру SNOW-2.0 (прототип будущего национального стандарта поточного шифрования Украины), позволяет сделать обоснованный вывод о практической стойкости этого шифра относительно обобщенной статистической атаки (при этом время выполнения компьютерной программы составляет примерно 187 часов).

В целом, полученные новые научные и практические результаты имеют универсальный характер и позволяют существенно сократить время проведения экспертных исследований алгоритмов поточного шифрования, предназначенных для защиты государственных информационных ресурсов Украины.

Ключевые слова: безопасность государственных информационных ресурсов, криптографическая защита информации, синхронный поточный шифр, статистическая атака, алгебраически вырожденное приближение булевой функции.

ABSTRACT

Storozhuk A.Yu. Evaluation and provability methods of the stream ciphers' security against statistical attacks based on algebraic degenerate approximations of Boolean functions. – Manuscript.

The thesis for a Candidate of Technical Science degree by specialty 21.05.01 – Information security of the state. – National Aviation University, Kyiv, 2016.

This thesis describes methods that allow evaluate and scientifically prove the synchronous stream ciphers' security against statistical attacks based on algebraic degenerate approximations of Boolean functions. Obtained results allow practically evaluate and prove the synchronous stream cipher' security and also give an opportunity to significantly reduce time of expert researches applied to stream encryption algorithms used to secure Ukrainian state information resources. Main applied result is a scientific provability of SNOW-2.0 (prototype of future Ukrainian national stream encryption standard) security against statistical attacks based on algebraic degenerate approximations of Boolean functions.

Key words: state information resources, cryptographic protection of information, synchronous stream cipher, statistical attack, algebraic degenerate approximation of Boolean function.

Підписано до друку 14.02.17. Зам. №14-02(1)/15.
Формат 60х84/16. Обл. вид. арк. 1,1. Наклад 100 прим.
Друк «НВФ «Славутич-Дельфін».
пр-т Космонавта Комарова, 1.
Тел./факс: 406-74-41