Схема побудови нелінійних полікриптосистемних криптографічних протоколів

Ігор Муляр[1], Володимир Анікін[2]

[1,2] Хмельницький національний університет
вул. Інститутська, 11, Хмельницький, Україна, 29000
[1] muliariv@khmnu.edu.ua, https://orcid.org/0000-0002-6659-605X
[2] anikin_volodymyr@khmnu.edu.ua, https://orcid.org/0000-0003-3395-2764

Received 13.05.2024, accepted 20.05.2024
https://doi.org/10.32347/uwt.2024.14.1101

Анотація. В роботі висвітлено способи побудови нелінійних систем шифрування та запропоновано схему побудови нелінійного полікриптосистемного криптографічного протоколу, що виконує шифрування блоків даних різними криптографічними системами у псевдовипадковій послідовності.

Використання запропонованої схеми дозволяє побудувати криптографічний протокол із використанням готових та перевірених систем шифрування, без внесення жодних змін до їх конструкції. Псевдовипадкове чергування криптосистем в процесі шифрування ґрунтується на криптостійкому алгоритмі розгортання гами, що підвищує нелінійність шифрування та покращує загальну криптографічну стійкість систем.

В статті було розглянуто будову криптосистем на основі нелінійних криптографічних примітивів, складено модель процесу розгортання модифікаторів нелінійних криптосистем та сформовано загальну схему будови нелінійних криптографічних протоколів із використанням однієї або кількох різних криптосистем, за умови їх відповідності зазначеним вимогам.

Перевагами запропонованої схеми є велика гнучкість та масштабованість, можливість застосування висвітленої концепції як на рівні криптографічних алгоритмів чи їх фрагментів, так і на рівні криптосистем та криптографічних протоколів.

Запропоновані рішення дозволяють просто та ефективно удосконалювати існуючі криптографічні системи або окремі їх алгоритми та є перспективними для подальших досліджень.

Ключові слова: криптографія, нелінійне шифрування, криптосистема, криптографічний протокол, захист інформації.

Муляр Ігор Володимирович
к.т.н., доц. ст. викладач
кафедри кібербезпеки

Анікін Володимир Андрійович
асистент кафедри
кібербезпеки

ВСТУП

Криптографічний захист є одним з найбільш поширених на сьогоднішній день напрямків кібербезпеки та інформаційної безпеки, що має широкий спектр практичного застосування. Методи криптографії використовуються для організації безпечної комунікації, захисту мережевих інформаційно-телекомунікаційних систем, та сховищ даних.

Дослідження, спрямовані на підвищення стійкості криптосистем та криптографічних протоколів є особливо актуальними в умовах зростаючої кіберзлочинності, активної розвідувальної та диверсійно-підривної діяльності різноманітних організацій, угруповань, спецслужб та навіть військових спецпідрозділів.

Сучасна криптографія постійно стикається із щоразу новими викликами, одним із основних серед яких є значний ріст рівня обчислювальної потужності комп'ютерної

техніки, який робить практично реальними атаки грубої сили та різноманітні криптоаналітичні статистичні дослідження. При цьому використані криптосистеми повинні працювати не лише в реальному часі, а й з певним запасом стійкості, оскільки шифровані повідомлення можуть логуватися, а компрометація криптосистеми може спричинити послідовний злам усієї історії повідомлень [1].

Одним із способів підвищення стійкості криптографічних систем є використання нелінійних перетворень у процесі шифрування. Нелінійні криптосистеми є більш стійкими перед криптоаналізом, оскільки можуть містити додатковий набір параметрів, окрім, безпосередньо, криптографічного ключа, що впливають на вихідний шифротекст, що в свою чергу повинно ускладнити статистичні дослідження як шифротексту, так і пар відкритих та шифрованих повідомлень.

Вказаний підхід може бути застосований як в рамках окремої криптосистеми, із внутрішніми розгалуженнями її алгоритму шифрування, так і при побудові криптографічних протоколів, на основі однієї системи шифрування, або певної їх множини. Перевагою побудови нелінійних криптографічних протоколів на основі множини криптосистем є можливість одразу використовувати готові та перевірені криптографічні системи, без необхідності їх модифікації та внесення будь-яких змін до їх алгоритмів чи логіки функціонування.

Побудова нелінійних криптопротоколів дасть можливість підвищити загальну криптографічну стійкість шифрованих даних із мінімальним додатковим обчислювальним навантаженням при виконанні шифрування та дешифрування інформації.

Таким чином, створення універсальної схеми побудови нелінійних полікриптосистемних криптографічних протоколів відкриє можливість їх імплементації для довільних криптосистем, без внесення жодних змін у їх конструкцію. При цьому вихідний шифротекст буде важче піддаватись криптографічному аналізу, ніж шифротекст будь-якої із складових криптографічних систем.

АНАЛІЗ ПРЕДМЕТНОЇ ОБЛАСТІ ТА АКТУАЛЬНИХ НАУКОВИХ ДОСЯГНЕНЬ

Криптографія – це наука, у галузі інформаційної безпеки, що вивчає методи захисту інформації шляхом їх шифро-перетворення, розшифрування, хешування, в агресивному середовищі із урахуванням можливості регулярних активних спроб порушення їх конфіденційності та цілісності. Сучасна криптографія знаходиться на перетині кількох фізико-математичних дисциплін, зокрема теорії ймовірності, комбінаторики та інших [1-3]. Вона також безпосередньо пов’язана із інформаційними технологіями.

Окрім забезпечення конфіденційності, криптографія також вирішує завдання аутентифікації, верифікації та контролю цілісності повідомлень. Криптографія також може використовуватись із елементами стеганографії.

Методи шифрування сучасної криптографії поділяються на два основних напрямки: симетричні та асиметричні [1, 3-5].

Асиметричні методи шифрування, також відомі як шифрування з відкритим ключем, передбачають використання двох різних криптографічних ключів для шифрування та розшифрування відповідно. Вони, як правило, базуються на односторонніх функціях, обчислення яких є достатньо простим, проте зворотне перетворення – практично вкрай складним та неефективним [1, 3].

Симетричні методи шифрування використовують один криптографічний ключ як для шифрування, так і для розшифрування даних. Стійкість даних алгоритмів, як правило, ґрунтується на:

- достатньо великому розмірі ключа, недоступному для перебору навіть із використанням навіть найкращих комп’ютеризованих рішень;
- складності математичних операцій шифрування та розшифрування, які повинні бути практично вкрай складними без знання ключа
- рівномірності шифрування, яка повинна забезпечувати максимально однакову ймовірність розподілу шифрованих даних задля ускладнення будь-яких

статистичних досліджень;
- нелінійності шифрування, що має усувати прямі залежності між ключем, вхідним та шифрованим повідомленням.

Переважна більшість сучасних алгоритмів шифрування є блочними, тобто такими, що оперують блоками даних фіксованого розміру і зміна бітів ключа повинна впливати на весь блок [1-3, 6-8].

Також термінуємо поняття криптосистеми та криптографічного протоколу. Найбільш поширеним є визначення криптосистеми як системи взаємопов'язаних алгоритмів, необхідних для реалізації криптографічного захисту інформації. Як правило криптосистема складається з алгоритму генерації ключа, який є особливо значущим в асиметричних криптосистемах, та алгоритмів шифрування та розшифрування [1, 3].

Криптографічний протокол – це набір правил та процедур криптографічного захисту. Він може включати елементи як симетричного так і асиметричного методів шифрування. Криптографічний протокол може включати в себе криптосистеми та додаткові криптографічні алгоритми [1, 3].

Важливим принципом сучасної криптографії є принцип Керкгоффса, нідерландського криптографа XIX сторіччя, згідно якого єдиним таємним параметром криптосистеми повинен бути її ключ, тоді як усі інші дані, зокрема структура алгоритмів шифрування та розшифрування, повинні бути публічними. При цьому криптосистема повинна унеможливлювати будь-які способи дешифровки повідомлень без знання криптографічного ключа, на чому і ґрунтується її стійкість. Дотримання цього принципу дозволяє зберігати конфіденційність захищеної інформації навіть якщо прототипи шифрувального обладнання, або програмного забезпечення потрапили до рук криптоаналітика та були досліджені методами реверсивної інженерії. Окрім цього публічність алгоритмів шифрування дозволяє проводити незалежні дослідження та оцінки зі сторони усіх зацікавлених спеціалістів, структур та організацій, що в свою чергу допомагає виявляти помилки, вразливості та прорахунки криптосистеми, усувати їх.

Серед основних типів атак на сучасні симетричні криптосистеми виділяють чотири категорії:
1. Атаки на шифрований текст.
2. Атаки на пари відкритих та шифрованих текстів.
3. Атаки на обраний відкритий текст.
4. Атаки на обраний шифрований текст.

Основними методами криптоаналізу є лінійний та диференційний криптоаналіз, а також частково методи класичного криптоаналізу. Лінійний криптоаналіз це метод криптоаналізу, що використовує лінійні наближення для побудови математичної моделі процесу шифрування криптосистеми та включає два кроки: виявлення відношень між відкритими та шифрованими даними, та їх використання. Диференційний криптоаналіз навпаки досліджує статистичні відмінності у парах відкритих та шифрованих текстів. Підвищення нелінійності шифрування підвищує стійкість перед лінійним та диференційним криптоаналізом [1-3, 6].

Таким чином, структура криптографічних систем, протоколів та алгоритмів повинна бути загальновідомою, та базуватися на математичній складності обчислень із рівномірним розподілом даних у шифрованому повідомленні. Підвищення криптографічної стійкості може досягатися за рахунок додаткової нелінійності криптографічних алгоритмів, що ускладнить лінійний та диференційний, криптоаналіз а також супутнього збільшення розміру криптографічного ключа, при чому дане збільшення відбуватиметься також із високою значимістю доданих бітів.

ПОБУДОВА КРИПТОСИСТЕМ НА ОСНОВІ НЕЛІНІЙНИХ КРИПТОГРАФІЧНИХ ПРИМІТИВІВ

Запропонована концепція нелінійних криптографічних систем передбачає введення додаткових параметрів в процес шифрування [6-8]. Відповідно до цього, введемо поняття лінійного та нелінійного криптографічних примітивів, що є складовою алгоритмів криптосистеми та наведені на Рис. 1.

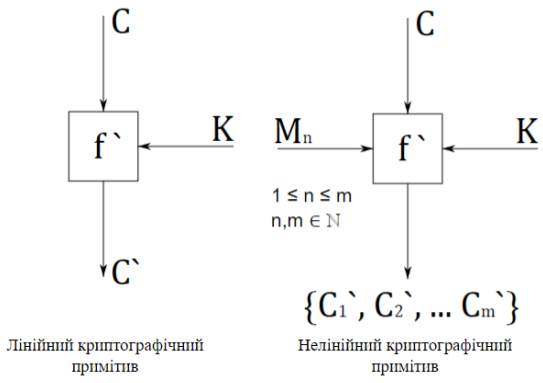

Рис. 1. Схеми криптографічних примітивів

Fig. 1. Schemes of cryptographic primitives

Нелінійна криптосистема, створена за даною концепцією може містити в собі деяку кількість типових криптоперетворень f, із множини можливих перетворень F. Усі криптоперетворення із множини F повинні приймати однакові за розміром ключі та блоки відкритих даних на вході та повертати однакові за розміром шифровані блоки даних, чим повинна забезпечуватись їх повна взаємозамінність. Кожен із них повинен зберігати рівномірність розподілу при шифруванні та відповідати звичайним критеріям стійкості. Шифрування вхідного блоку даних C використовуватиме додатковий параметр M – модифікатор, окрім криптографічного ключа K. Даний модифікатор буде відігравати роль перемикача, який обиратиме яке криптоперетворення із множини F буде застосоване. У результаті шифрування дана криптосистема утворюватиме множину шифрованих блоків $\bar{C}$, що включатиме варіанти шифротексту для різних модифікаторів шифрування:

$$F = \{f_1, f_2, \dots, f_n\} \quad n \in \mathbb{N}$$
$$\grave{C_M} = f_M(C, K) \quad f \in F$$
$$\overline{C} = \{\grave{C_1}, \grave{C_2}, \dots, \grave{C_n}\} \quad n \in \mathbb{N}$$

Фрагмент нелінійного алгоритму шифрування, згідно запропонованої концепції, представлятиме собою гілкове розгалуження із перемикачем, що за поточним модифікатором M визначатиме яка саме гілка спрацює. Дана схема зображена на Рис. 2.

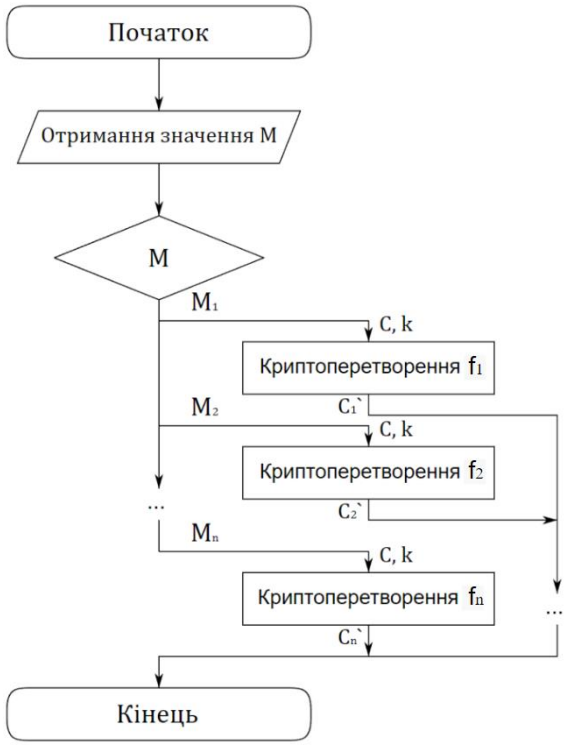

Рис. 2. Фрагмент нелінійного алгоритму шифрування

Fig. 2. A fragment of a non-linear encryption algorithm

Згідно принципу Керкгоффса, жоден із наведених елементів не є таємним, допускається що криптоаналітик досконало знає структуру та усі особливості криптосистеми, єдиним невідомим для нього є криптографічний ключ. Підвищення криптографічної стійкості відбувається за рахунок того що, при m криптографічних перетворень у складі нелінійної криптосистеми, утворюється m варіантів шифрованих блоків, для одного і того ж вхідного блоку даних, серед яких обирається один [7-8].

Важливу роль в цій схемі також відіграє модифікатор. Теоретично, він може бути публічним, генеруватися випадково та передаватися разом із повідомленням, або ж братися з якогось публічного набору даних. Навіть в такому випадку це позитивно вплине на криптографічну стійкість шифрування, оскільки суттєво збільшить необхідну кількість зашифрованих повідомлень для успішної реалізації лінійного криптоаналізу. Максимально дана кількість шифротекстів може бути

збільшена в m разів, відносно початкової, проте на практиці ця кількість завжди буде меншою.

Проте найкращих результатів можливо досягнути якщо модифікатори будуть не доступні для аналітика. Це можна зробити кількома способами, зокрема:

1. Передавати модифікатори окремо по безпечному каналу зв'язку. Це є найбільш безпечний спосіб, проте найменш практичний. Як один із варіантів даного способу – набір модифікаторів може бути переданий завчасно, проте навіть у такому випадку доцільність даного способу сумнівна.
2. Передавати модифікатори разом з повідомленням у шифрованому вигляді. Даний спосіб може бути використаний на практиці, проте серед його основних недоліків – збільшення розміру шифротексту, відносно вхідних даних.
3. Генерувати модифікатори на основі деякого алгоритму розгортання гами, сідом якого виступає ключ, або окремий його параметр.

Останній варіант є найбільш оптимальним у більшості випадків, оскільки він не розширяє шифровані дані, не дає аналітику жодної додаткової інформації, та розгортається на основі криптографічного ключа, що повністю відповідає принципу Керкгоффса.

МОДЕЛЬ ПРОЦЕСУ РОЗГОРТАННЯ МОДИФІКАТОРІВ НЕЛІНІЙНИХ КРИПТОСИСТЕМ

Розглянемо детальніше процес розгортання модифікаторів. Для виконання цього завдання можна застосувати практично будь-який алгоритм розгортання гами, такий як RC4, Salsa20 тощо. При цьому серед вимог до процесу розгортання модифікаторів можна виділити:

1. Розгортання повинне бути одностороннім, тобто, відновивши послідовність модифікаторів аналітик не повинен мати можливість отримати початковій сід.
2. Повторні розгортання повинні давати ідентичний результати до попередніх.
3. Розгортання повинно бути криптографічно стійким, компрометація одного чи кількох модифікаторів на повинна давати аналітику можливості для знаходження наступних, або попередніх.
4. Розподіл модифікаторів повинен бути рівномірним по всій їх множині.

Окрім цього, рекомендується щоб процес розгортання також деяким чином залежав від самого повідомлення, оскільки в інакшому випадку, коли розгортання відбуватиметься виключно на основі криптографічного ключа або якогось статичного параметру, послідовність модифікаторів для усіх повідомлень, зашифрованих одним ключем, буде однаковою. Це дасть можливість аналітику однозначно стверджувати що n-ний блок кожного повідомлення був гарантовано зашифрований із однаковим модифікатором та дасть можливість згрупувати ці блоки між собою для подальшого дослідження. Для усунення даної вразливості достатньо передавати разом із повідомленням деякий вектор, який не є секретним та сам по собі не представлятиме жодної значимості, проте задаватиме різні «траєкторії» шифрування для кожного повідомлення. В якості цього вектору може передаватись час шифрування, або деякий ідентифікатор повідомлення, чи просто якесь випадкове значення. Не рекомендується повторно використовувати однакові вектори для різних повідомлень.

На основі перелічених рекомендацій, побудуємо модель процесу розгортання модифікаторів нелінійної криптосистеми. Графічне зображення даної моделі продемонстровано на Рис. 3.

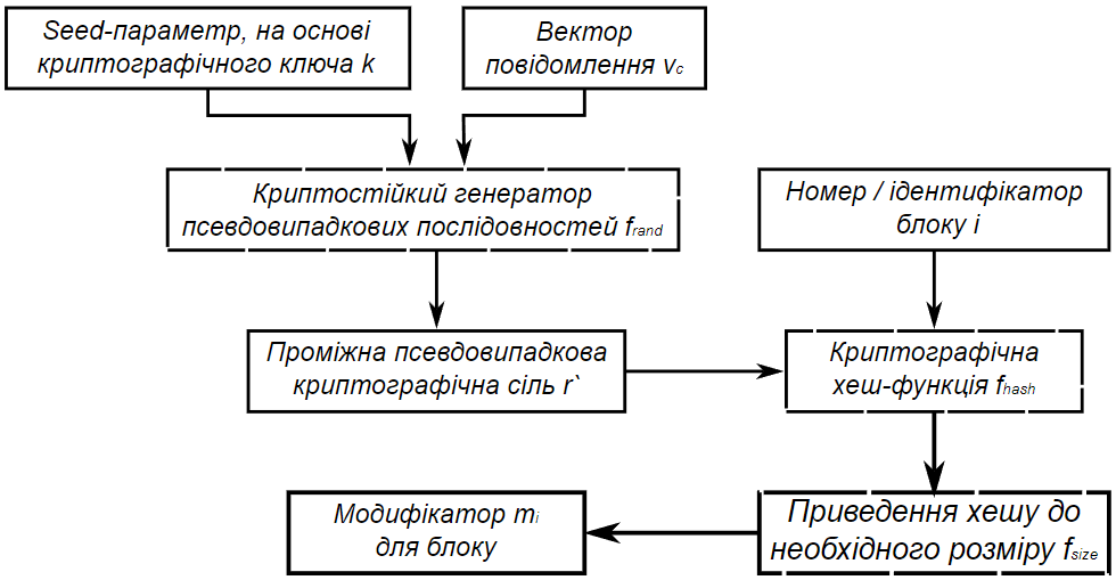

Рис. 3. Модель розгортання модифікатора нелінійної криптосистеми

Fig. 3. The model of the deployment of the modifier of the nonlinear cryptosystem

Генератор гами (псевдовипадкових послідовностей) f_{rand} може використовуватись довільний. В прототипних версіях було використано власний генератор, на основі алгоритму AES CTR DRBG. В цілому для дотримання вимоги №2, вказаної раніше, краще використовувати алгоритми генерації гами на основі хеш-функцій.

У якості початкового сід-параметра можна використати основний криптографічний ключ. Якщо розміру ключа не достатньо, його можна збільшити згідно вимог алгоритму генерації гами. Також можна взагалі розділити ці елементи, утворивши криптографічний ключ з двох параметрів: ключа криптоперетворення та окремого сід-параметра. Обидва варіанта дають можливість нелінійно збільшити розмір ключа, що також підвищує стійкість перед атаками грубої сили, проте якщо розмір ключа має критичне значення – можна залишити його без змін, адаптувавши генератор гами під нього.

Модифікатор можна утворювати напряму із утвореної гами, проте для зменшення навантаження на програмно-апаратні рішення, створені за даною схемою, рекомендується додати механізм, який дозволив б отримувати модифікатори для конкретного блоку на довільній позиції шифротексту, без необхідності обчислювати усі попередні. З цією метою у наведеній схемі додано проміжний модуль f_{hash}, який утворює модифікатор із згенерованої гами, яка виступає в ролі проміжної криптографічної солі $\grave{r}$, та ідентифікатора блоку. Існують алгоритми генерації, що мають подібну можливість конструктивно, при використанні їх, даний крок може бути пропущено.

Фінальне приведення f_{size} повинно перетворювати результат роботи генератора до, безпосередньо, модифікатора із множини можливих, обов'язково зберігаючи при цьому рівномірність розподілу. В найпростішому варіанті для досягнення цього може бути використане звичайне ділення за модулем m, де m – це кількість можливих модифікаторів. Даний спосіб можливий для використання тільки за умови що генератор гами також на виході дає значення із рівномірним розподілом. Утворення модифікатора m для i-того блоку, згідно запропонованої схеми, можна записати формулою:

$$r` = f_{rand}(k, v_c)$$
$$m_i = f_{size}\left(f_{hash}(r`, i)\right),\ \ i \in \mathbb{N}$$

Модель процесу шифрування нелінійної криптосистеми, із процесом розгортання модифікатора, зображена на Рис. 4.

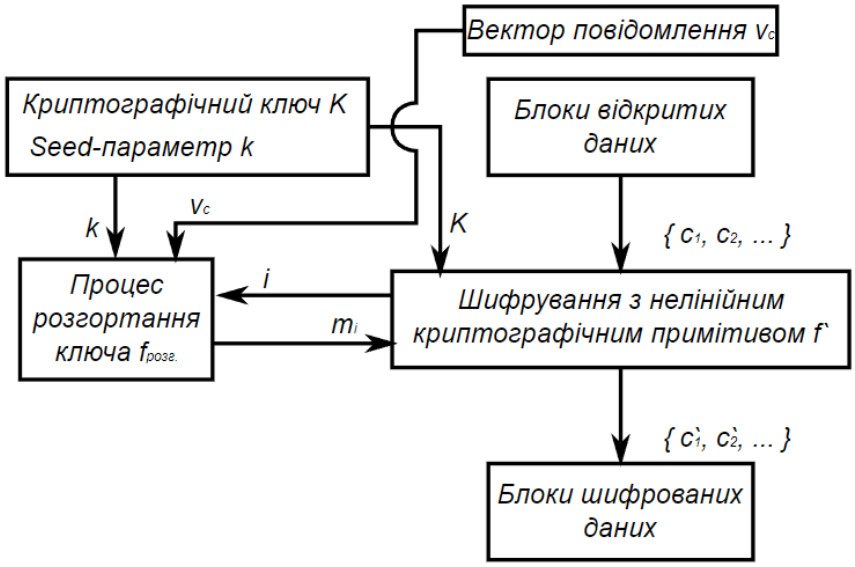

Рис. 4. Модель процесу шифрування нелінійної криптосистеми із процесом розгортання модифікатора

Fig. 4. The model of the encryption process of the nonlinear cryptosystem with the modifier deployment process

ПОБУДОВА ПОЛІКРИПТОСИСТЕМНИХ КРИПТОГРАФІЧНИХ ПРОТОКОЛІВ

Значним недоліком запропонованих рішень на рівні криптосистеми є необхідність модифікувати, змінювати та доповнювати конструкцію її алгоритмів, що однозначно буде порушенням затверджених сертифікованих та перевірених стандартів. Це не забороняє проектувати нові криптосистеми, або модифікувати існуючі, з використанням описаних методів, проте це створює необхідність досконалого кропіткого тестування, повторної сертифікації та усіх інших кроків, через які проходить нова криптосистема перед початком практичної експлуатації.

З іншого боку, перевагою запропонованого підходу є те що він легко масштабується під будь які рівні та може бути застосований на рівні протоколу шифрування, без необхідності змінювати структуру існуючих криптосистем. У якості криптографічних перетворень можуть бути використані вже існуючі криптографічні системи, із дотриманням вимог, подібних до тих що стояли перед криптографічними перетвореннями криптосистеми, зокрема:

- криптосистеми повинні мати приблизно рівну криптографічну стійкість, жодна із систем не повинна мати критичних вразливостей;
- використані в протоколі криптосистеми повинні мати однаковий, або кратний розмір вхідних та шифрованих блоків;
- рекомендується щоб обрані криптосистеми мали однаковий розмір ключа;
- вихідний шифротекст не повинен мати ознак, що вказують на криптосистему, якою він був створений.

В цілому криптосистеми можуть бути абсолютно різними за конструкцією та принципами роботи.

Загальна схема побудови нелінійного полікриптосистемного протоколу шифрування буде повністю подібною до схеми нелінійної криптосистеми, за вийнятком того, що криптоперетворення в ній представлені самостійними криптосистемами. Схема нелінійного криптографічного протоколу, на прикладі криптосистем Twofish та AES зображена на Рис. 5.

Для прикладу було обрано криптосистеми AES та Twofish. Обидві із них є достатньо криптостійкими, мають розмір блоку 128 біт та можуть працювати із криптографічним ключем, розміром 256 біт. В такому випадку множина модифікаторів матиме розмір 2, де, наприклад, Twofish матиме модифікатор «0», а AES – «1».

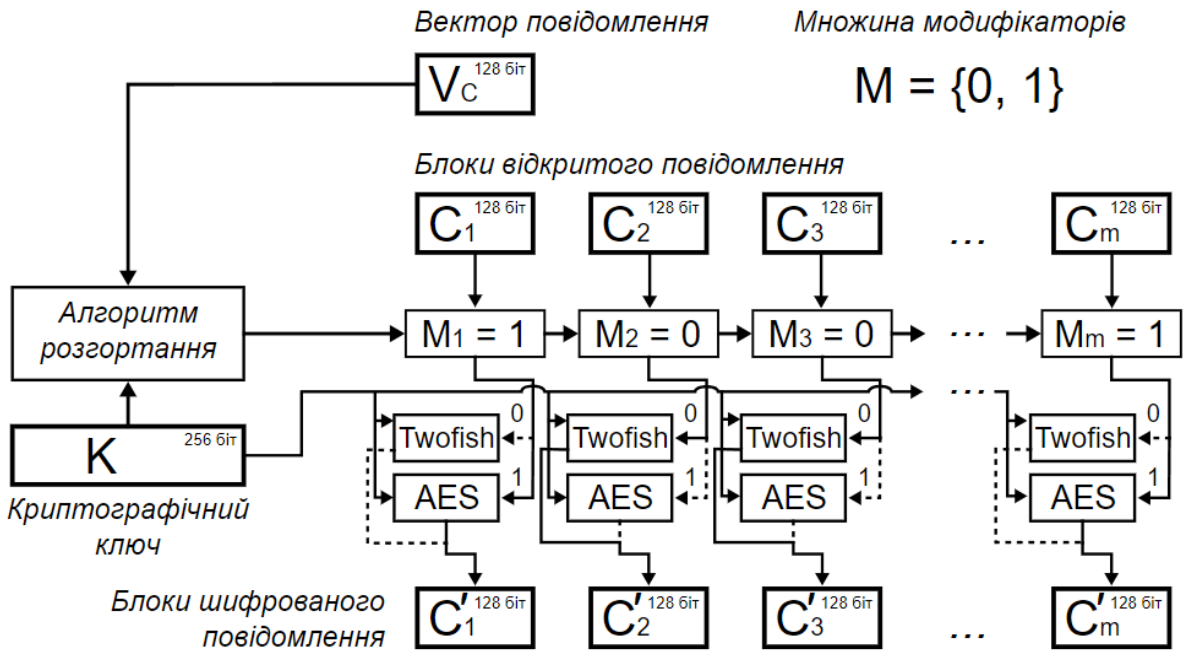

Рис. 5. Схема нелінійного полікриптосистемного криптографічного протоколу на прикладі криптосистем Twofish та AES. запропонованій схемі здійснюється за допомогою алгоритму розгортання, на основі наведеної раніше моделі

Fig. 5. Scheme of a nonlinear polycryptosystem cryptographic protocol based on the example of the Twofish and AES cryptosystems. the proposed scheme is carried out using the deployment algorithm, based on the model given earlier

Таким чином блоки зашифрованого повідомлення будуть шифруватись за допомогою однієї із двох криптографічних систем у псевдовипадковій послідовності. При цьому криптоаналітик не матиме можливості встановити цю псевдовипадкову послідовність, оскільки вона розгортається на основі криптографічного ключа за допомогою криптостійкого генератора гами, а не маючи послідовності використаних модифікаторів, аналітику буде значно важче організувати дослідження шифротексту.

Запропонована схема жодним чином не перешкоджає шифруванню у різних режимах. Зокрема, користуючись наведеною схемою, можна без жодних проблем проводити зчеплення блоків у режимі CBC, PCBC, чи будь-яких інших.

Подібний протокол також можна побудувати і на основі однієї криптосистеми. Нелінійність в такому разі може бути реалізована шляхом, наприклад, передобробки криптографічного ключа, перед виконанням раундів шифрування. Наприклад розмір криптографічного ключа протоколу може бути збільшений, а ключ для конкретного блоку може формуватися за одним із підготовлених наперед паттернів і/або із застосуванням інших криптографічних перетворень. В такому випадку для шифрування конкретного блоку даних буде застосований один із заданої множини криптографічних ключів, обраний також на основі модифікатора, а зашифровані різними криптографічними ключами блоки також будуть різними, що буде схоже на ефект попередньої схеми. Проте в даному випадку слід ретельно перевіряти алгоритми передобробки, на предмет відсутності прихованих вразливостей вихідних ключів і в цілому даний спосіб потребує додаткового вивчення.

Загалом, наведена схема нелінійного полікриптосистемного криптографічного протоколу є проста в реалізації як на

програмному, так і на апаратному рівні, що в свою чергу додатково спрощується наявністю вже готових серійних рішень, із високою швидкістю роботи, для конкретних криптосистем.

ВИСНОВКИ

Таким чином, на основі запропонованих раніше підходів нелінійного шифрування, було створено схему нелінійного полікриптосистемного криптографічного протоколу, на прикладі криптосистем AES та Twofish. Запропонована схема є дуже гнучкою та може бути легко адаптована практично під будь-які криптосистеми, що відповідають поставленим вимогам. Використання запропонованої концепції дозволяє підвищити криптографічну стійкість алгоритмів шифрування за рахунок алгоритмічних розгалужень в процесі шифрування, що, в поєднанні із алгоритмами генерації гами, значно ускладнює статистичні дослідження шифротексту.

Основними перевагами запропонованої схеми є:

1. Підвищення загальної криптографічної стійкості.
2. Велика гнучкість та масштабованість запропонованої схеми.
3. Використання в своїй структурі готових рішень із високою криптостійкістю, без жодної модифікації їх конструкції.

Серед недоліків можна виділити зростання кількості обчислень при шифруванні кожного блоку даних, що обов’язково вплине на швидкість шифрування реального прототипу.

В цілому описана тематика є перспективною для подальших досліджень, оскільки відкриває можливості простого та ефективного удосконалення існуючих криптографічних рішень.

ЛІТЕРАТУРА

1. **Корченко О. Г.** Прикладна криптологія: системи шифрування : підручник / О.Г. Корченко, В.П. Сіденко, Ю.О. Дрейс. – К. : ДУТ, 2014. – 448 с.
2. **Bellare Mihir**, and Phillip Rogaway. "Introduction to modern cryptography." Ucsd Cse 207 (2005): 207.
3. **Бурячок В. Л.** Інформаційний та кіберпростори: проблеми безпеки, методи та засоби боротьби : посібник / [В. Л. Бурячок, С. В. Толюпа, В. В. Семко та ін.]. – К.: ДУТ-КНУ, 2016. – 178 с.
4. **Qadir, Abdalbasit Mohammed**, and Nurhayat Varol. "A review paper on cryptography." 2019 7th international symposium on digital forensics and security (ISDFS). IEEE, 2019.
5. **Джулій В. М.** Модель стеганосистеми на основі просторових та форматних принципів приховування інформації / В. Джулій, М. Капустян, Ю. Кльоц, В. Орленко, В. Чешун // MEASURING AND COMPUTING DEVICES IN TECHNOLOGICAL PROCESSES. – 2023. – Вип. №2. – С. 58-64.
6. **Tang, Deng**, Claude Carlet, and Xiaohu Tang. "Highly nonlinear Boolean functions with optimal algebraic immunity and good behavior against fast algebraic attacks." IEEE transactions on information theory 59.1 (2012): 653-664.
7. **Анікін В. А.** Симетрична криптосистема з нелінійним шифруванням та можливістю контролю шифротексту з метою маскування / В. А. Анікін, В. М. Джулій, І.В. Муляр, В.С. Орленко, В.Ю. Тітова // Вісник Хмельницького національного університету. Технічні науки. – 2020. – № 6. – С. 12-19.
8. **Анікін В. А.** Побудова симетричної криптосистеми з нелінійним шифруванням / В. А. Анікін , А. О. Рамський, О. В. Мірошніченко, С. Ф. Стремецький // Тези доповідей Всеукраїнської науково-практичної конференції молодих вчених, ад’юнктів, слухачів, курсантів і студентів "Молодіжна військова наука у Київському національному університеті імені Тараса Шевченка", 23 квітня 2021 р. – Київ : ВІКНУ , 2021. – Т. 1. – С. 100

REFERENCES

1. **Korchenko O. G., Sydenko V. P., Drais Yu. O.** (2014). Applied cryptology: encryption systems: textbook. Kyiv, DUT, 448 (in Ukrainian).
2. **Bellare Mihir and Phillip Rogaway**. (2005). Introduction to modern cryptography. Ucsd Cse 207.
3. **Buriachok V. L., Toliupa S. V., Semko V. V.** (2016). Informatsiinyi ta kiberprostory: problemy bezpeky, metody ta zasoby borotby. Kyiv, DUT-KNU, 178 (in Ukrainian).
4. **Qadir Abdalbasit Mohammed**, **and Nurhayat Varol.** (2019). A review paper on cryptography. 2019 7th international symposium on digital forensics and security (ISDFS). IEEE.

5. **Dzhulii V. M., Kapustian M., Klots Yu., Orlenko V., Cheshun V.** (2023). Model stehanosystemy na osnovi prostorovykh ta formatnykh pryntsypiv prykhovuvannia informatsii. Measuring and computing devices in technological processes, No.2, 58-64.
6. **Tang Deng**, **Claude Carlet, and Xiaohu Tang**. (2012). Highly nonlinear Boolean functions with optimal algebraic immunity and good behavior against fast algebraic attacks. IEEE transactions on information theory 59.1, 653-664.
7. **Anikin V.A., Dzhulii V. M., Muliar I. V., Orlenko V. S., Titova V. Y.** (2020). Symmetric cryptosystem with nonlinear encryption and the possibility of control of ciphertext for concealment. Herald of Khmelnytskyi National University, Technical sciences, No.6, 12-19.
8. **Anikin V.A., Ramskyi A. O., Miroshnichenko O. V., Stremetskyi S. F.** (2021). Pobudova symetrychnoi kryptosystemy z neliniinym shyfruvanniam. Tezy dopovidei Vseukrainskoi naukovo-praktychnoi konferentsii molodykh vchenykh, ad'iunktiv, slukhachiv, kursantiv i studentiv "Molodizhna viiskova nauka u Kyivskomu natsionalnomu universyteti imeni Tarasa Shevchenka, Kyiv, VIKNU, Vol.1. 100.

Scheme of construction of nonlinear polycryptosystem cryptographic protocols

Ihor Muliar, Volodymyr Anikin

Abstract. The paper highlights the ways of constructing nonlinear encryption systems and proposes a scheme for constructing a nonlinear polycryptosystem cryptographic protocol that performs encryption of data blocks by various cryptographic systems in a pseudo-random sequence.

Using the proposed scheme allows you to build a cryptographic protocol using ready-made and proven encryption systems, without making any changes to their design. The pseudo-random alternation of cryptosystems in the encryption process is based on a cryptographically strong gamma expansion algorithm, which increases the nonlinearity of encryption and improves the general cryptographically strong of systems.

The article considered the structure of cryptosystems based on nonlinear cryptographic primitives, developed a model of the deployment process of modifiers of nonlinear cryptographic systems, and formed a general scheme of the structure of nonlinear cryptographic protocols using one or more different cryptosystems, provided they meet the specified requirements.

The advantages of the proposed scheme are great flexibility, scalability, and the possibility of applying the highlighted concept both at the level of cryptographic algorithms or their fragments and at the level of cryptosystems and cryptographic protocols.

The proposed solutions allow simple and effective improvement of existing cryptographic systems or their separate algorithms and are promising for further research.

Keywords: cryptography, nonlinear encryption, cryptosystem, cryptographic protocol, information protection