ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
РАДІОЕЛЕКТРОНІКИ

ШИРОКОВ ОЛЕКСІЙ ВІКТОРОВИЧ

УДК 681.3.06:519.248.681

МЕТОДИ ФОРМУВАННЯ S-БЛОКОВИХ КОНСТРУКЦІЙ ВИПАДКОВОГО ТИПУ З ПОКРАЩЕНИМИ ПОКАЗНИКАМИ СТІЙКОСТІ ДЛЯ БЛОКОВИХ СИМЕТРИЧНИХ ШИФРІВ

Спеціальність: 05.13.21 – системи захисту інформації

Автореферат
дисертації на здобуття наукового ступеня
кандидата технічних наук

Харків - 2010 р.

Дисертацією є рукопис.
Робота виконана в Харківському національному університеті радіоелектроніки Міністерства освіти і науки України.

Науковий керівник: кандидат технічних наук, доцент
Лисицька Ірина Вікторівна,
Харківський національний
університет радіоелектроніки,
доцент кафедри безпеки
інформаційних технологій

Офіційні опоненти: доктор технічних наук, професор
Сорока Леонід Степанович,
в.о. ректора Академії митної служби України,
м.Дніпропетровськ

доктор технічних наук, професор
Олексійчук Анатолій Миколайович,
професор Інституту спеціального зв'язку та захисту
інформації Національного технічного університету
України «Київський політехнічний інститут», м. Київ

Захист відбудеться «7» грудня 2010 р**.** о 10 годині на засіданні спеціалізованої вченої ради К 64.052.05 у Харківському національному університеті радіоелектроніки за адресою: 61166, м. Харків, просп. Леніна,14.

З дисертацією можна ознайомитись у бібліотеці Харківського національного університету радіоелектроніки за адресою: 61166, м. Харків, пр. Леніна,14.

Автореферат розісланий «6» листопада 2010 р.

Вчений секретар
спеціалізованої вченої ради М.М. Рожицький

ЗАГАЛЬНА ХАРАКТЕРИСТИКА РОБОТИ

Актуальність теми. Симетричні методи шифрування зберігають свою придатність й переваги для використання, як в ближній, так і в далекій перспективі, і питання їх подальшого удосконалення складає одне з важливіших й актуальніших напрямів розвитку сучасної криптографії.

Історично для України судьба склалася так, що вона не має симетричного блочного шифру власної розробки. І сьогодні діючим стандартом в Україні є ГОСТ 28147-89, розроблений у колишньому Радянському Союзі та сьогодні перезатверджений як ДСТУ ГОСТ 28147:2009. Цей стандарт, однак, в світі останніх досягнень сучасної криптографії вже не може рахуватися достатньо надійним. На заміну діючих стандартів шифрування новими сьогодні пішли все країни-лідери засвоєння сучасних інформаційних технологій.

Актуальність прогресивного подальшого розвитку технологій симетричного шифрування ярко підтверджується організацією й проведенням міжнародних конкурсів, минулі в останні десятиріччя: AES (по вибору нового стандарту шифрування США), а також NESSIE і CRYPTREC.

По цьому ж шляху пішла й Україна. 30 червня 2005 р. на сайті ДСТЗІ України з'явилася офіційна об'ява о проведенні конкурсу по висуванню кандидатів на національній стандарт шифрування. В процесі проведення конкурсу було розглянуто п'ять пропозицій, з котрих на остаточний розгляд було представлено чотири (шифри ADE, Калина, Мухомор и Лабіринт). В відборі й аналізі представлених рішень прийняли участь вчені та розробники колективу ЗАТ ІІТ, котрі представили на конкурс дві своїх пропозиції (Калина, Мухомор). Звичайно, робота над експертизою проектів потребувала засвоїти накопичений міжнародний досвід, й форсувати розробку власних підходів та методик, які дозволяють прискорити процес аналізу та прийняття рішень. За результатами конкурсу прийнято рішення зупинитися на загальноприйнятому мировому стандарті Fips-197. Національні пропозиції оказались або занадто близькими за конструкцією до мирового лідера, або недостатньо прозорими з точки зору очікуваних показників стійкості в порівнянні з світовим авторитетом. Це означає, що робота по пошуку більш перспективних рішень, по подальшому розвитку й удосконаленню технологій блочного симетричного шифрування для України зберігає свою актуальність та затребуваність.

Актуальність теми даної роботи визначається необхідністю розвитку національної криптографічної бази по розробці нових симетричних блочних алгоритмів шифрування. Інтереси роботи зосереджуються на вивченні та дослідженні перспективних принципів побудування блоків нелінійних замін для сучасних шифрів, котрі багато в чому визначають їх криптографічні

властивості й показники.

Зв'язок роботи з науковими програмами, планами, темами. Автор роботи приймав участь в розробках ЗАТ ІІТ-а по блочним симетричним шифрам, що були представлені на український конкурс по відбору кандидата на національний стандарт шифрування в частині обґрунтування й оцінки поданих рішень, а також у виконанні НДР №09-06 ″Дослідження та розробка комбінованих інфраструктур з відкритими ключами на основі використання існуючих ІВК та системи на ідентифікаторах″ (ДР № 0109U002498), що виконувалась в ХНУРЕ, в частині реалізації протоколів з застосуванням блочних симетричних шифрів.

Мета та задачі досліджень. *Метою досліджень* є розробка (удосконалення) методів побудування (відбору) підстановочних конструкцій (S-блоків) блочних шифрів з покращеними крипрографічними показниками стійкості.

Для досягнення поставленої мети вирішені наступні *основні задачі*:

1. Оцінити сучасний стан і методи проектування і розробки S-блокових конструкцій БСШ, що будуються з використанням математичного апарату булевої алгебри. Виконати дослідження алгебраїчних показників блоків замін сучасних шифрів, у тому числі шифрів, представлених на український конкурс.

2. Розробити (розвинути) альтернативний підхід до побудови (відбору) S-блоків з використанням показників випадковості, зокрема, удосконалити методи відбору підстановок за комбінаторними показниками (інверсіям, зростанням і циклам) на основі посилювання існуючих критеріїв.

3. Дослідити (оцінити) очікувану ефективність (реалізуємість) двох нових запропонованих методів відбору випадкових підстановок, що будуються на основі оцінки близькості емпіричних законів розподілу XOR таблиць і емпіричних законів розподілу зсувів таблиць лінійних апроксимацій S-блоків теоретичним законам розподілів ймовірностей випадкових підстановок.

4. Дослідити можливості удосконалення цих двох методів на основі посилювання критеріїв відбору, аж до наближення їх до теоретичних значень.

5. Виконати дослідження показників випадковості і кореляційних властивостей S-блокових конструкцій сучасних блокових симетричних ширах (БСШ), у тому числі і БСШ, представлених на український конкурс з вибору кандидата національного стандарту.

6. Виконати дослідження кореляційних властивостей і інших криптографічних показників S-блоків, відібраних по новій системі критеріїв з метою підтвердження їх ефективності.

7. Виробити пропозиції і рекомендації по побудові S-блоковіх конструкцій

для перспективних шифрів.

Об'єктом досліджень є процеси криптографічних перетворень з використанням блокових симетричних шифрів.

Предметом досліджень є криптографічні показники S-блокових конструкцій сучасних шифрів.

Методи досліджень. При виконанні дисертаційної роботи використовувались наступні методи: теорії ймовірностей; математичної статистики; комбінаторіки і системнного аналізу; методи статистичних випробувань; методи булевої алгебри.

Наукова новизна отриманих результатів дисертаційної роботи полягає в наступному:

1. Удосконалені та розроблені нові методи відбору випадкових підстановок за комбінаторними, диференціальними і лінійними показниками, що дозволяють відібрати підстановки з покращеними криптографічними показниками.

2. Теоретично обґрунтовані значення параметрів відбору і відповідні цим значенням параметри проходження випадкових підстановок, що реалізуються.

3. За допомогою методів алгебри і комбінаторних аналізу досліджені криптографічні показники підстановочних перетворень сучасних шифрів і підстановок нового типа. Показано, що в цілому алгебраїчні властивості розглянутих підстановочних перетворень виявляються близькими одні до других. Зроблений висновок, що алгебраїчні методи аналізу за допомогою апарату булевої алгебри є малоефективними для оцінки криптографічних показників підстановок. Всі розглянуті підстановочні перетворення не володіють кореляційною імунністю, і для них не виконується критерій розповсюдження.

4. Вперше показано, що досконалі підстановки (підстановки, відібрані за новими критеріями), не дивлячись на те, що вони не реалізують мінімально можливих значень максимумів XOR таблиць і зсувів таблиць лінійних апроксимацій, володіють вищими показниками по середньому числу векторів, що задовольняють критерію розповсюдження і кореляційної імунності.

5. На прикладах оцінки показників стійкості зменшених моделей ряду сучасних шифрів, і, зокрема, шифрів, представлених на український конкурс з вибору кандидата на національний стандарт, показана підвищена ефективність вживання в таких шифрах підстановочних конструкцій нового типа в порівнянні з підстановками, використаними в оригіналах. Нові підстановки забезпечують не менше або менше на один-два загальне число циклів, необхідне для досягнення шифром асимптотичних показників диференціальних та лінійних характеристик.

Практична значимість отриманих результатів полягає у наступному:

1. Введене нове визначення випадкової підстановки, засноване на вживання системи жорстких критеріїв відбору (комбінаторних критеріїв, доповнених диференціальними і лінійними критеріями).

2. Встановлена можливість відбору досконалих підстановок, що володіють теоретичними значеннями показників випадковості підстановки, вибраної з повного ансамблю підстановок симетрическької групи довільним (випадковим) чином.

3. Теоретично і експериментально встановлено, що для підстановок порядку 2^8, що використовуються в сучасних шифрах (байтових підстановок), із загального числа підстановок симетричної групи $8{,}578 \cdot 10^{506}$ досконалими і близькими до них є близько $6{,}862 \cdot 10^{502}$ підстановок.

4. Зроблений висновок про практичну недоцільність вживання алгебраїчних методів оцінки властивостей булевих функцій для виконання реальних оцінок криптографічних показників S-блоків. Диференціальні і лінійні властивості підстановок можуть бути визначені і без залучення апарату булевої алгебри.

5. Запропоновані конкретні підстановочні конструкції для вживання в перспективних шифрах.

Основні результати роботи використані в ЗАТ ″Інститут Інформаційних Технологій″, а також в учбовому процесі в Харківському національному університеті радіоелектроніки.

Особистий внесок здобувача. Дисертація є результатом самостійної роботи автора. У роботах, написаних в співавторстві, претендентові належить: у [1] – постановка статистичного експерименту і статистична обробка результатів експериментальних досліджень за оцінкою впливу значень критеріїв відбору на відсоток проходження (відбору) випадкових підстановок; [2] – дослідження диференціальних властивостей зменшеної моделі шифру ″Лабіринт″; [3] – виведення розрахункових співвідношень за оцінкою відсотка проходження підстановок при виборі параметрів відбору, що забезпечують збіг значень емпіричних законів розподілу зсувів таблиць лінійних апроксимацій випробовуваних підстановок з теоретично обчисленими значенням, і експериментальна перевірка відповідності розрахункових даних результатам статистичного експерименту по відбору ″досконалих″ (що пройшли нові критерії відбору) підстановок.

Апробація результатів. Основні положення дисертаційної роботи та результати досліджень доповідалися і обговорювалися на конференціях: Перша Міжнародна науково-технічна конференція ✧Комп’ютерні науки и

технології✧ (Білгород, 2009р.); XII Міжнародна науково-практична конференція ″Безпека інформації в інформаційно-телекомунікаційних системах″ (Київ, 2009р.) – два доклади; XIII Міжнародна науково-практична конференція ″Безпека інформації в інформаційно-телекомунікаційних системах″ (Київ, 2010р.) – чотири доклади.

Публікації. Результати дисертаційної роботи опубліковані в трьох статтях у наукових журналах та збірниках наукових праць, що входять до переліку наукових фахових видань України, та 7 матеріалах і тезах наукових конференцій.

Структура та об'єм дисертації. Робота складається зі вступу, чотирьох розділів, чотирьох додатків. Загальний обсяг дисертації складає 227 сторінок, з яких основний зміст викладено на 173 сторінках друкованого тексту, 3 рисунки, 52 таблиці. Список використаних джерел складається з 159 найменувань на 16 сторінках.

ОСНОВНИЙ ЗМІСТ РОБОТИ

У **вступі** до дисертації обґрунтовано актуальність проблеми, сформульована мета роботи, дано стислу анотацію отриманих результатів, відзначено їх наукову новизну та практичне значення.

У **першому розділі** надана загальна характеристика сучасного етапу розвитку технологій захисту інформації в України. Відмічається, що симетричні шифри й сьогодні є серцем криптографічного захисту усіх скільки-небудь відповідальних систем управління господарчою, економічною, виробничої і багатьох інших галузей діяльності суспільства, колективу, регіону, держави, забезпечуючи інформаційну взаємодію між органами та об'єктами управління.

Актуальність прогресивного подальшого розвитку технологій симетричного шифрування ярко підтверджується організацією й проведенням міжнародних конкурсів, що пройшли в останні десятиріччя (AES по вибору нового стандарту шифрування США, а також NESSIE та CRYPTREC).

В цій роботі під технологіями блочного симетричного шифрування розуміється як проектування та розробка безпосередньо шифрів, так і забезпечуючи методи проектування й розробки шифрів відповідні теоретичні та практичні методи оцінки показників стійкості (надійності) шифрів (методи криптоаналізу).

По цьому ж шляху рухається й Україна. 30 червня 2006 року на сайті ДСТЗІ України з'явилась офіційна об'ява о проведенні конкурсу по висуванню кандидатів на національний стандарт шифрування. В процесі проведення конкурсу було розглянуто п'ять пропозицій, з котрих на остаточний розгляд

було представлено чотири (шифри ADE, Калина, Мухомор та Лабіринт). У відборі й аналізі представлених рішень прийняли участь й вчені і розробники колективу ЗАТ ІІТ, котрі самі представили на конкурс дві своїх пропозиції (Калина, Мухомор). Звичайно, робота над експертизою проектів потребувала засвоїти міжнародний досвід, і форсувати розробку власних підходів і методик, що дозволяють прискорити процес аналізу та прийняття рішень. По результатам конкурсу прийнято рішення зупинитися на загально признаному світовому стандарті Fips-197. Національні пропозиції виявилися або надто близькими за конструкцією до світового лідера, або недостатньо прозорі з точки зору сподіваних показників стійкості в порівнянні з світовим авторитетом. Це означає, що робота по пошуку більш перспективних рішень, подальшому розвитку й удосконаленню технологій блочного симетричного шифрування для України зберігає свою актуальність та затребуваність й сьогодні.

Зосереджується увага на новому підході в теорії та методах криптоаналізу, що розвивається на кафедрі БІТ ХНУРЕ. Він орієнтований, з одного боку, на використання при визначенні очікуваних показників стійкості БСШ результатів аналізу їх зменшених версій, а з другої, – уточненій за останній час на основі вивчення властивостей та показників випадкових підстановок та зменшених моделей шифрів, що розглядаються як підстановочні перетворення, концепції (нової ідеології) визначення показників стійкості БСШ к атакам диференційного та лінійного крипто аналізу. У цьому випадку вдається подолати труднощі аналізу повномасштабних моделей (алгоритмів) за рахунок розробки й дослідження зменшених моделей прототипів, для котрих обчислювальних ресурсів, що маються, виявляється вже достатнім. Виникає можливість вирішити багато які задачі аналізу й порівняння показників стійкості відповідних великих версій.

Ілюструється важлива роль та місце блочних симетричних шифрів у сучасних технологіях захисту інформації, на прикладі широко розповсюдженого SKIP протоколу, реалізовано в багатьох сучасних стандартах у вигляді гібридних шифрів, у котрих ″асиметричні шифри використовуються для зашифрування секретного ключа, який у свою чергу використовуються для зашифрування фактичного повідомлення з застосуванням симетричних криптографічних методів″.

На прикладі шифру Rijndael кратко обговорюються сучасні методи проектування й розробки БСШ, де відмічається важлива роль, яка приділяється вибору S-блоків (блоків нелінійної заміни) при конструюванні цього шифру.

Викладається характеристика сучасних підходів до оцінки показників

стійкості БСШ к атакам диференційного та лінійного криптоаналізу, які пов’язуються в більшості робіт з диференційними та лінійними властивостями S-блоків, що використовуються практично у всіх шифрах.

Формулюються мета й задачі роботи, які визначаються актуальністю рішення ряду теоретичних та практичних задач удосконалення технологій блочного симетричного шифрування, спрямованих, в першу чергу, на пошук нових рішень по побудуванню підстановочних перетворень з покращеними криптографічними показниками по відношенню до найбільш потужних атак лінійного та диференційного криптоаналізу.

Другий розділ присвячений розгляду відомих методів аналізу та проектування підстановочних конструкцій сучасних блочних шифрів. Відмічається, що у теперішній час найбільш розробленим та найбільш популярним математичним апаратом оцінки криптографічних властивостей нелінійних елементів заміни (S-блоків) став апарат лінійної алгебри й зокрема апарат булевих функцій. Його розвитку та застосуванню присвячена велика кількість публікацій.

Відмічається також запропонований у свій час на кафедрі БІТ ХНУРЕ підхід до відбору підстановок, що будується на основі оцінки показників їх випадковості (значень числа циклів, зростань та інверсій), доповнений обмеженнями на максимально припустимі значення таблиць XOR різниць та таблиць лінійних апроксимацій. Вже давно виникло бажання знайти зв’язок між відміченими підходами й, зокрема, оцінити місто й корисність критеріїв випадковості в спільному комплексі питань, пов’язаних з рішенням задач побудування криптографічно стійких підстановочних конструкцій. Цьому напрямку й буде в подальшому присвячена дана робота.

Отже значна частина розділу присвячена викладенню методики аналізу властивостей нелінійних елементів заміни з допомогою апарату булевих функцій.К теперішньому моменту напрацьований вже достатньо великий набір підходів до опису та аналізу властивостей нелінійних елементів заміни в термінах булевої алгебри.

К показникам стійкості нелінійних перетворень в термінах булевих функцій відносять: збалансованість вихідної послідовності; нелінійність функції; кореляційний імунітет; критерій розповсюдження; алгебраїчну степінь перемінних; значення функції автокореляції та інші. В розділі розглянута розроблена в цьому напрямку термінологія, введені терміни й означення.

Окремо розглядаються критерії оцінки криптографічних властивостей S-блоків, побудовані з використанням алгебраїчних методів серед яких: нормалізоване значення квадратів помилок, нормалізована коваріація і варіація, кореляційний коефіцієнт,лавинний вектор або лавинна змінна, критерій бітовій

незалежності, критерій нелінійності, суворий лавинний критерій, максимальний порядок Суворого Лавинного Критерію, лінійна апроксимаційна таблиця – LAT, XOR таблиця.

Подальший матеріал присвячений викладенню суті відомих підходів до побудуванню (генерації) криптографічно стійких S-блоків.Висвітлюються не всі відомі підходи та методи конструювання S-блокових конструкцій. Увага зосереджується лише на тих роботах, котрі відрізняються найбільшою теоретичною завершеністю, а також практичною спрямованістю та результативністю.

В числі регулярних методів конструювання S-блоків що відрізняються теоретичною завершеністю розглядаються два підходи, що відібрані на основі виконаного аналізу великої кількості публікацій у даному напрямку. Це перш за все підходи й результати, викладені в роботах К. Нюберг, а також розробки групи австралійських вчених під керівництвом Дж. Себеррі.

У відношенні до підходу, що розвинутий групою Дж. Себеррі робиться висновок, що запропонований підхід, не глядячи на красивий математичний апарат, котрий дозволив виконати строге обґрунтування властивостей S-блоків, що конструюються, він все ж таки представляється достатньо складним для практичного застосування. Наші спроби скористатися цим методом для породження S-блоків розміру $n \times n$ ($n = 8$) закінчилися невдачею, – ми не змогли отримати набір підходящих булевих функцій необхідного розміру. Підкреслимо також, що нам не вдалося знайти й свідоцтв застосування цього підходу для конструювання S-блоків іншими дослідниками.

Більш прогресивними бачаться пропозиції й розробки К. Нюберг. Саме вони знайшли подальший розвиток та практичне застосування при побудові таких сучасних шифрів, як Camellia, Rijndael, ADE, Калина, Лабіринт та інші.

Наводиться опис конструкцій S-блоків, що виникли в процесі створення нових блочних симетричних шифрів, у тому числі і шифрів представлених на український конкурс. В основі багатьох з них лежить використання результатів й пропозицій К. Нюберг.

Найбільш результативна частина розділу присвячена дослідженню криптографічних властивостей S-блоків сучасних шифрів з допомогою викладеного апарату булевих функцій, доповнених перевіркою виконання критеріїв випадковості. Для здійснення цих досліджень були розроблені програмні комплекси, які дозволили одразу отримати (розрахувати) дві групи криптографічних показників. В одну групу увійшли:число зростань, число циклів, число інверсій, δ-рівномірність S-блоку, максимальне значення лінійної апроксимаційної таблиці.

В другу групу показників, які, орієнтовані на алгебраїчний опис S-блоків з допомогою математичного апарату булевих функцій, ввійшли: збалансованість булевих функцій S-блоку, середня й мінімальна за множиною функцій S-блоку кількість термів АНФ, середня й мінімальна за змінними множин функцій кількість термів, кореляційний імунітет S-блоку $-KI(k)$, критерій розповсюдження (суворий лавинний критерій) функції $-KP(k)$, алгебраїчна степінь булевих поліномів S-блоку $-\deg_f(S)$, сума квадратів автокореляцій, тобто, $\sigma_f = \sum_s r_f(s)^2$ й пов'язане с цим показником нормалізоване значення квадратів помилок $1 - \overline{\sigma}_S^2 = \min_f(1 - \overline{\sigma}_f^2)$.

Численні розрахункові й статистичні результати не вдається подати в авторефераті. Ми тут лише відмітимо, що були розглянуті й перевірені по визначеним вище групам показників S-блоки шифрів AES, ADE, Лабіринт, Мухомор, Калина, FOX, ICEBERG, Camellia, GrandCru та Anudis.

Аналіз показав, що усі розглянуті S-блоки сучасних шифрів виходять за рамки випадкових підстановок по інверсіям, зростанням і циклам, і, що більш цікаво, не задовольняють таким важливим показникам булевих функцій як критерій розповсюдження та не володіють кореляційною імунністю.

Отже робиться висновок, що хоча і в літературі приділяється велика увага до розвитку й застосуванню для оцінки криптографічних показників S-блоків алгебраїчних методів на основі математичного апарату булевих функцій, однак, цей алгебраїчний підхід для розглянутих конструкцій S-блоків не є визначальним. Більш того, S-блокові конструкції, що використані у сучасних шифрах володіють далеко не кращими, а по ряду показників й надто низькими криптографічними показниками булевих функцій, котрі входять (визначають) S-блок. Реальні конструкції S-блоків будуються, скоріше, спираючись на першу групу відокремлених вище криптографічних показників, котрі можуть бути визначені без при притягання апарату булевих функцій (хоча й мається прямий зв'язок деяких з показників цієї групи з властивостями булевих функцій S-блоку).

У третьому розділі здійснюється розробка й дослідження нової (вдосконаленої) методики відбору випадкових підстановок за рахунок поширення критеріїв їх відбору (к уточненим комбінаторним показникам додаються ще два критерії, пов'язані з новими даними по теоретичному опису диференційних та лінійних властивостей випадкових підстановок).

Спочатку увага зосереджується на короткому викладенні підходу до визначення випадкових підстановок, що базується на використанні відомих з комбінаторики асимптотичних законів розподілу інверсій, зростань та циклів.

Випадковою при цьому підході вважається підстановка, котра по інверсіям, зростанням і циклам попадає в інтервали, що задаються середньоквадратичним відхиленням кожного із цих параметрів від математичного очікування відповідного асимптотичного (нормального) закону розподілу, що відповідає значенню критерію відбору по комбінаторним показникам $a = 1$ (a– нормуючий коефіцієнт перед середньоквадратичним відхиленням, котре також визначається з теоретичного розподілу).

Виконуючи оцінку цих результатів з позицій теперішнього часу, робиться висновок, що запропоновані в відомих роботах параметри відбору є вельми м'якими. Досвід показує, що границі, які використовуються в відомому підході, проходять підстановки з далеко не кращими криптографічними властивостями. Тому в роботі вивчаються можливості підвищення жорсткості критеріїв відбору по інверсіям, зростанням і циклам. Реалізуючи цю задачу було виконано теоретичне обґрунтування цієї можливості з подальшою наступною експериментальною перевіркою. Результати розрахунків підтвердили можливість здійснення значень інверсій, зростань і циклів навіть співпадаючих з теоретичними значеннями, які випливають з асимптотичних законів розподілу відповідних параметрів (можна реалізувати критерії відбору практично для параметру $a = 1$). Розрахунки свідчать, що показниками, співпадаючими з теоретичними (одночасно по інверсіям, зростанням і циклам), володіють 4% підстановок 16-го порядку (експеримент – 1%). Для байтових підстановок відповідні цифри складають 0,002% (експеримент – 0,001%). Отже, підвищення жорстокості критеріїв відбору привело до суттєвого зменшення множини допустимих підстановок (старі критерії проходило близько 50% всіх підстановок).

Подальші дослідження концентруються на двох нових методах (нових критеріях) відбору випадкових підстановок. Ці два критерії були сформульовані як додатні к трьом розглянутим вище.

Основна ідея побудування нових критеріїв містилась в тому, щоб перенести властивості криптографічних перетворень, властиві блочним симетричним шифрам, що розглядаються як підстановки, на підстановочні конструкції в цілому, тобто була поставлена задача розширити критерії відбору випадкових підстановок за рахунок додатних критеріїв випадковості, характерних саме для шифрів.

Ідея підходу міститься на доведених вченими кафедри БІТ в останній час двох теоремах, які визначають теоретичні закони розподілу переходів таблиць XOR різниць та зміщень таблиць лінійних апроксимацій.

Нагадаємо спочатку сутність запропонованих критеріїв відбору. У цитує мій

роботі вони були сформульовані у вигляді четвертого і п'ятого критеріїв (1-ий, 2-ий та 3-ій – це комбінаторні критерії) наступним чином:

– підстановка задовольняє критерію випадковості 4, якщо закон розподілу переходів $\Pr(\Lambda_\pi(\Delta X, \Delta Y) = 2k,\ \Delta X, \Delta Y \in Z_2^n,\ k = 0,1,..., k^*$ її таблиці XOR різниць для входів, що приписуються до ненульових характеристик, відповідає за критерієм згоди Колмогорова теоретичному закону розподілу переходів для випадкових підстановок, тобто найбільше значення модуля різниці теоретичного і емпіричного інтегральних законів розподілу вірогідності задовольняє умові $|F_T(x_k) - F(x_k)| \le b$;

– підстановка задовільняє критерію випадковості 5, якщо закон розподілу однотипних переходів $\Pr(\lambda^*(\alpha, \beta) = 2k,\ k = 0,1,..., k^*$ для масок входу і виходу $\alpha, \beta \ne 0,\ \alpha, \beta \in Z_2^n$, її таблиці лінійних апроксимацій відповідає за критерієм згоди Колмогорова теоретичному закону розподілу лінійних апроксимацій випадкових підстановок, тобто найбільше значення модуля різниці теоретичного і емпіричного інтегральних законів розподілу вірогідності задовольняє умові $|F_T(x_k) - F(x_k)| \le c$.

Тут *k** половинні значення максимумів переходів XOR таблиці і зміщень LAT (лінійної апроксимаційної таблиці) випадкової підстановки відповідно. Значення граничних параметрів *b* і *c* були визначені як такі що підлягають уточненню за результатами експериментів. Отже в роботі і розглядається задача обґрунтування граничних значень параметрів *b* і *c* в критеріях відбору для запропонованих правил.

Для вирішення цієї задачі був розроблений програмний комплекс, що дозволяв генерувати підстановки, з допомогою якого й було здійснено дослідження впливу граничних значень критерію Колмогорова на показники відбору підстановок.

Досліджувалися підстановки порядку 2^4 та 2^8, що є найбільш популярними при конструюванні сучасних шифрів.

Спочатку були використані граничні значення параметрів *b* і *c*, які були розраховані відповідно до критерію Колмогорова (для $\alpha = 0{,}5$ з таблиці розподілу Колмогорова-Смірнова маємо $Q(\lambda_0) = 1 - \alpha = 1 - 0{,}5 = 0{,}95 \to \lambda_0 = 1{,}36$). Отже для підстановок порядку 2^4 (в критерії Колмогорова використовується параметр $n = 225$) маємо $b = c = \frac{\lambda_0}{\sqrt{n}} = \frac{1{,}23}{15} = 0.082$. Відповідно для підстановок порядку 2^8 (параметр критерію Колмогорова $n = 255^2$) приходимо до результату $b = c = \frac{\lambda_0}{\sqrt{n}} = \frac{1{,}23}{255} = 0{,}00482$.

Ці граничні значення були використані при налаштуванні програмного комплексу, що реалізовує викладену методику відбору випадкових підстановок (за трьома критеріями випадковості). Були проведені численні експерименти при різних сполученнях і значення п’яти критеріїв. В результаті обробки даних експериментів встановлено, що всі критерії випадковості є в значній мірі незалежними, кожен із критеріїв вносить свою частку в відсів підстановок, що виключаються з кандидатів на випадкові підстановки. Граничні значення параметрів відбору (допустимих розбіжностей емпіричного і теоретичного законів розподілу ймовірностей) істотно залежать від порядку досліджуваних підстановок. Зі збільшенням порядку підстановки мінімально досяжна ступінь розбіжності розподілів швидко зменшується.

Встановлено також, що критерії відбору з диференціальних і лінійних властивостей є більш жорсткими. При зменшенні значення допустимої розбіжності розподілів число підстановок, що пройшли перевірку за всіма критеріями, швидко зменшується. В цілому зроблений висновок, зо запропонована система критеріїв є досить гнучкою і може розглядатися як конструктивний підхід до відбору підстановок, що наближаються за своїми властивостями до властивостей шифруючих багатоциклових перетворень.

Далі була виконана теоретична оцінка очікуваного числа випадкових підстановок с заданими розподілами переходів парних різниць XOR таблиць зміщень таблиць лінійних апроксимацій, тобто з’ясовувалися питання практичної реалізуємості підстановок с ″граничними″ показниками, що відповідають ″еталонним″.

В основі отриманих результатів лежить використання рівняння, котре виконується для ймовірності $Pr(\Lambda_{\pi}(\Delta X,\Delta Y) = 2k_D^*$ події, яка міститься в тому, що випадкова взята підстановка буде мати перехід вхідної різниці в вихідну рівний $2k_D^*$ (максимально можливому значенню таблиці XOR різниць)

$$(2^n - 1)^2 Pr(\Lambda_{\pi}(\Delta X,\Delta Y) = 2k_D^* \approx 1.$$

Подібний вираз можна отримати і для таблиць лінійних апроксимацій.

В результаті для практично цікавих ситуацій використання в шифрах S-блоків з розмірами бітових входів рівними n=4 і n=8 для вірогідності отримання (генерації) S-блоків випадкового типу з параметрами таблиць XOR різниць і лінійних апроксимацій, що повторюють теоретичні розподіли таблиць, приходимо до таких значень:

$$Pr\left(\Lambda_{\pi}(\Delta X,\Delta Y) = 2k_D^*\right) \le \frac{1}{(2^n - 1)} \rightarrow$$

$$\rightarrow \begin{cases} n = 4 \rightarrow \Pr(\Delta_{\pi}(\Delta X, \Delta Y) = 8) = \dfrac{1}{15} = 0{,}07 \\ \\ n = 8 \rightarrow \Pr(\Delta_{\pi}(\Delta X, \Delta Y) = 12) = \dfrac{1}{255} = 0{,}004 \end{cases}$$

(при отриманні цього виразу враховано, що максимальне значення може досягатися в одному з $2^n - 1$ ненулевих рядків XOR таблиці).

Подібні результати отримані і для таблиць лінійних апроксимацій.

Результати експериментів підтвердили можливість генерації підстановок з показниками, що відповідають ″еталонним″ значенням законів розподілу ймовірностей. Підстановки, що проходять систему самих жорстких критеріїв відбору по всім п’яти критеріям запропоновано називати досконалими.

Результатом цього напрямку досліджень стало побудування (відбір) досконалих підстановок порядків 2^4 та 2^8.

Окремо також були виконані дослідження на відповідність новим критеріям відбору підстановочних конструкцій сучасних БСШ. Всі вони крім шифру DES опинилися далекими від досконалих.

В четвертому розділі роботи виконується оцінка ефективності підстановок, відібраних за новою системою критеріїв.

Спочатку виконується дослідження криптографічних показників S-блоків нового типу з допомогою апарату булевих функцій. Результати свідчать, що S-блоки, відібрані за новими критеріями випадковості, за перевіреними показниками статистичної безпеки (ступеня повноти, ступеня лавинного критерію, ступеня суворого лавинного критерію) виявилися близькими за значеннями до показників S-блоків сучасних шифрів. У той же час показники випадково взятих (довільних) S-блоків виявилися істотно нижчими.

Подальші дослідження концентруються на визначенні кореляційних властивостей підстановочних конструкцій. В основі використаної методики розрахунок матриці залежностей та матриці відстаней. Вони визначаються як

$$a_{ij} = \#\left\{x \in X \middle| \left(f(x^{(i)})\right)_j \neq \left(f(x)\right)_j\right\},$$
$$b_{ij} = \#\left\{x \in X \middle| w\left(f(x^{(i)}) - f(x)\right) = j\right\}$$

для $i = 1, \ldots, n$ і $j = 1, \ldots, n$, де X “підходяще” випадково обрана підмножина $\left(GF(2)\right)^n$.

З допомогою матриць $A = \{a_{ij}\}$ та $B = \{b_{ij}\}$ розраховуються наступні величини:

ступінь повноти

$$d_c = 1 - \frac{\#\{(i,j) \mid a_{ij} = 0\}}{n^2};$$

ступінь лавинногоефекту

$$d_a = 1 - \frac{\sum_{i=1}^{n} \left| \frac{1}{\#X} \sum_{j=1}^{m} 2jb_{ij} - m \right|}{nm};$$

ступінь суворого лавинного критерію

$$d_{sa} = 1 - \frac{\sum_{i=1}^{n} \sum_{j=1}^{m} \left| \frac{2a_{ij}}{\#X} - 1 \right|}{nm}.$$

Для більш наочного порівняння кореляційних властивостей (ступеня лавинного ефекту, ступеня суворого лавинного критерію, ступеня повноти) розглянутих у розділі вузлів заміни вони систематизовані у зведеній таблиці (табл. 1).

Таблиця 1

Зведена таблиця кореляційних властивостей розглянутих підстановок

	AES	DES	Kalina/ Muchmor	Labirinth	Anubis	New Sboxes. 1	New Sboxes. 2
d_c	0.88281	0,81250	0.89063	0.89063	0.88281	0.89063	0.89063
d_a	0,81641	0,64063	0,82104	0,80298	0,80615	0,79565	0,80786
d_{sa}	0.85791	0,72135	0.85681	0.86389	0.85596	0.86072	0.85950

Зроблений висновок, що перетворення, відібрані запропонованим методом, мають кореляційні показники близькі до показників S-блоків сучасних шифрів (сформованих або відібраних за допомогою спеціалізованих процедур).

Заключний матеріал розділу присвячений дослідженню криптографічних показників шифрів з блоками замін, відібраними за методикою, що запропонована.

За основу була взята 16 бітна конструкція шифру, представлена в роботі проф. Хеуса. Вона повторювала класичну конструкцію SPN шифру, запропоновану ще у 1974 р. Х.Фейселем. Розглядалася залежність значень максимумів повних диференціалів шифру від кількості циклів (табл. 2).

Таблиця свідчить, що шифру Хейса з S-блоком шифру Rijndael (Міні-AES) поступається за динамічними показниками S-блоку шифру DES. Аналогічні експерименти з S-блоками нового типу свідчать, що для більшість S-блоків показує результат співпадаючий з показниками S-блоку шифру DES (сім циклів), хоча і серед нових S-блоків зустрічаються не ″досконалі″ S-блоки.

Таблиця 2

Значення повного диференціалу для алгоритму Хейса з S-блоками шифру Міні-AES, напівбайтового S-блоку DES та рядом довільних S-блоків

Sbox / *r*	Sbox AESD4	Sbox HEYSD8	Sbox D6F2	Sbox D6F0	Sbox D12F0	Sbox D8F0
1	16384,00	32768,00	24576,00	24576,00	49152,00	32768,00
2	4096,00	12288,00	6144,00	6144,00	15552,00	8192,00
3	2036,27	2303,33	2802,40	1920,00	1587,20	3432,00
4	596,00	222,27	649,33	601,20	613,13	1184,47
5	190,33	64,13	292,93	148,93	265,73	457,07
6	77,47	24,80	71,47	50,00	104,87	178,40
7	35,87	**18,80**	32,00	22,00	46,87	87,33
8	21,07	18,80	19,67	**19,07**	23,87	39,93
9	**19,27**	19,00	**18,93**	18,87	**19,13**	24,60
10	19,33	18,93	19,33	19,27	19,00	24,27

Таблиця 3 ілюструє значення повного диференціала для SPN шифру з лінійним перетворенням MixColumn і ShiftRow GF (2^8) (аналог зменшеної моделі шифру Rijndael).

Таблиця 3

Значення повного диференціала для SPN шифру з лінійним перетворенням MixColumn і ShiftRow GF (2^8) (S_1, S_2, S_3та S_4–"досконалі")

S-box / *r*	Sbox AESD4	Sbox HEYSD8	Sbox S_1	Sbox S_2	Sbox S_3	Sbox S_4
1	16384,00	32768,00	24576,00	24576,00	24576,00	24576,00
2	4983,47	3635,20	5102,93	4522,67	4078,93	3515,73
3	647,47	542,93	530,13	833,07	700,80	443,73
4	42,40	22,13	34,00	66,53	21,00	**19,20**
5	20,67	**19,07**	**19,60**	40,93	**19,33**	18,93
6	**19,20**	19,27	19,33	**19,27**	19,20	18,97
7	19,13	19,00	19,20	19,20	19.33	19,53

Були розглянути і інші конструкції лінійного перетворення (MixColumn та ShiftRow GF(2^4)). Отримані результати свідчать, що S-блоки нової конструкції для всіх розглянутих зменшених моделей шифру Rijndael не поступаються за диференціальним показниками S-блокам шифру AES. Але навіть у цьому випадку вони мають перевагу перед S-блоками шифру Rijndael – це S-блоки

випадкового типу, що не піддаються алгебраїчному опису. Очікується, що цей ефект буде зберігатися і для відповідних великих прототипів;

Висновки містять основні наукові та практичні результати дисертаційної роботи.

У додатках наведено результати експериментів та табличні данні за різними розділами дисертації.

ВИСНОВКИ

В результаті досліджень, виконаних в роботі, вирішено важливе наукове і практичне завдання по розвитку теоретичної і практичної бази формування (відбору) випадкових підстановок (S-блоків) з поліпшеними криптографічними показниками для використання в перспективних БСШ.

Загальним результатом досліджень, проведених в дисертації, є обґрунтування нових (вдосконалених) критеріїв відбору випадкових підстановок за системою показників, що включають комбінаторні характеристики спільно із законами розподілу переходів таблиць XOR різниць і зміщень таблиць лінійних апроксимацій.

Головним результатом роботи слід вважати підтвердження можливості застосування найжорсткіших критеріїв відбору для породження підстановок порядку 2^4 і 2^8 за комбінаторними показниками (значенням інверсій, зростань і циклів), що повторюють математичні очікування відповідних асимптотичних законів розподілу ймовірностей, а за емпіричними законами розподілу ймовірностей переходів таблиць XOR різниць і зміщень таблиць лінійних апроксимацій повторюють відповідні теоретичні закони розподілу ймовірностей випадкових підстановок, а також експериментальне підтвердження досягнення при використанні в шифрах таких підстановок підвищених показників стійкості БСШ.

Достовірність отриманих теоретичних результатів підтверджується збігом розрахункових даних з результатами, отриманими за допомогою численних статистичних експериментів, їх несуперечністю з відомими положеннями математичної теорії підстановок, теорії ймовірності і математичної статистики.

Основні висновки.

1. Симетричні методи шифрування зберігають свою затребуваність і переваги для вирішення завдань захисту інформації, як в найближчій, так і в далекій перспективі, і подальше вдосконалення цих методів складає один з найважливіших і актуальніших напрямів розвитку сучасної криптографії.

2. Одним з напрямів, що має проблемний характер для України, є розробка вітчизняного стандарту БСШ, що задовольняє найбільш жорстким вимогам безпеки і що враховує останні досягнення теорії і практики криптоаналізу (що

має доказову безпеку до атак диференціального і лінійного криптоаналізу і до інших методів криптоаналізу).

3. Ряд теоретичних і практичних завдань вдосконалення технологій блокового симетричного шифрування може бути вирішено на основі пошуку нових рішень по побудові підстановочних перетворень з поліпшеними криптографічними показниками, застосування яких для побудови перспективних шифруючих перетворень дозволить забезпечити підвищену захищеність алгоритмів шифрування, в першу чергу, від атак лінійного і диференціального криптоаналізу.

4. Хоча і в літературі приділяється дуже велика увага розвитку і застосуванню для оцінки криптографічних показників S-блоків методів алгебри на основі математичного апарату булевих функцій, проте, цей алгебраїчний підхід для конструкцій S-блоков сучасних блокових шифрів не є визначальним. Більше того, використані в сучасних шифрах S-блокові конструкції мають далеко не кращі, а по ряду показників і дуже низьки криптографічні властивості булевих функцій, що входять в них. Реальні конструкції S-блоків можна побудувати, спираючись на групу криптографічних показників, які можуть бути визначені (розраховані) без залучення апарату булевих функцій (хоча і є прямий зв'язок деяких з показників цієї групи з властивостями булевих функцій S-блоку).

5. Результатами роботи підтверджена працездатність запропонованих на кафедрі БІТ додаткових критеріїв відбору випадкових підстановок. Зроблений висновок про те, що граничні значення параметрів відбору (допустимих розбіжностей емпіричного і теоретичного законів розподілу вірогідності) істотно залежать від порядку досліджуваних підстановок. Із збільшенням порядку підстановки мінімально досяжна міра розбіжності розподілів швидко зменшується. Запропонована система критеріїв представляється досить гнучкою і може розглядатися як конструктивний підхід до відбору підстановок, що наближаються за своїми властивостями до властивостей багатоциклових шифруючих пертворень.

6. Підтверджена теоретично і експериментально працездатність запропонованих в роботі удосконалень критеріїв відбору і можливість їх посилення за усіма показниками випадковості, що розглядаються. Підстановки, що задовольняють найжорсткішим критеріям випадковості, запропоновано називати досконалими.

7. Аналіз підстановочних перетворень сучасних шифрів свідчить про те, що використовувані в шифрах Rijndael і шифрах, представлених на український конкурс, S-блоки не є досконалими. Існують підстановки з більш високими криптографічними показниками.

8. Дослідженням впливу на результуючі показники стійкості шифрів конструкцій S-блоків, отриманих за допомогою розглянутих в роботі методів, підтверджена підвищена ефективність підстановок нового типу. Шифри з підстановками нового типу приходять до асимптотичних (потенційним) значень максимальних значень повних диференціалів і лінійних корпусів за теж саме. Або менше число циклів шифрування.

Важливим окремим результатом досліджень слід також вважати висновок про те, що за рахунок використання S-блоков випадкового типу в шифрі Rijndael перекриваються потенційні погрози, пов'язані з можливістю реалізації алгебраїчних атак. При цьому показники стійкості (до атак диференціального і лінійного криптоаналізу) не погіршуються.

Представлені в роботі результати досліджень можуть бути використані для поліпшення показників вже експлуатованих алгоритмів шифрування, а також при проектуванні і розробці нових конструкцій БСШ.

У число завдань подальших досліджень, що мають важливе значення для вдосконалення технологій БСШ, можна виділити аналіз стійкості криптографічних перетворень (шифрів) з підстановками нового типу до інших методів криптоаналізу, спрямований на підтвердження підвищеної стійкості шифрів з такими підстановками і до інших методів криптоаналізу, і обґрунтування на цій основі можливості зменшення числа циклів шифрування алгоритмів БСШ без втрати їх стійкості.

СПИСОК ОПУБЛІКОВАНИХ ПРАЦЬ ЗА ТЕМОЮ ДИСЕРТАЦІЇ

1. И.В. Лисицкая. Экспериментальная проверка работоспособности новых критериев отбора случайных подстановок / И.В. Лисицкая, К.Е. Лисицкий, А.В. Широков, Е.Д. Мельничук // Радіоелектронні та комп’ютерні системи. – 2010. – № 6 (47). – С. 87-93.

2. В.И. Долгов. Исследование циклических и дифференциальных свойств уменьшенной модели шифра ″Лабиринт″ / В.И. Долгов, И.В. Лисицкая, А.В. Григорьев, А.В. Широков // Прикладная радиоэлектроника. – 2009. – Т.8. – №3. – С. 283-289.

3. И.В. Лисицкая. Оценка числа случайных подстановок с заданным распределением парных разностей XOR таблиц и таблиц линейных аппроксимаций / И.В. Лисицкая, А.В. Широков, Е.Д. Мельничук, К.Е. Лисицкий // Прикладная радиоэлектроника. – 2010. – Т. – №3. – С. 341-345.

4. В.И. Долгов. Об одном подходе к криптоанализу БСШ / В.И. Долгов, Р.В. Олейников, В.И. Руженцев, И.В. Лисицкая, А.В. Григорьев, А.В. Широков // XII Міжнародна науково-практична конференція ″Безпека інформації в

інформаційно-телекомунікаційних системах″, 19-22 травня 2009р. – Київ. – С.18.

5. В.И. Долгов. Формирование полных дифференциалов в современных БСШ / В.И. Долгов, В.И. Руженцев, И.В. Лисицкая, А.В. Григорьев, А.В. Широков // XII Міжнародна науково-практична конференція ″Безпека інформації в інформаційно-телекомунікаційних системах″. – 19-22 травня 2009р. – Київ. – С.25.

6. В.И. Долгов. Исследование показателей стойкости БСШ, представленных на Украинский конкурс / В.И. Долгов, И.В. Лисицкая, Р.В. Олейников, В.И. Руженцев, А.В. Широков // XIII Міжнародна науково-практична конференція ″Безпека інформації в інформаційно-телекомунікаційних системах″, 18-21 травня 2010р. – Київ. – С.44.

7. И.В. Лисицкая. Анализ усовершенствований шифра Rijndael / И.В. Лисицкая, А.В. Казимиров, Е.Д. Мельничук, А.В. Широков // XIII Міжнародна науково-практична конференція ″Безпека інформації в інформаційно-телекомунікаційних системах″, 18-21 травня 2010р. – Київ. – С.45.

8. И.В. Лисицкая. Экспериментальные исследования критериев отбора подстановок по критериям близости эмпирических законов распределения вероятностей XOR таблиц и таблиц линейных аппроксимаций теоретическим / И.В. Лисицкая, Е.Д. Мельничук, А.В. Широков // XIII Міжнародна науково-практична конференція ″Безпека інформації в інформаційно-телекомунікаційних системах″, 18-21 травня 2010р. – Київ. – С.49.

9. Р.В. Олейников. Исследование дифференциальных свойств подстановок / Р.В. Олейников, И.В. Лисицкая, А.В. Широков, К.Е. Лисицкий // Сборник трудов Первой Международной научно-технической конференции ✧Компьютерные науки и технологии✧, 8-10 октября 2009г.. – Белгород. – Ч.I. – С.59-63.

10. И.В. Лисицкая. Случайные подстановки с асимптотическими значениями комбинаторных показателей / И.В. Лисицкая, А.В. Широков, А.Е. Обухов // XIII Міжнародна науково-практична конференція ″Безпека інформації в інформаційно-телекомунікаційних системах″, 18-21 травня 2010р.. – Київ. – С.46.

11. И.В. Лисицкая. Оценка числа случайных подстановок с заданным распределением парных разностей XOR таблиц и таблиц линейных аппроксимаций / И.В. Лисицкая, Е.Д. Мельничук, А.В. Широков // XIII Міжнародна науково-практична конференція ″Безпека інформації в інформаційно-телекомунікаційних системах″, 18-21 травня 2010р. – Київ. –

С.43.

АНОТАЦІЯ

Широков О.В. Методи формування S-блокових конструкцій випадкового типу з покращеними показниками стійкості для блокових симетричних шифрів– Рукопис.

Дисертація на здобуття наукового ступеня кандидата технічних наук по спеціальності 05.13.21 – системи захисту інформації. Харківський національний університет радіоелектроніки, Харків, 2010р..

Дисертаційна робота присвячена розробці методики побудування підстановочних конструкцій (S-блоків) блокових шифрів з покращеними криптографічними показниками.

В роботі знаходить свій подальший розвиток метод відбору випадкових підстановок на основі уточнення комбінаторних показників випадковості (інверсій, зростань та циклів), а також розробляються ще два методи, основані на критеріях, що пов'язані з оцінкою близькості емпіричних законів розподілу переходів таблиць XOR різниць та зміщень таблиць лінійних апроксимацій теоретичним розподілам. Теоретично і експериментально показано що можна будувати підстановки, що мають показники випадковості з самими жорсткими критеріями відбору (котрі збігаються з теоретичними значеннями).

Запропоновані конкретні підстановочні конструкції для застосування в перспективних шифрах. Підтверджена підвищена ефективність підстановок нового типу шляхом дослідження впливу на результуючі показники стійкості до атак диференціального крипоаналізу (максимальні значення повного диференціалу) зменшених моделей ряду сучасних шифрів.

Ключові слова: S-блок, підстановка, критерії випадковості, повний диференціал, таблиця диференційних різностей, таблиця линійних апроксимацій.

АНОТАЦИЯ

Широков А.В. Методы формирования S-блокових конструкций случайного типа с улучшенными показателями стойкости для блочных симметричных шифров – Рукопись.

Диссертация на соискание ученой кандидата технических наук по

специальности 05.13.21 – системы защиты информации. Харковский национальный университет радиоэлектроники, Харков, 2010.

Дисертация посвящена разработке методики построения подстановочных конструкций (S-блоков) блочних шифров с улучшенными криптографическими показателями стойкости.

В работе развивается метод отбора случайных подстановок на основе уточнения комбинаторных показателей случайности (инверсий, возростаний и циклов), а также разрабатываются еще два метода, основанные на критериях связанных с оценкой близости эмпирических законов распределения переходов таблиц XOR разностей и смещений таблиц линейных аппроксимаций теоретическим распределениям. Теоретически и экспериментально показана возможность построения подстановок, которые имеют показатели случайности с самыми жесткими критериями отбора (которые совпадают с теоретическими значениями).

Показано, что используемые в шифрах Rijndael и шифрах, представленных на украинский конкурс, S-блоки обладают далеко не лучшими, а по ряду показателей и очень низкими, криптографическими показателями булевых функций входящий в их состав.

Предложены конкретные подстановочные конструкции для применения в перспективных шифрах. Подтверждена повышенная эффективность подстановок нового типа путем исследования влияния на результирующие показатели стойкости к атакам дифференциального криптоанализа (максимумы значений полного дифференциала) уменьшенных моделей ряда современных шифров.

Ключевые слова: S-блок, подстановка, критерии случайности, полный дифференциал, таблица дифференциальных разностей, таблица линейных апроксимаций.

ABSTRACT

Shyrokov A.V. Methods of forming S-block structures of a random type with improved security indicators for block symmetric ciphers – Manuscript.

A thesis for the Scholarly Degree of candidate of technical sciences, speciality 05.13.21 – Information security systems. – Kharkov National University of Radio

Electronics, Kharkov, 2010.

The dissertation is devoted to the development of methods for constructing substitution structures (S-blocks) of block ciphers with improved cryptographic security indicators.

In this paper we improve a random substitutions selection method based on combinatorial refinement of randomness indicators (inversions, growths and cycles), and also developed two new methods based on criterias related to assessing closeness of the empirical distribution laws of transition XOR difference tables and displacements of linear approximation tables to the theoretical distributions. Theoretically and experimentally demonstrated the possibility to construct substitutions that have randomless indicators with the most stringent selection criterias (which coincide with the theoretical values).

Some new substitutions have been offered to use in future ciphers. The increased efficiency of new type substitutions was confirmed by examining the influence on the resulting indicators of resistance to differential cryptanalysis attacks (maximum values of the total differential) of reduced models of some modern ciphers.

Keywords: S-block substitution, the criteria of randomness, a total differential, XOR difference table, linear approximation table.