ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
РАДІОЕЛЕКТРОНІКИ

КАЗИМИРОВ ОЛЕКСАНДР ВОЛОДИМИРОВИЧ

УДК 004.421:004.056.55

МЕТОДИ ТА ЗАСОБИ ГЕНЕРАЦІЇ НЕЛІНІЙНИХ ВУЗЛІВ ЗАМІНИ ДЛЯ СИМЕТРИЧНИХ КРИПТОАЛГОРИТМІВ

Спеціальність: 05.13.21 – системи захисту інформації

Автореферат
дисертації на здобуття наукового ступеня
кандидата технічних наук

Харків - 2014 р.

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

Науковий керівник: кандидат технічних наук, доцент
Олійников Роман Васильович,
Харківський національний
університет радіоелектроніки,
доцент кафедри безпеки
інформаційних технологій

Офіційні опоненти: доктор технічних наук, професор
Толюпа Сергій Васильович,
Навчально-науковий інститут захисту інформації
Державного університету телекомунікацій,
директор інституту

кандидат технічних наук, доцент
Конюшок Сергій Миколайович,
Національний технічний університет України
«Київський політехнічний інститут»,
заступник начальника Інституту з навчальної
та наукової роботи

Захист відбудеться «___» _____ 2014 р. о _____ 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 «___» _____ 2014 р.

Вчений секретар
спеціалізованої вченої ради І.В. Лисицька

ЗАГАЛЬНА ХАРАКТЕРИСТИКА РОБОТИ

Актуальність теми. Симетричні алгоритми шифрування є одними з найважливіших елементів у системах захисту інформації України, особливо якщо необхідно забезпечити високу швидкодію обробки інформації. У зв'язку з чим, актуальними є напрямки розвитку та вдосконалення методів симетричних криптопримітивів.

У 2010 році в Україні закінчився відкритий конкурс на алгоритм-прототип блокового симетричного шифрування. У якості «еталону» для багатьох розробників був шифр Rijndael, який своєю перемогою на конкурсі Advanced Encryption Standard (AES) багато в чому зобов'язаний переконливому обґрунтуванню авторами швидкодії і високих показників стійкості шифру до відомих на той час атак. Багато претендентів на українському конкурсі були представлені у вигляді вдосконалених версій Rijndael. Основною метою було підвищення їх стійкості до потенційних атак, які, як передбачається, можуть використовувати простоту його алгебраїчного опису та слабкості простої схеми розгортання ключа (СРК). Після тривалого і детального процесу вивчення і дослідження представлених рішень був відзначенний шифр «Калина». Однак, в якості стандарту залишається алгоритм ДСТУ ГОСТ 28147:2009. У зв'язку з чим, також є актуальними питання щодо підвищення надійності та захищеності телекомунікаційних систем, при використанні даного алгоритму шифрування.

Однією з головних особливостей блокових симетричних шифрів (БСШ) «Калина» є нелінійне відображення, яке задається у вигляді фіксованих байтових підстановок і враховує диференціальну, лінійну та алгебраїчну атаки. На відміну від алгоритму шифрування Rijndael, де підстановка (S-блок) генерувалася на основі конструкції, наведеної ще в роботах К. Нюберг і Т. Дінга (перетворення використовує обчислення зворотного елемента в полі $GF(2^8)$ з наступним аффінним ускладненням), «Калина» має декілька випадково згенерованних нелінійних вузлів заміни. Їх основною перевагою є опис за допомогою системи алгебраїчних рівнянь степеня 3, на відміну від 2-го – для AES.

Враховуючи, що в більшості сучасних блокових симетричних шифрів для введення циклових ключів в алгоритм шифрування використовується лінійна операція (побітове додавання за модулем 2), S-блоки виявляються єдиними елементами, що визначають нелінійність шифрувального перетворення і рівень його стійкості до більшості криптоаналітичних атак. Необхідна кількість циклів БСШ обчислюється на підставі забезпечення стійкості до відомих видів криптоаналізу за умови заданих властивостей нелінійних вузлів заміни.

Таким чином, актуальність теми даної роботи визначається необхідністю створення та вдосконалення сучасних симетричних криптоалгоритмів, що підвищують надійність і захищеність інформаційно-телекомунікаційних систем

передачі даних. Зокрема, потрібні ефективні методи та засоби формування нелінійних вузлів заміни, що призводять до забезпечення високих показників стійкості і необхідних властивостей симетричних криптоперетворень.

Зв'язок роботи з науковими програмами, планами, темами. Автор роботи приймав участь у аналізі та вдосконаленні блокових симетричних шифрів, що були представлені на український відкритий конкурс алгоритму-прототипу блокового симетричного шифрування, а саме у аналізі схем розгортання ключа, захищеності алгоритмів від алгебраїчної атаки та перевірці властивостей і формування нелінійних вузлів заміни для поданих рішень. Додатково, брав участь у виконанні НДР «Розробка перспективних методів та засобів криптографічного захисту інформації в державних відомствах України» (№ДР0102U003739), «Дослідження та розробка перспективних криптографічних систем та протоколів захисту інформації у телекомунікаційних системах та мережах України» (№ ДР 0103U001981), що виконувалися в ХНУРЕ, в частині формування нелінійних відображень для блокових симетричних шифрів.

Мета та задачі досліджень. *Метою досліджень* є підвищення рівня стійкості сучасних ітеративних криптографічних примітивів до диференційного, лінійного та алгебраїчного криптоаналізів за рахунок розробки методів генерації нелінійних вузлів заміни.

Для досягнення поставленої мети вирішені наступні *основні задачі*:

1. Проведено аналіз методів формування нелінійних відображень у симетричній криптографії.

2. Розроблена математична модель представлення лінійних відображень, заданих над полем $GF(2^n)$, у матричному вигляді, що призводить до зменшення складності перевірки нелінійних відображень на еквівалентність.

3. Удосконалено метод оцінки стійкості блокових симетричних шифрів до алгебраїчної атаки на основі рішення системи нелінійних рівнянь над полем $GF(2)$.

4. Розроблено метод формування довгострокових ключових елементів для шифру ДСТУ ГОСТ 28147:2009, підстановки яких належать різним класам розширено афінної (РА) еквівалентності.

5. Розроблено ефективний метод генерації нелінійних вузлів заміни з одночасним врахуванням δ-рівномірності, нелінійності та алгебраїчних показників для перспективних блокових симетричних шифрів.

Об'єктом досліджень є процеси генерації вузлів нелінійної заміни для використання в симетричних криптоалгоритмах.

Предметом досліджень є методи генерації нелінійних вузлів заміни для сучасних симетричних криптоалгоритмів.

Методи досліджень. При виконанні дисертаційної роботи застосовувалися

наступні методи.

1. Для аналізу методів формування нелінійних відображень у симетричній криптографії використовувалися методи теорії булевих та векторних булевих функцій і статистичних випробувань.

2. При розробці математичної моделі представлення лінійних відображень, заданих над полем $GF(2^n)$, у матричному вигляді були застосовані методи теорії кінцевих полів, векторних булевих функцій та теорії складності.

3. Для удосконаленя метода оцінки стійкості блокових симетричних шифрів до алгебраїчної атаки були використані методи кінцевих полів, теорії складності, комбінаторіки та системного аналізу.

4. При розробці методу формування довгострокових ключових елементів для шифру ДСТУ ГОСТ 28147:2009 використовувалися методи теорії векторних булевих функцій та теорії множин.

5. При розробці методу генерації нелінійних вузлів заміни з одночасним врахуванням δ-рівномірності, нелінійності та алгебраїчних показників для перспективних блокових симетричних шифрів були використані методи теорії ймовірностей, статистичних випробувань, булевих та векторних булевих функцій.

Наукова новизна отриманих результатів дисертаційної роботи полягає в наступному:

1. Вперше запропоновано метод генерації вузлів нелінійної заміни для перспективних блокових симетричних шифрів з одночасним врахуванням δ-рівномірності, нелінійності та алгебраїчних показників на основі векторних булевих функцій, що дозволяє знаходити підстановки з покращеними показниками алгебраїчного імунітету і нелінійності при малих витратах ресурсів.

2. Вперше запропоновано метод формування довгострокових ключових елементів (ДКЕ) на основі класів еквівалентності векторних булевих функцій, що дозволяє генерувати вузли нелінійної заміни, які належать різним класам РА-еквівалентності та мають максимальні показники захисту від диференційного та лінійного криптоаналізів.

3. Удосконалено метод знаходження матриці лінійного відображення, заданого у вигляді полінома над полем $GF(2^n)$, який, на відміну від відомих, для рішення системи матричних рівнянь використовує набір вхідних векторів бінарного виду з одиничною вагою Геммінга, застосування якого дозволяє зменшити складність знаходження алгебраїчної форми високорівневих конструкцій криптографічних алгоритмів та перевірки векторних булевих функцій на частково розширену афінну (ЧРА) еквівалентність.

4. Отримав подальший розвиток метод оцінки стійкості блокових симетричних шифрів до аглебраічної атаки, який відрізняється від відомих

врахуванням показників кількості рівнянь у системі і її розрідженость, що дозволяє уточнити значення верхньої границі складності атаки.

5. Отримав подальший розвиток метод відбору підстановок для блокових симетричних шифрів, який базується на критеріальному підході та відрізняється від відомих комплексною оцінкою стійкості, зокрема з урахуванням запропонованого алгебраїчного критерія, що дозволяє генерувати S-блоки, використання яких в симетричних алгоритмах шифрування підвищує складність криптоаналітичних атак.

Практична значимість отриманих результатів полягає у наступному:

1. Розроблено алгоритм знаходження 8-бітових підстановок та його програмна реалізація на основі запропонованого методу генерації нелінійних вузлів заміни для перспективних блокових симетричних шифрів, що дозволяє знаходити перестановки з відсутністю фіксованих точок, нелінійністю 104, мінімальним степенем 7, алгебраїчним імунітетом 3 і δ-рівномірністю 8 на однопроцесорному комп'ютері з середнім часом роботи 3,5 години.

2. Розроблено алгоритм генерації ДКЕ для шифру ДСТУ ГОСТ 28147:2009 та його програмна реалізація на основі запропонованого методу формування довгострокових ключових елементів, що дозволяє визначити перестановки з різних класів РА-еквівалентності з показниками δ-рівномірність 4 і нелінійність 4.

3. Розроблені програмні засоби обчислення показників мінімального степеня, нелінійності, кореляційного імунітету, δ-рівномірності, циклічної структури, алгебраїчного імунітету, абсолютного індикатора, критерію розповсюдження, глобальної лавинної характеристики «сума квадратів», а також програмні засоби перевірки на збалансованість і відсутність фіксованих точок довільних векторних булевих функцій, що дозволило сформувати вимоги до вузлів нелінійної заміни.

4. Розроблено комплекси програмного забеспечення оцінювання верхньої межі ймовірності знаходження підстановок з заданими показниками стійкості до диференційного, лінійного та алгебраічного криптоаналізів на основі моделювання методу випадкової генерації підстановок в розподілених кластерних системах.

5. Розроблені практичні рекомендації щодо генерації вузлів нелінійної заміни, які дозволяють скоротити час проектування перспективних симетричних криптопримітивів.

Основні результати роботи впроваджені в ЗАТ «Інститут Інформаційних Технологій», а також в учбовому процесі Харківського національного університету радіоелектроніки.

Особистий внесок здобувача. Дисертація є результатом самостійної роботи автора. Особистий внесок здобувача в роботах, виконаних у співавторстві, полягає у наступному. У роботі [1] автором викладені основні ідеї алгебраїчної атаки на блокові симетричні шифри та проведено аналіз алгоритму шифрування «Лабіринт». Алгебраїчний криптоаналіз схеми розгортання ключа шифру «Калина» виконано у [3]. При підготовці спільної публікації [6] автор брав участь у розробці методу знаходження диференційних характеристик для мініверсій БСШ, заснованих на мережі підстановок-перестановок (SPN). У роботі [4] автором проведен аналіз критеріїв для вузлів нелінійної заміни з точки зору блокових симетричних шифрів. Основні критерії для S-блоків з використанням математичного апарату булевих функцій наведено у [5]. У статті [7] розглянуті криптографічні критерії векторних булевих функцій, а в [10] запропоновано критерій для множини підстановок. Розроблену методику практичної оцінки потужності множини станів потокового шифру «Mickey-80» та «Mickey-128», яку можна застосовувати для аналізу циклічних властивостей S-блоків, викладено у [12] та [13] відповідно. Теоретичне обґрунтування результатів робіт [12, 13] опубліковано в [11]. У роботі [9] запропоновано метод перевірки векторних булевих функцій на еквівалентність, а у статті [2] проведена порівняльна характеристика швидкодії схем розгортання ключа сучасних блокових симетричних шифрів. Аналіз існуючих методів побудови вузлів нелінійної заміни викладено у [5]. В роботі [8] запропоновано метод генерації оптимальних підстановок.

Апробація результатів. Основні положення дисертаційної роботи та результати досліджень доповідалися і обговорювалися на конференціях: 3-й Міжнародний радіоелектронний форум «Прикладна радіоелектроніка. Стан та перспективи розвитку» (Харків, 2008р.); 14-й Міжнародний молодіжний форум «Радіоелектроніка та молодь в 21 столітті» (Харків, 2010р.); 15-й Міжнародний молодіжний форум «Радіоелектроніка та молодь в 21 столітті» (Харків, 2011р.); XII Міжнародна науково-практична конференція «Безпека інформації в інформаційно-телекомунікаційних системах» (Київ, 2009р.); XIII Міжнародна науково-практична конференція «Безпека інформації в інформаційно-телекомунікаційних системах» (Київ, 2010р.) – три доповіді; XV Міжнародна науково-практична конференція «Безпека інформації в інформаційно-телекомунікаційних системах» (Київ, 2012р.); I Науково-технічна конференція з міжнародною участю «Комп'ютерне моделювання в наукомістких технологіях» (Харків, 2010р.); Міжнародна науково-технічна конференція «Гарантовані системи, сервіси та технології» (Кіровоград, 2010р.); Міжнародна науково-практична конференція «Перспективи розвитку інформаційних та транспортно-митних технологій у митній справі, зовнішньоекономічній діяльності та

управлінні організаціями» (Дніпропетровськ, 2011р.); Proceedings International Conference SAIT 2011 (Київ, 2011р.); VI Міжнародна науково-практична конференція "Наука і соціальні проблеми суспільства: інформатизація та інформаційні технології". (Харків, 2011р.); XV Науково-практична конференція «РусКрипто'2013» (Москва, 2013р.); CTCrypt 2013 (Єкатеринбург 2013р.) – три доповіді; Arithmetic of Finite Fields. 4th International Workshop (Бохум, 2012р.).

Публікації. Результати дисертаційної роботи викладені у 10 статтях, що опубліковані у наукових фахових виданнях України, та у 3 закордонних виданнях, що входять в науково-метричні бази, і 18 матеріалах і тезах наукових конференцій.

Структура та об’єм дисертації. Робота складається зі вступу, п'яти розділів та двох додатків. Загальний обсяг дисертації складає 190 сторінок, з яких основний зміст викладено на 144 сторінках друкованого тексту. Робота містить 21 рисунок та 33 таблиці. Список використаних джерел складається з 222 найменувань на 27 сторінках.

ОСНОВНИЙ ЗМІСТ РОБОТИ

У **вступі** до дисертації обґрунтовано актуальність теми досліджень, сформульовані мета та задачі, наведено стислий переказ отриманих результатів, відзначено їх наукову новизну та практичне значення.

У **першому розділі** наводяться сучасні тенденцій та аналітичне дослідження поточного стану та розвитку симетричних криптопримітивів.

По-перше, представляється загальна характеристика конкурсів по створенню алгоритмів симетричного шифрування. Причинами цього стали успішні теоретичні атаки на шифр Data Encryption Standard (DES) і недоліки у БСШ, який був поданий на заміну цьому стандарту. Внаслідок чого, у Сполучених Штатах Америки (США) в 1997 був організований конкурс Advanced Encryption Standard (AES), спрямований на вибір стандарту блокового симетричного шифрування нового покоління. Після декількох років досліджень був прийнятий стандарт FIPS-197, що базується на алгоритмі Rijndael. Успіх конкурсу взяли до уваги і інші країни. Так, через кілька років, аналогічні конкурси організували Європейський союз (NESSIE і eSTREAM) та Японія (CRYPTEC).

В Україні рекомендований до використання блоковий симетричний шифр ДСТУ ГОСТ 28147:2009 був прийнятий в 1989 році і вже поступається як по швидкодії, так і по криптографічним показниками багатьом сучасним шифрам, у тому числі і AES. Тому, з метою пошуку альтернативи чинному стандарту БСШ, в Україні було оголошено відкритий конкурс на розробку алгоритму нового покоління. Високий рівень стійкості, відносно відомих видів криптоаналітичних атак, і швидкодія, сумірна з існуючими алгоритмами, були основними вимогами до перспективного шифру. У 2009 році був відзначений алгоритм шифрування

«Калина», основною особливістю якого стали нелінійне відображення байтів та схема розгортання ключа (СРК). Варто відзначити, що Росія не пішла шляхом відкритого конкурсу, а використала в якості прототипу ґеш-функцію «Стрибог», яка є єдиним відомим варіантом проекту державного стандарту криптографічні ґеш-функції ГОСТ Р 34.11-2012 .

По-друге, розглядаються узагальнені моделі симетричних криптоалгоритмів. Зокрема, описуються загальні структури блокового симетричного шифру, потокового шифру і ґеш-функції. Наводиться узагальнена модель ітеративного БСШ, яка складається з циклової функції, початкового і кінцевого забілювання, процедури змішування ключа і схеми розгортання ключа. Подібне узагальнення наводиться і для ґеш-функцій, спираючись на алгоритми, подані на конкурс SHA-3.

Далі робота фокусується на методах криптоаналізу блокових симетричних шифрів, включаючи диференційний, лінійний, алгебраїчний, та їх зв'язок з математичними моделями. Додатково відзначається, що в 2011 році вперше були представлені методи аналізу повноциклових версій шифрів ГОСТ 28147 та AES, заснованих на комбінуванні декількох типів атак, серед яких найефективнішою є атака із застосуванням повного дводольного графу (biclique) на мережи замін-перестановок (SPN).

Наприкінці даного розділу вводяться визначення та позначення, які використовуються протягом дисертації, включаючи розширено афінну (РА), частково розширено афінну (ЧРА) і Карле-Шарпен-Зінов'єв (КШЗ) еквівалентності; наводяться теоретичні аспекти подання та побудови векторних булевих функцій, а також пов'язані з ними актуальні криптографічні властивості для симетричних криптоалгоритмів. Застосування математичного апарату векторних булевих функцій дозволяє спростити опис основних елементів симетричних методів шифрування, що дає можливість узагальнити множину критеріїв, у тому числі й тих, що застосовуються до нелінійних вузлів заміни.

На підставі проведених досліджень наприкінці розділу робиться висновок про те, що застосування теоретичного підходу не завжди може задовольнити практичні потреби, зокрема по генерації S-блоків із заданими неграничними показниками. Незважаючи на велику кількість існуючих рішень в області симетричної криптографії, досі залишається актуальним питання щодо знаходження підстановок, застосування яких в алгоритмах шифрування забезпечує захист від існуючих і перспективних видів атак.

У другому розділі описуються підходи до оцінки нелінійних вузлів заміни на основі критеріїв. У першій частині проводиться аналіз відомих характеристик, критеріїв і показників, та викладаються вимоги до блокових симетричних шифрів, включаючи DES, Rijndael, ГОСТ 28147-89, «Калина» та загальні вимоги

до нелінійних блоків потокових шифрів. Відзначається, що підстановки більшості сучасних симетричних криптоалгоритмів не задовольняють більшості критеріїв. У багатьох випадках, це пов'язано з тим, що багато критеріїв, представлених для захисту поточних шифрів (де використовуються переважно булеви функції) від різних типів атак, були безпосередньо перетворені в критерії для векторних булевих функцій. Це призвело до того, що безліч критеріїв для нелінійних вузлів заміни, які використовуються в БСШ, не базуються на реальних атаках. Іншими словами, методику проведення атаки, на якій було засновано даний критерій, не можливо застосувати для БСШ. Для прикладу можна навести S-блок шифру AES, який не задовольняє ряду розглянутих критеріїв включаючи критерій розповсюдження та кореляційний імунітет.

Далі відмічається, що на сьогоднішній день існує два підходи до генерації вузлів нелінійної заміни: орієнтування на граничні показники для захисту від певних атак; захист від усіх відомих на сьогоднішній день атак. З представлених алгоритмів на національний конкурс перший метод був застасований в шифрах ADE і Лабіринт. Процедура генерації нелінійних вузлів заміни ідентична Rijndael, за винятком використання інших афінних перетворень. Однак, останнім часом другий метод застосовується все частіше. Багато криптопримітивів (наприклад, «Мухомор», «Калина», «Стрибог») переважно турбуються про захист від усіх існуючих атак, чим про досягнення граничних показників.

Значна частина розділу присвячена обґрунтуванню критеріїв відбору таблиць підстановок для блокових симетричних алгоритмів. Виходячи з відомих криптографічних атак відмічається, що до обов'язкових критеріїв відносяться: δ-рівномірність, нелінійність і мінімальний степінь. Також обґрунтувується необхідність в розширеному критерії алгебраїчного імунітету, відсутності фіксованих точок і приналежності S-блоків до різних класів еквівалентності. Останній необхідно враховувати лише за наявності декількох підстановок в нелінійному шарі.

У цьому ж розділі вводиться загальне визначення оптимальної підстановки. У дисертаційній роботі під оптимальним нелінійним відображенням розуміється перестановка з максимальними показниками мінімального степіня і алгебраїчного імунітету; з граничними показниками (при фіксованих попередніх) δ-рівномірності і нелінійності; відсутністю фіксованих точок (циклів довжиною 1). Таким чином, для $n = 8$ оптимальна підстановка є бієктивне відображення без фіксованих точок та має мінімальний степінь 7, алгебраїчний імунітет 3, δ-рівномірність рівну 8 або менше та нелінійність не менш 104.

У кінці розділу, описується запропонований поліноміальний метод перетворення лінійних функцій, заданих над полем, у матричне подання. Наводиться декілька методів перевірки векторних булевих функцій на ЧРА-

еквівалентність, складність яких, за певних умов, є поліноміальною. Порівняння складностей (у логарифмічному вигляді з основою 2) запропонованих методів з відомими (виділені) для деяких значень n представлено у таблиці 1, де СПП – складність повного перебору, а СВМ – складність вдосконалених методів.

Таблиця 1

Порівняння складностей вирішення проблеми ЧРА-еквівалентності для декількох значень n

ЧРА еквівалентность	$n=8$		$n=10$		$n=12$	
	СПП	СВМ	СПП	СВМ	СПП	СВМ
$F(x)=M_1\cdot G(M_2\cdot x)$	125	14	197	17	285	20
$F(x)=M_1\cdot G(M_2\cdot x\oplus V_2)\oplus V_1$	141	19	217	24	309	28
$F(x)=M_1\cdot G(x\oplus V_2)\oplus V_1$	79	17	119	21	167	25
$F(x)=M_1\cdot G(x\oplus V_2)\oplus V_1$		27		34		40
$F(x)=G(M_2\cdot x\oplus V_2)\oplus V_1$		14		17		20
$F(x)=G(x\oplus V_2)\oplus M_3\cdot x\oplus V_1$	80	11	120	14	168	16
$F(x)=M_1\cdot G(x\oplus V_2)\oplus M_3\cdot x\oplus V_1$	143	17	219	21	311	25
$F(x)=M_1\cdot G(x\oplus V_2)\oplus M_3\cdot x\oplus V_1$		27		34		40

Крім того, модифікація методу перетворення лінійних функцій дозволяє відновлювати високорівневі конструкції симетричних криптоперетворень, заданих в алгоритмічному вигляді (наприклад, ґеш-функції ГОСТ Р 34.11-2012). Таким чином, запропоновані методи не тільки є додатковими інструментами для розвитку теорії векторних булевих функцій, але і дозволяють вирішувати практичні задачі.

Результати цього напрямку досліджень свідчать про те, що ідеальних підстановок, найімовірніше, не існує. Тому, вводиться термін «оптимальна підстановка», критерії якої визначаються для конкретного алгоритму шифрування (або групи алгоритмів) і є оптимальними з точки зору захисту від існуючих видів атак.

У третьому розділі розглядається кілька найбільш ефективних із відомих методів генерації підстановок та можливі шляхи їх вдосконалення. Спочатку увага зосереджується на генерації випадкових підстановок із заданими характеристиками. Описуються основні переваги та недоліки даного методу, а також обґрунтовуються часові обмеження при практичній реалізації за допомогою розподілених обчислень для найбільш розповсюдженого значення $n=8$. Зокрема зазначається, що навіть за 22 роки роботи одного однопроцесорного (з одним ядром) комп'ютера, перестановок краще, ніж з характеристикою нелінійність 100, мінімальний степінь 7, δ-рівномірність 8 і алгебраїчний імунітет 3 не було знайдено.

Далі, розглядається другий підхід – генерація підстановок із заданими показниками. Зазвичай підстановки, сформовані за допомогою цього методу, мають граничні (максимальні або мінімальні залежить від властивості) показники. Наводиться опис відомих класів степеневих функцій із заданими криптографічними параметрами. Більше того, зазначається, що існують «майже зовсім нелінійні» функції для парних значень n, наприклад над полем $GF(2^6)$. Однак, питання про існування таких функція для $n \geq 8$ залишається відкритим.

Також відзначаються переваги комбінованих методів на прикладі методу градієнтного спуску для булевих функцій. Проте, використовувати безпосередньо даний метод для генерації векторних функцій неможливо. Відзначається, що ймовірність генерації перестановок методом «набору булевих функцій» для $n \geq 8$ прямує до нуля.

Таким чином, більшість сучасних методів генерації підстановок засновані на теоретичному підході, де за основу беруться векторні булеві функції з теоретично доведеними властивостями. Однак, у більшості випадків розглядається лише одна або дві з них, в той час як на практиці необхідно враховувати 4 і більше. Внаслідок чого, все частіше застосовуються модифіковані версії евристичних методів з використанням алгебраїчних структур. Застосування такого підходу дає можливість значно зменшити складність практичного пошуку підстановок з високими показниками криптографічної стійкості.

В четвертому розділі описуються запропоновані методи генерації нелінійних вузлів заміни для діючого і перспективних блокових симетричних шифрів.

Спочатку увага зосереджується на методі генерації довгострокових ключових елементів для шифру ДСТУ ГОСТ 28147:2009, що заснований на відомих класах РА-еквівалентностей векторних булевих функцій. Відзначається, що для $n = 4$ всього існує 16 різних перестановочних векторних булевих функцій, які не є еквівалентними, 8 з яких 4-рівномірні, з нелінійністю 4 і мінімальним степенем 3. Проведений аналіз показав, що ці функції належать лише 4 різним КШЗ-еквівалентностим класам. Інакше кажучи, максимум 4 підстановки довільного ДКЕ з вищезазначеними показниками будуть КШЗ-нееквівалентні.

Суть методу генерації полягає в наступному: кожному з 8 S-блоків ДКЕ (K_1, …, K_8) ставиться у відповідність одна з 8 РА-нееквівалентних векторних булевих функцій; далі послідовно застосовуються різні афінно-еквівалентні перетворення до тих пір, поки нелінійні вузли заміни не міститимуть фіксованих точок. При цьому, кількість ДКЕ, які можна отримати використовуючи даний

метод, не перевищує $\left(\prod_{i=1}^{4}(2^4-2^{i-1})\right)^2 \cdot 2^8 \cdot 8! \approx 2^{51}$. Приклад довгострокового ключового елементу, згенерованого за допомогою запропонованого методу, представлено у таблиці 2.

Таблиця 2

Приклад довгострокового ключового елемента для шифру ДСТУ ГОСТ 28147:2009, згенерованого за допомогою запропонованого методу

	Ключ
K_1	[5, 11, 13, 10, 8, 4, 1, 0, 6, 12, 3, 15, 2, 9, 7, 14]
K_2	[7, 8, 12, 10, 2, 1, 15, 14, 11, 13, 5, 9, 0, 3, 6, 4]
K_3	[15, 14, 7, 5, 3, 13, 9, 2, 10, 6, 11, 1, 8, 0, 12, 4]
K_4	[15, 8, 9, 14, 1, 4, 13, 11, 3, 5, 6, 12, 0, 2, 7, 10]
K_5	[5, 10, 6, 15, 8, 4, 2, 3, 9, 7, 13, 0, 14, 1, 12, 11]
K_6	[7, 9, 12, 8, 10, 2, 13, 14, 0, 5, 4, 6, 3, 15, 1, 11]
K_7	[8, 14, 11, 5, 1, 4, 7, 6, 13, 2, 9, 15, 3, 10, 12, 0]
K_8	[13, 14, 6, 10, 2, 15, 0, 5, 12, 1, 11, 4, 9, 8, 3, 7]

Найбільш результативна частина розділу присвячена опису метода генерації нелінійних вузлів заміни для перспективних симетричних криптопримітивів з використанням ідей методу градієнтного спуску. Основна сутність полягає у наступному: на вхід приймається перестановочна векторна функція з мінімальним показником δ-рівномірності і кількість значень (NP), які необхідно поміняти місцями для досягнення оптимальних криптографічних показників. Для конкретного значення $n = 8$ була взята функція $F(x) = x^{-1}$ і $NP = 22$.

Після 1 години роботи кластера було згенеровано 1152 оптимальні підстановки. Звідки випливає, що якщо значення функції F змінюються випадковим чином, тоді час, необхідний на генерацію одного оптимального S-блоку на однопроцесорному комп'ютері (з одним ядром), дорівнює 3,5 годинам. Таким чином, результати експериментів підтвердили можливість генерації перестановок без фіксованих точок, з показниками:

– мінімальний степінь 7;

– алгебраїчний імунітет 3;

– δ-рівномірність 8;

– нелінійність 104.

Порівняльна характеристика одного із згенерованих S-блоків («О»),

підстановок блокових симетричних шифрів AES («А»), СТБ 34.101.31-2011 («С»), геш-функції ГОСТ Р 34.11-2012 («Г») і нелінійного вузла заміни «S0» алгоритму «Калина», наведена в таблиці 3, де $|AC|_{\max}$ – максимальне абсолютне значення спектру автокореляції, SSI – глобальна характеристика «сума квадратів», МТД – максимальне значення таблиці диференціалів, МТЛА – максимальне значення таблиці лінійної апроксимації, AI/KP/SP – алгебраїчний імунітет, кількість рівнянь та розрідженість системи відповідно.

Таблиця 3

Порівняння криптографічних характеристик згенерованої підстановки з відомими

Властивості	Показники				
	«А»	«С»	«Г»	«S0»	«О»
Компонентних булевих функцій					
Збалансованість	Так	Так	Так	Так	Так
Нелінійність	112	102	100	96	104
$\|AC\|_{\max}$	32	88	96	88	80
SSI	133120	232960	258688	244480	194944
Мінімальний степінь	7	6	7	7	7
Підстановки					
МТД	4	8	8	8	8
МТЛА	16	26	28	32	24
Циклічна структура	115:2, 11:27, 0:59, 1:81, 4:87	22:7, 1:35, 3:78, 0:136	21:13, 0:243	85:4, 4:24, 1:41, 2:78, 0:109	123:6, 6:7, 0:243
AI/KP/SP	2/39/0,687	3/441/0,823	3/441/0,824	3/441/0,826	3/441/0,828

У заключній частині розділу наводиться розрахунок складностей диференціальної («Диф.»), лінійної («Лін.») та алгебраїчної («XL») атак. На рисунку 1 зображені результати цього розрахунку, де вертикальною лінією позначена складність атаки повного перебору.

Для порівняння були взяті наступні підстановки: «S0» шифра «Калина», випадкова (В), отримана за допомогою виподкового метода генерації на кластері (ВМ), з алгебраїчним імунітетом 2 і 1 рівнянням (МКР), з алгебраїчним

імунітетом 2 і 13 рівняннями (НКР), блокового симметричного шифру AES та отриманого за допомогою запропонованого методу (О).

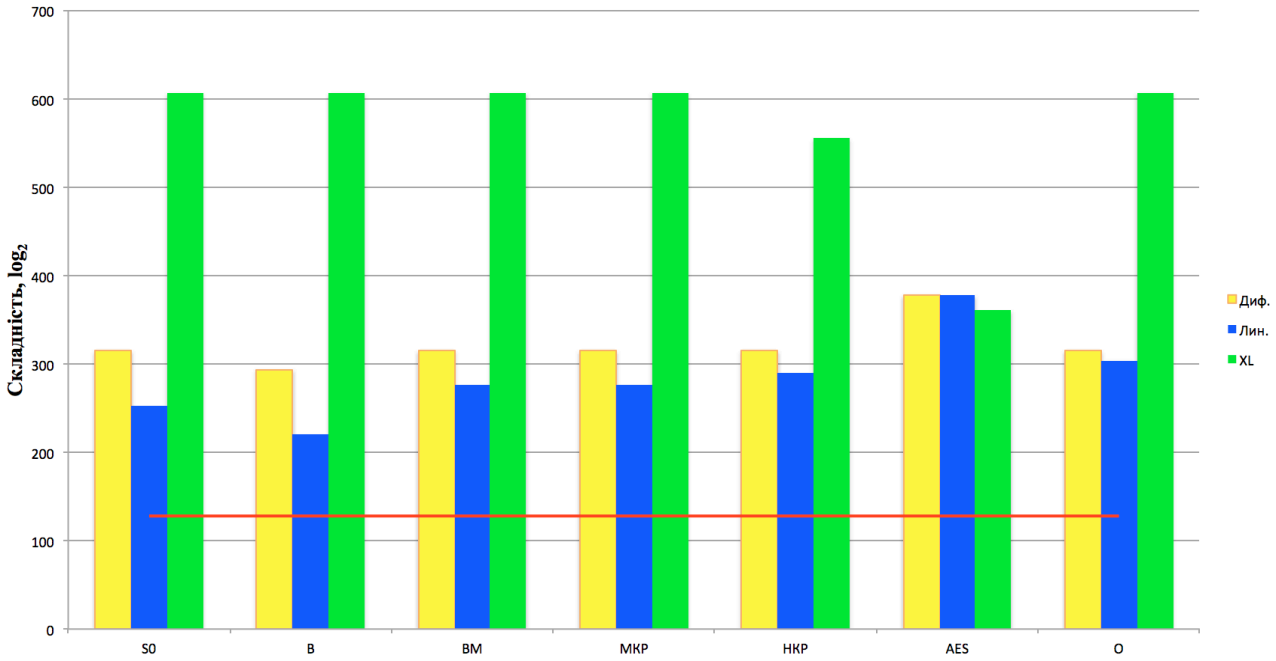

Рисунок 1 – Порівняння складностей атак на шифр «Калина 128/128» з різними нелінійними шарами.

На основі проведених досліджень робиться висновок про те, що нові вузли нелінійної заміни значно збільшують складність лінійного криптоаналізу, в порівнянні з S-блоком шифру «Калина», при цьому зберігають на високому рівні складності диференційної та алгебраїчної атак.

В п’ятому розділі досліджуються практичні аспекти реалізації теоретично отриманих результатів. Відмічається, що на сьогоднішній день не існує досить швидких і ефективних засобів знаходження характеристик для довільних підстановок. У зв'язку з чим, були покращені деякі алгоритми знаходження показників векторних булевих функцій. Наприклад, запропоновано метод знаходження алгебраїчного імунітету для довільних n і m без необхідності побудови системи рівнянь.

Далі наводяться особливості реалізації бібліотеки «Sbox», яка містить у собі найбільшу кількість відомих функцій для підрахунку показників S-блоків і декілька методів генерації підстановок, та «maxNL» – програми формування оптимальних підстановок для $n = 8$ використовуючи розподільні системи.

У кінці цього розділу відзначається, що доказ практичної складності генерації оптимальних підстановок можливий лише з використанням великих обчислювальних ресурсів, таких як кластер. У рамках дослідження методів швидкої генерації оптимальних підстановок було показано, що задача не є послідовною і, отже, може розглядатися як безліч дрібніших підзадач, які виконуються паралельно, що призводить до зменшення часу генерації S-блоків.

ВИСНОВКИ

Дослідження, проведені в роботі, вирішили одну з актуальних науково-практичних задач розробки теоретичної та практичної бази перевірки криптографічних властивостей і генерації нелінійних вузлів заміни для перспективних та існуючих засобів криптографічного захисту інформації з оптимальними показниками.

Результати проведеного аналізу показують, що основними критеріями для підстановок, які застосовуються у БСШ, є бієктивність, відсутність фіксованих точок, δ-рівномірність, мінімальний степінь, алгебраїчний імунітет і нелінійність. Додатковий аналіз шифрів, представлених на український конкурс, показав, що стійкість перетворення до алгебраїчної атаки залежить не тільки від алгебраїчного імунітету, але і від кількості рівнянь і розрідженості системи, яка описує нелінійний шар та весь криптоалгоритм. Таким чином, було запропоновано розширений критерій алгебраїчного імунітету, який дозволяє відбирати нелінійні вузли заміни, що забезпечують максимальний захист від алгебраїчної атаки.

Більш того, перспективні шифри вносять додаткові вимоги до S-блоків. Однією з таких вимог є приналежність всіх підстановок, що використовуються в одному алгоритмі шифрування, до різних класів еквівалентності. Відповідність даному критерію призводить до зменшення кількості ізоморфних представлень циклової функції і всього шифрувального перетворення, а отже і зменшує ймовірність знаходження слабкого подання. Внаслідок чого, виникає необхідність в знаходженні еквівалентних перетворень, які можуть бути використані для побудови ізоморфних відображень.

У ході роботи були запропоновані нові методи перевірки на еквівалентність двох нелінійних векторних булевих функцій. Ці методи засновані на методі перетворення лінійної функції, заданої над полем $GF(2^n)$, в матричне подання. Останній відрізняється від відомих поліноміальною складністю. Варіації даних методів дозволяють знаходити початкові подання високорівневих конструкцій, таких як ГОСТ Р 34.11-2012 .

Запропонований метод генерації нелінійних вузлів заміни для перспективних блокових симетричних шифрів засновано на комбінації теорії векторних булевих функцій і евристичному методі генерації S-блоків. Він дозволяє генерувати підстановки з поліпшеними показниками алгебраїчного імунітету і нелінійності при малих витратах ресурсів. Зокрема, застосування цього методу для національних симетричних алгоритмів шифрування при $n = 8$ дозволяє отримати перестановки з відсутністю фіксованих точок та показниками: δ-рівномірності 8, нелінійності 104, мінімального степеня 7 та алгебраїчного імунітету 3. З чого

слідує, що використання таких підстановок в відзначеному на національного конкурсу з вибору перспективного алгоритму шифрування «Калина» дозволяє збільшити нелінійність з 96 до 104 при збереженні всіх інших показників.

Застосування теорії векторних булевих функцій на практиці призводить до розробки методу, що скорочує час генерації довгострокових ключових елементів для шифру ДСТУ ГОСТ 28147:2009 до 1 с. Кожен такий ДКЕ складається з підстановок, що належать різним РА-еквівалентним класам.

Таким чином, головним науковим результатом роботи слід вважати розробку методів генерації оптимальних підстановок для перспективних симетричних криптоалгоритмів і довгострокових ключових елементів для блочного симетричного шифру ДСТУ ГОСТ 28147:2009 .

Основним практичним результатом є розробка програмного забезпечення для генерації та перевірки криптографічних властивостей довільних нелінійних вузлів заміни, яке дозволяє формувати базові параметри для схем симетричного криптоперетвореня, що призводить до можливості застосування розроблених методів для вирішення завдань забезпечення безпеки в інформаційно-телекомунікаційних системах України.

Показники підстановок, отримані з використанням розроблених методів, значно перевершують аналоги, які застосовуються в стандартах СТБ 34.101.31-2011, ГОСТ Р 34.11-2012 і відзначеному на національного конкурсу з вибору перспективного алгоритму шифрування «Калина».

СПИСОК ОПУБЛІКОВАНИХ ПРАЦЬ ЗА ТЕМОЮ ДИСЕРТАЦІЇ

1. Казимиров А. В. Построение переопределенной системы уравнений для описания алгоритма шифрования «Лабиринт» [Текст] / А. В. Казимиров, Р. В. Олейников // Прикладная радиоэлектроника. – 2009. – Т. 8, № 3. – С. 247–251.

2. Казимиров А. В. Сравнение функций разворачивания ключа симметричных блочных шифров [Текст] / А. В. Казимиров, Р. В. Олейников, // Защита информации : сб. науч. тр. / НАУ. – К., 2010. – Вып. 17. – С. 162–165.

3. Казимиров А. В. Алгебраические свойства схемы разворачивания ключей блочного симметричного шифра «Калина» [Текст] / А. В. Казимиров, Р. В. Олейников // Радіоелектронні і комп'ютерні системи. – Х. : ХАІ, 2010. – № 5 (46). – С. 61–66.

4. Олейников Р. В. Выбор S-блоков для симметричных криптографических алгоритмов на основе анализа алгебраических свойств [Текст] / Р. В. Олейников, А. В. Казимиров // Вісн. Харк. нац. ун-ту. Сер. Математичне моделювання. Інформаційні технології. Автоматизовані системи управління. – Х., 2010. – № 925. – С. 79–86.

5. Казимиров А. В. Использование векторных функций при генерации подстановок для симметричных криптографических преобразований [Текст] / А.

В. Казимиров, Р. В. Олейников // Системи обробки інформації. – 2012. – № 6 (104). – С. 97–102.

6. Казимиров А.В. Вариации на тему шифра Rijndael [Текст] / В. И. Долгов, И. В. Лисицкая, А. В. Казимиров // Прикладная радиоэлектроника. – 2010. – Т. 9, № 3. – С. 321–325.

7. Kazymyrov O. An Impact Of S-Box Boolean Function Properties To Strength Of Modern Symmetric Block Ciphers [Text] / R. Oliynykov, O. Kazymyrov // Радиотехника : Всеукр. межвед. науч.-техн. сб. – 2011. – Вып. 166 : Информационная безопасность. – С. 11–16.

8. Казимиров, А.В. Метод построения нелинейных узлов замены на основе градиентного спуска [Текст] / А. В. Казимиров, Р. В. Олейников // Радиотехника : Всеукр. межвед. науч.-техн. сб. – 2013. – Вып. 172 : Информационная безопасность. – С. 104–108.

9. Budaghyan L. Verification of restricted EA-equivalence for vectorial boolean functions [Text] / L. Budaghyan, O. Kazymyrov // Arithmetic of Finite Fields : 4th International Workshop, WAIFI 2012, Bochum, Germany, July 16–19, 2012. – Berlin ; Heidelberg : Springer, 2012. – P. 108–118. – (Lecture Notes in Computer Science ; vol. 7369).

10. Kazymyrov O. Extended Criterion for Absence of Fixed Points [Text] / O. Kazymyrov // Прикладная радиоэлектроника. – 2013. – Т. 12, № 2. – С. 209–214.

11. Kazymyrov O. State space cryptanalysis of the MICKEY cipher [Text] / T. Helleseth, C. J. A. Jansen, O. Kazymyrov, A. Kholosha // Information Theory and Applications Workshop (ITA), Feb. 10–15, 2013, San Diego, CA. – P. 1–10.

12. Казимиров А. В. Оценка количества допустимых внутренних состояний в поточном алгоритме Mickey [Текст] / А. В. Казимиров, Р. В. Олейников // Прикладная радиоэлектроника. – 2011. – Т. 10, № 2. – С. 112–115.

13. Казимиров А.В. Криптоанализ шифра Mickey на основе анализа внутренних состояний [Текст] / А. В. Казимиров, Р. В. Олейников // Радиотехника : Всеукр. межвед. науч.-техн. сб. – Х., 2012. – Вып. 171 : Информационная безопасность. – С. 24–28.

14. Kazymyrov O. Verification of Restricted EA-Equivalence for Vectorial Boolean Functions / O. Kazymyrov, L. Budaghyan // Arithmetic of finite Fields. 4th International Workshop, WAIFI 2012.

15. Казимиров А.В. Подход к криптоанализу блочного симметричного шифра «Лабиринт» [Текст] / А. В. Казимиров, Р. В. Олейников, А. Б. Небывайлов // Прикладная радиоэлектроника. Состояние и перспективы развития : материалы 3-го междунар. радиоэлектрон. форума (МРФ'2008), 22–24 окт. 2008 г. / АНПРЭ, ХНУРЭ. – Х. : ХНУРЭ, 2008. – Т. 5 : Междунар. конф. "Информационные компьютерные технологии и системы" (ИКТС–2008). – С. 262–263.

16. Казимиров А.В. Сравнение производительности функций разворачивания ключа блочных симметричных алгоритмов шифрования [Текст] / А. В. Казимиров // Радиоэлектроника и молодежь в XXI веке : материалы 14-го междунар. молодежного форума, 18–20 марта 2010 г. – Х. : ХНУРЭ, 2010. – Ч. 2. – С. 82.

17. Казимиров А.В. Подходы к формированию подстановок с оптимальными показателями [Текст] / А. В. Казимиров // Радиоэлектроника и молодежь в XXI веке : материалы XV Юбилейного Междунар. молодежного форума, 18–20 апр. 2011 г. – Х. : ХНУРЭ, 2011. – Т. 5. – С. 155.

18. Казимиров А. Алебраическая атака на модифицированный вариант алгоритма "Лабиринт" [Текст] / Р. Олейников, А. Казимиров // Безпека інформації в інформаційно-телекомунікаційних системах : матеріали XII Міжнар. наук.-практ. конф., 19–22 трав. 2009 р. – К., 2009. – С. 29.

19. Казимиров А. Выбор S-блоков для симметричных криптографических алгоритмов на основе анализа алгебраических свойств [Текст] / Р. Олейников, А. Казимиров // Компьютерное моделирование в наукоемких технологиях : материалы науч.-техн. конф. с междунар. участием (КМНТ–2010), 18–21 мая 2010 г. – Х. : Изд-во ХНУ. – Ч. 2. – С. 177–179.

20. Казимиров А.В. Анализ графа обратных состояний шифра Mickey [Текст] / А. В. Казимиров, Р. В. Олейников // Перспективи розвитку інформаційних та транспортно-митних технологій у митній справі, зовнішньоекономічній діяльності та управлінні організаціями : матеріали Міжнар. наук.-практ. конф., 2 груд. 2011 р. – Дніпропетровськ, 2011. – С. 211–212.

21. Казимиров А. Анализ усовершенствований шифра Rijndael [Текст] / И. Лисицкая, А. Казимиров, Е. Мельничук и др. // Безопасность информации в информационно-телекомуникационных системах : тез. докл. XIII Междунар. науч.-практ. конф., 18–21 мая 2010 г. – К., 2010. – С. 42.

22. Казимиров А. Сравнение функций разворачивания ключа симметричных блочных шифров [Текст] / Р. Олейников, А. Казимиров // Захист інформації в інформаційно-комунікаційних системах : матеріали наук.-практ. конф., 24–26 трав. 2010 р. – К., 2010. – С. 138.

23. Казимиров А.В. Алгебраические свойства схемы разворачивания ключей блочного симметричного шифра Калина [Текст] / Р. В. Олейников, А. В. Казимиров // Гарантоздатні системи, сервіси та технології (DESSERT 2010) : матеріали 5-ї Міжнар. наук.-техн. конф. – Харків ; Полтава ; Кіровоград, 2010.

24. Казимиров А. Выбор узлов нелинейного преобразования на основе анализа алгебраических свойств подстановок [Текст] / И. Горбенко, Р. Олейников, А. Казимиров // Безопасность информации в информационно-

телекомуникационных системах : тез. докл. XIII Междунар. науч.-практ. конф., 18–21 мая 2010 г. – К., 2010. – С. 36.

25. Казимиров А.В. Об участии S-блоков в формировании максимальных значений дифференциальных вероятностей блочных симметричных шифров [Текст] / И. В. Лисицкая, А. В. Казимиров // Proceedings International Conference SAIT 2011, May 23–28, 2011, Ukraine. – Kyiv, 2011 – P. 460.

26. Казимиров А.В. Восстановление ключей шифра ГОСТ 28147 на основе слайд атаки [Текст] / А. В. Казимиров // Наука и социальные проблемы общества: информатизация и информационные технологии : тез. докл. VI Междунар. науч.-практ. конф., 24–25 мая 2011 г. – Х., 2011. – С. 272–273.

27. Казимиров А.В. Генерация подстановок на основе векторных функций [Текст] / А. В. Казимиров // Безопасность информации в информационно-телекомуникационных системах : тез. докл. XV Междунар. науч.-практ. конф., 22–25 мая 2013 г. – К., 2013.

28. Казимиров А.В. О создании эффективных программных реализаций отечественных криптографических стандартов [Электронный ресурс] / А. В. Казимиров, С. В. Смышляев, С. Е. Леонтьев, В. О. Попов // РусКрипто'2013 : материалы XV науч.-практ. конф., 27–30 марта 2013 г., Россия, Моск. обл. – Режим доступа : http://www.ruscrypto.ru/accotiation/archive/rc2013/.

29. Kazymyrov O. A Method For Generation Of High-Nonlinear S-Boxes Based On Gradient Descent [Text] / V. Kazymyrova, O. Kazymyrov, R. Oliynykov // Second workshop on Current Trends in Cryptology (CTCrypt 2013), Ekaterenburg, Russian, June 23–24, 2013. – Ekaterenburg, 2013. – P. 107–115.

30. Kazymyrov O. Algebraic Aspects of the Russian Hash Standard GOST R 34.11–2012 [Text] / V. Kazymyrova, O. Kazymyrov // Second workshop on Current Trends in Cryptology (CTCrypt 2013), Ekaterenburg, Russian, June 23–24, 2013. – Ekaterenburg, 2013. – P. 160–176.

31. Kazymyrov O. Extended Criterion for Absence of Fixed Points [Text] / V. Kazymyrova, O. Kazymyrov // Second workshop on Current Trends in Cryptology (CTCrypt 2013), Ekaterenburg, Russian, June 23–24, 2013. – Ekaterenburg, 2013. – P. 177–191.

АНОТАЦІЯ

Казимиров О.В. Методи та засоби генерації нелінійних вузлів заміни для симетричних криптоалгоритмів – Рукопис.

Дисертація на здобуття наукового ступеня кандидата технічних наук по спеціальності 05.13.21 – системи захисту інформації. Харківський національний університет радіоелектроніки, Харків, 2014.

Дисертація присвячена розробці методів побудови вузлів нелінійної заміни для симетричних криптопримітивів з оптимальними криптографічними

показниками стійкості.

У роботі пропонуються декілька методів формування підстановок як для відомих, так і для перспективних симетричних криптоалгоритмів. Запропоновані методи засновані на критеріальному підході з використанням теорії векторних булевих функцій. Виходячи з алгебраїчного криптоанализа шифрів, представлених на український конкурс, був розширений критерій алгебраїчного імунітету, а також доданий критерій приналежності кількох підстановок до різних класів еквівалентності.

Показується, що застосування підстановок, згенерованих на основі запропонованих методів у відзначеному алгоритмі блокового симетричного шифру «Калина», що був представлен на національний конкурс з вибору перспективного алгоритму шифрування, дозволяє збільшити нелінійність з 96 до 104 при збереженні на високому рівні всіх інших показників.

Запропоновано конкретні підстановочні конструкції для застосування в симетричних криптоалгоритмах. Результати практичного застосування запропонованих методів з використанням кластера підтверджують ефективність генерації підстановок нового типу.

Ключові слова: вузел нелінійної заміни, підстановка, критерій, метод генерації, S-блок, криптоанализ, алгебраїчний імунітет.

АННОТАЦИЯ

Казимиров А.В. Методы и способы генерации нелинейных узлов замены для симметричных криптоалгоритмов – Рукопись.

Диссертация на соискание ученой степени кандидата технических наук по специальности 05.13.21 – системы защиты информации. Харковский национальный университет радиоэлектроники, Харков, 2014.

Дисертация посвящена разработке методов построения узлов нелинейной замены для симметричных криптопримитивов с оптимальными криптографическими показателями стойкости.

В работе предлагаются несколько методов формирования подстановок как для известных, так и для перспективных симметричных криптоалгоритмов. Предложенные методы основаны на критериальном подходе с использованием теории векторных булевых функций. Исходя из алгебраического криптоанализа шифров, представленных на украинский конкурс, был расширен критерий алгебраического иммунитета, а также добавлен критерий принадлежности нескольких подстановок к различным классам эквивалентности.

Показывается, что применение подстановок, сгенерированных на основе предложенных методов в отмеченном алгоритме блочного симметричного шифра «Калина», представленного на национальный конкурс по выбору перспективного алгоритма шифрования, позволяет увеличить нелинейность с 96

до 104 при сохранении на высоком уровне всех остальных показателей.

Предложены конкретные подстановочные конструкции для применения в симметричных криптоалгоритмах. Результаты практического применения предложенных методов с использованием кластера подтверждают эффективность генерации подстановок нового типа.

Ключевые слова: узел нелинейной замены, подстановка, критерий, метод генерации, S-блок, криптоанализ, алгебраический иммунитет.

ABSTRACT

Kazymyrov O.V. Methods and Techniques of Generation of Nonlinear Substitutions for Symmetric Encryption Algorithms – Manuscript.

The thesis for the scholarly degree of candidate of technical sciences, speciality 05.13.21 – Information security systems. – Kharkiv National University of Radioelectronics, Kharkiv, 2014.

New methods of constructing nonlinear substitutions, which are used in symmetric cryptographic primitives, with optimal properties are presented in the thesis.

Several methods of substitutions' generation for both existing and prospective symmetric cryptographic algorithms are proposed. These methods are based on the criteria approach using the theory of vectorial Boolean functions. Based on the algebraic cryptanalysis of ciphers submitted to the Ukrainian competition, the extended algebraic immunity criterion and the criterion for multiple substitutions belonging to different equivalence classes were taken into account in the search procedure.

Proposed methods allow to increase the non-linearity from 96 to 104. The usage of such substitutions in the block cipher «Kalyna», which was noted in the national competition for selection of prospective encryption algorithm, gives a high level resistance to all known attacks.

Efficiency of the new methods confirmed by practical search using a cluster system, which allows to find specific substitution constructions for symmetric cryptoalgorithms.

Keywords: nonlinear substutution, criteria, generation methods, S-box, cryptanalysis, algebraic immunity.