УДК 004.056 **doi: 10.26906/SUNZ.2022.1.084**

Т. В. Смірнова, Л. В. Константинова, С. А. Смірнов, Н. М. Якименко, О. А. Смірнов

Центральноукраїнський національний технічний університет, Кропивницький, Україна

ДОСЛІДЖЕННЯ СТІЙКОСТІ ДО ЛІНІЙНОГО КРИПТОАНАЛІЗУ ЗАПРОПОНОВАНОЇ ФУНКЦІЇ ГЕШУВАННЯ УДОСКОНАЛЕНОГО МОДУЛЯ КРИПТОГРАФІЧНОГО ЗАХИСТУ В ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ СИСТЕМАХ

Анотація. Об'єктом дослідження є процес забезпечення конфіденційності даних в інформаційно-комунікаційних системах управління технологічними процесами на базі хмарних технологій. **Предметом дослідження** є дослідження стійкості до лінійного криптоаналізу запропонованої функції гешування удосконаленого модуля криптографічного захисту в інформаційно-комунікаційних системах. **Мета роботи** полягає у дослідженні стійкості до лінійного криптоаналізу запропонованої функції гешування удосконаленого модуля криптографічного захисту в інформаційно-комунікаційних системах управління технологічними процесами на базі хмарних технологій. **У результаті дослідження** удосконалено модуль криптографічного захисту інформації. Проведено дослідження стійкості до лінійного криптоаналізу запропонованої функції гешування удосконаленого модуля криптографічного захисту в інформаційно-комунікаційних системах. Проведене експериментальне дослідження підтвердило криптостійкість удосконаленого алгоритму до лінійного криптоаналізу. **Висновки.** Удосконалено модуль криптографічного захисту інформації, який за рахунок фіксування інформації про ідентифікатор користувача, ідентифікатор сесії, час відправлення, довжину повідомлення та його порядковий номер, а також використання нової процедури формування сеансового ключа для шифрування, дозволяє забезпечити конфіденційність і цілісність даних в інформаційно-комунікаційних системах управління технологічними процесами. Для ефективного використання цього модуля важливим є вибір криптостійких методів шифрування та гешування, а також синхронізація секретного ключа. У якості функцій можуть бути використані криптоалгоритми, стійкі до лінійного, диференціального, алгебраїчного, квантового та інших відомих видів криптоаналізу. Проведено дослідження стійкості до лінійного криптоаналізу запропонованої функції гешування удосконаленого модуля криптографічного захисту в інформаційно-комунікаційних системах. Проведене експериментальне дослідження підтвердило криптостійкість удосконаленого алгоритму до лінійного криптоаналізу.

Ключові слова: криптоаналіз, гешування, інформаційно-комунікаційні системи, захист інформації.

Вступ

На сучасному етапі розвитку хмарних технологій, існує завдання захисту даних, які зберігаються у відповідних інформаційно-комунікаційних системах. За останній час проти України було реалізовано декілька криптоатак на різні хмарні сервіси, а саме:

– 14 січня 2022 р. – масована кібератака, у результаті якої постраждали 22 сайти органів державної влади. Шести сайтам було завдано значної шкоди, 70 – відключено за вказівкою Держспецзв'язку та Служби безпеки України [1].

– 15 лютого 2022 року – DDoS-атака на низку інформаційних ресурсів України. Зокрема, було зафіксовано перебої в роботі веб-сервісів Приватбанку та Ощадбанку. Також атаки зазнали сайти Міністерства оборони та Збройних Сил України [2].

Аналіз цих криптоатак показав, що потребується розроблення нових або удосконалення існуючих механізмів захисту інформації. Одними з таких механізмів є програмні модулі криптографічного захисту даних, у яких необхідно реалізовувати вибір стійких методів шифрування та гешування, а також синхронізацію секретного ключа. У якості зазначених процедур можуть використовуватись відомі криптографічні методи і засоби, стійкі до лінійного, диференціального, алгебраїчного, квантового та інших відомих видів криптоаналізу.

Аналіз останніх досліджень і публікацій. Сьогодні серед множини методів захисту інформації особливе місце займають криптографічні методи [3]. У теперішній час в хмарних сервісах використовуються такі відомі програмні модулі криптографічного захисту даних:

– MTProto 1.0 [4] – модуль, який використовується для шифрування повідомлень при передаванні клієнтами Telegram;

– Signal Protocol [5] – використовується для шифрування миттєвих повідомлень Facebook Messenger;

– TLS Skype [6] – для миттєвих повідомлень використовується TLS (безпека на рівні транспорту) для шифрування повідомлень між клієнтом Skype та службою чату, коли вони надсилаються безпосередньо між двома клієнтами Skype.

Проведений порівняльний аналіз розглянутих модулів захисту інформації у сучасних інформаційно-комунікаційних системах та мережах (ІКСМ). за такими критеріями, як використовувані криптоалгоритми; швидкість роботи (ШР); зручність для користувачів (ЗК); кросплатформеність (КП). Наведемо результати цього порівняльного аналізу.

1. MTProto 1.0 [16]:

– використовувані криптоалгоритми; SHA-256, AES-256.

– швидкість роботи (ШР) – висока;

– зручність для користувачів (ЗК) – висока;

– кросплатформеність (КП) – присутня частково.

2. Signal Protocol [16]:

– використовувані криптоалгоритми; Curve25519, AES-256, HMAC, SHA-256;

– швидкість роботи (ШР) – середня;

– зручність для користувачів (ЗК) – висока;

– кросплатформеність (КП) – присутня.

3. TLS Skype [16]:

– використовувані криптоалгоритми; AES-256, RSA;

– швидкість роботи (ШР) – середня;

– зручність для користувачів (ЗК) – низька;

– кросплатформеність (КП) – присутня частково.

Таким чином з порівняльного аналізу розглянутих модулів захисту інформації можливо зробити висновок, що розглянуті програмні модулі мають низку недоліків і можуть бути удосконалені за рахунок використання сучасних процедур безпеки [16].

Зважаючи на зазначене, в роботі [16] був розроблений удосконалений модуль криптографічного захисту інформації для забезпечення конфіденційності та цілісності даних у сучасних ІКСМ. Для використання цього модуля на практиці потрібно визначитись з функціями гешування F_{hash} та шифрування F_{enc}.

Удосконалений модуль криптографічного захисту інформації, за рахунок фіксування інформації про ідентифікатор користувача; ідентифікатор сесії; час відправлення; довжину повідомлення; порядковий номер повідомлення; використання нової процедури формування сеансового ключа для шифрування, дозволяє забезпечити конфіденційність і цілісність даних в ІКСМ [16]. Для ефективного використання цього модуля важливим є вибір:

– криптостійких методів шифрування F_{enc};

– криптостійких методів гешування F_{hash};

– синхронізація секретного ключа *authKey*.

У якості функцій F_{enc} та F_{hash} можуть бути використані зокрема й алгоритми, запропоновані авторами у своїх попередніх роботах [8, 10-12, 16], або інші відомі криптоалгоритми [7, 9, 13-15], стійкі до лінійного, диференціального, алгебраїчного, квантового та інших відомих видів криптоаналізу.

Областю застосування запропонованих підходів є хмарні системи які описані у [19, 20].

Мета роботи полягає у дослідженні стійкості до лінійного криптоаналізу запропонованої функції гешування удосконаленого модуля криптографічного захисту в інформаційно-комунікаційних системах управління технологічними процесами на базі хмарних технологій.

Вимоги, особливості застосування і шляхи оптимізації сучасних криптосистем

Історично першими з'явилися симетричні криптографічні системи. У симетричній криптосистемі шифрування використовується один і той же ключ для зашифрування і розшифрування інформації. Це означає, що будь-який, хто має доступ до ключа шифрування, може розшифрувати повідомлення.

Для забезпечення необхідного рівня захисту інформації в інформаційних системах, до алгоритмів шифрування і системи ключів пред'являються деякі вимоги [4, 12, 16]:

1) криптограма (шифротекст) повинна дешифруватися лише за наявності ключа;

2) число операцій, необхідне для розтину ключа по відкритому тексту і відповідній йому криптограмі, має бути не менше числа всіх можливих ключів;

3) знання алгоритму шифрування не повинне спрощувати процедури дешифрування, що виконується з метою розтину ключів і дешифровки криптограм;

4) незначна зміна ключа, з використанням якого шифрується від критий текст, повинна приводити до істотної зміни відповідної криптограми;

5) незначна зміна відкритого тексту при незмінному ключі повинна приводити до істотної зміни відповідної криптограми;

6) структура алгоритму шифрування має бути постійною;

7) в процесі шифрування має бути передбачений контроль за шифрованим відкритим текстом і ключем;

8) довжина криптограми має дорівнювати довжині відкритого тексту;

9) складність розтину ключа, використовуваного для шифрування чергового відкритого тексту, по послідовності ключів, використаних для шифрування попередніх текстів, має бути порівнянною із складністю розтину ключа по відкритому тексту і відповідній йому криптограмі;

10) безліч всіх можливих ключів має бути однорідною і не повинно містити «слабких» ключів, стосовно яких процедури криптоаналізу відносно простіші і ефективніші;

11) криптограма має бути однорідною, тобто не повинна ділитися на фрагменти (символи, біти), одні з яких апріорі (умоглядно або інтуїтивно) відомі як що відносяться до відкритого тексту, а інші – як включені в шифротекст в процесі шифрування;

12) алгоритм шифрування повинен допускати як програмну, так і апаратну реалізацію;

13) зміну довжини ключа не повинні погіршувати характеристики алгоритму шифрування.

Криптосистема, повинна задовольняти перерахованим вимогам, тільки тоді вона буде вважатися вважається криптостійкою і придатною для використання та для захисту інформації в інформаційних системах.

Умови перераховані вище є обов'язковими для надійних криптосистем.

Криптоалгоритми поза сумнівом є ядром криптографічних систем, але, як ми зараз побачимо, їх безпосереднє вживання без яких-небудь модифікацій для кодування великих об'ємів даних насправді не дуже підходить.

Всі недоліки безпосереднього вживання криптоалгоритмів усуваються в криптосистемах.

Криптосистема – це завершена комплексна модель, що здатна виробляти двосторонні криптопретворень над даними довільного об'єму і підтверджувати час відправки повідомлення, володіє механізмом перетворення паролів і ключів і системою транспортного кодування.

Таким чином, криптосистема виконує три основні функції [4, 12, 16]:

1. Посилення захищеності даних.
2. Полегшення роботи з криптоалгоритмом з боку людини.
3. Забезпечення сумісності потоку даних з іншим програмним забезпеченням.

Наступним удосконаленням, направленим на підвищення стійкості всієї системи в цілому є створення ключів сеансу.

Ця операція необхідна в тих випадках, коли виробляється часте шифрування схожих блоків даних одним і тим же ключем.

Наприклад, це має місце при передачі інформації або команд в автоматизованих системах управління, в банківських операціях і багатьох інших випадках передачі інформації, що має визначений заздалегідь відомий формат.

В цьому випадку необхідне введення якої-небудь випадкової величини в процес шифрування. Це можна зробити декількома способами:

1. Записом в початок файлу даних псевдовипадкової послідовності байт заздалегідь обумовленої довжини з відкиданням її при дешифровці – цей метод працюватиме лише при вживанні алгоритмів створення ланцюжків з пам'яттю (CBC,CFB,OFB).
2. Вживанням модифікованих алгоритмів створення ланцюжків, які при шифрування кожного блоку змішують з ним або а) фіксовану випадкову величину, прикріплену на початок зашифрованого файлу, або б) значення, що обчислюються за допомогою того ж шифру і ключа від заздалегідь обумовленої величини.

Створенням спеціально для кожного файлу абсолютно випадкового ключа, так званого ключа сеансу, яким і шифрується весь файл (сам же ключ сеансу шифрується первинним ключем, званим в цьому випадку майстром-ключем і поміщається на початку зашифрованого файлу).

Теоретичне обґрунтування удосконалення модуля захисту

З огляду на результати проведеного аналізу, прототипом було обрано розглянутий модуль MTProto Mobile Protocol v.1.0 [4], порівняно з яким було змінено наступне [16]:

1. Змінені вхідні та вихідні дані.

На вході приймаються і обробляються такі дані:

– повідомлення M ;

– інформацію про ідентифікатор користувача та ідентифікатор сесії S ;

– інформацію про час відправлення і довжину повідомлення ID ;

– порядковий номер повідомлення PD .

На виході отримуємо:

– $mHash$ – геш значення:

$$DB \ (DB = (S, ID, M));$$

– $EncP$ – зашифроване повідомлення P [16].

2. Замість використання геш функції SHA-1 введено використання певної криптостійкої геш функції F_{hash} .

Слід зауважити, що у якості F_{hash} може бути використана функція гешування, що побудована на основі одного із методів [7-9, 16].

3. Замість використання блокового шифру AES введено використання функції F_{enc} .

Слід зауважити, що у якості F_{enc} може бути використаний певний криптостійкий алгоритм шифрування, побудований на основі блокових, потокових шифрів чи геш функцій тощо [10-12, 16].

4. У якості *authKey* , введено використання заздалегідь узгодженого секретного ключа користувачів, наприклад за допомогою протоколів асиметричної криптографії [16].

Для використання цього модуля на практиці потрібно визначитись з функціями гешування F_{hash} та шифрування F_{enc} .

На рис. 1 наведена схема роботи удосконаленого модуля криптографічного захисту інформації, який описаний у роботі [16].

Дослідження стійкості запропонованої функції гешування удосконаленого модуля криптографічного захисту в інформаційно-комунікаційних системах

Експериментальне дослідження запропонованої функції гешування для забезпечення удосконаленого модуля криптографічного захисту в інформаційно-комунікаційних системах включає у себе наступні етапи:

– Дослідження лінійних перетворень.

– Дослідження стійкості до диференціального криптоаналізу.

– Дослідження стійкості до лінійного криптоаналізу.

– Дослідження статистичної стійкості.

– Дослідження швидкісних характеристик.

Розглянемо ці методи криптоаналізу.

Дослідження лінійних перетворень.

Багато видів криптоаналітичних атак засновані на лінійності більшості перетворень, що використовуються у шифрах. Під лінійним перетворенням T відносно деякої операції $\oplus$. розуміється перетворення, для якого справедливо

$$T(X) \oplus T(X') = T(X \oplus X'),$$

де $T(X)$ – результат виконання перетворення T для вхідного блоку X.

Лінійні перетворення в БСШ вирішують завдання розсіювання, тобто поширюють вплив кожного вхідного біта на як можна більшу кількість вихідних бітів.

Основний показник, що характеризує якість розсіювання лінійного перетворення, це число галузей активізації (branch number) [7].

Дослідження стійкості до диференціального криптоаналізу.

Диференціальний криптоаналіз – це спроба розкриття секретного ключа блокових шифрів, які засновані на повторному застосуванні криптографічно слабкої цифрової операції шифрування r разів.

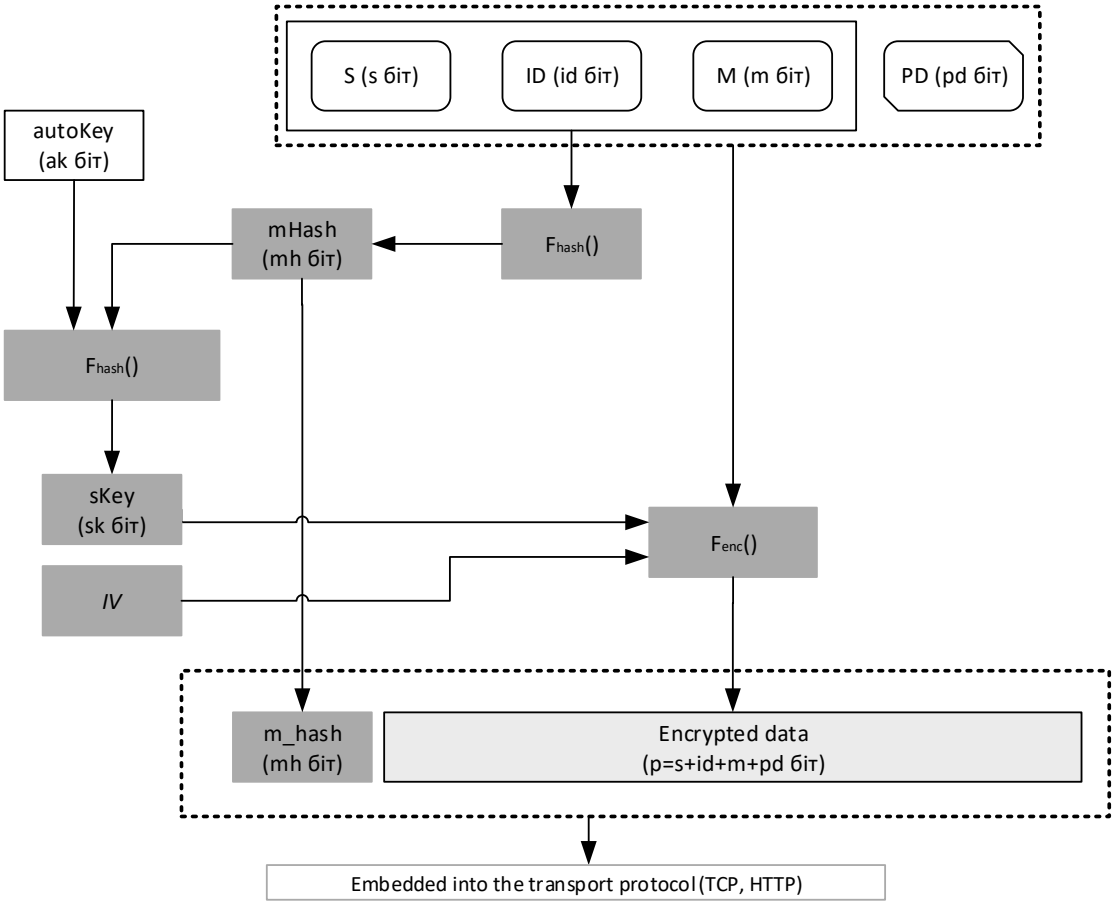

Рис. 1 . Схема роботи удосконаленого модуля криптографічного захисту інформації [16]

При аналізі передбачається, що на кожному циклі використається свій підключ шифрування.

Диференціальний криптоаналіз може використовувати як обрані, так і відомі відкриті тексти. Конкретний спосіб диференціального криптоаналізу залежить від аналізованого алгоритму шифрування.

Дослідження стійкості до лінійного криптоаналізу.

Лінійний криптоаналіз винайшов японський криптолог М. Мацуі (Mitsuru Matsui) і з тих пір вважається одним з найбільш ефективних для сучасних блокових симетричних шифрів. Цей метод використовує лінійні наближення перетворень, що виконуються алгоритмом шифрування. Даний метод дозволяє знайти ключ, маючи досить велику кількість пар (незашифрований текст, зашифрована текст). Розглянемо основні принципи, на яких базується лінійний криптоаналіз. Лінійний криптоаналіз базується на тому, що існує можливість замінити нелінійну функцію її лінійним аналогом.

Дослідження статистичної стійкості.

Для дослідження статистичної стійкості використовують тести NIST STS. Розглянемо опис тестів NIST STS. До них відносяться наступні тести:

– Частотний (монобітний тест).

– Частотний блоковий тест.

– Тест на щонайдовшу послідовність одиниць в блоці.

– Тест на послідовність однакових бітів.

– Тест рангів бінарних матриць.

– Спектральний тест.

– Тест на збіг шаблонів, що перекриваються.

– Універсальний статистичний тест Маурера.

– Тест приблизної ентропії.

– Тест на довільні відхилення.

– Інший тест на довільні відхилення.

– Тест на періодичність.

– Тест кумулятивних сум.

– Тест на збіг шаблонів, що не перекриваються.

– Тест на лінійну складність.

Дослідження швидкісних характеристик.

Для проведення порівняльного аналізу швидкісних характеристик прототипу (оригіналу криптоалгоритму) та удосконаленого методу перетворення інформації береться програмне забезпечення криптоалгоритму та створюється програмне забезпечення його модифікації.

Для проведення порівняльного аналізу швидкісних характеристик розробленого генератора криптографічних ключів з генератором ключів, що використовується в криптоалгоритму та лінійно конгруентним генератором береться програмне забезпечення зазначених генераторів та створюється програмне забезпечення розробленого генератора криптографічних ключів.

Запускаючи програмне забезпечення оригіналу та його модифікації на одній платформі, з використанням одних й тих же системних параметрів відбувається замір та порівняння відповідних швидкісних характеристик.

Дослідження стійкості до лінійного криптоаналізу запропонованої функції гешування удосконаленого модуля криптографічного захисту в інформаційно-комунікаційних системах

Дана робота присвячена дослідженню стійкості саме до лінійного криптоаналізу запропонованої функції гешування удосконаленого модуля криптографічного захисту в інформаційно-комунікаційних системах.

Для вираження результату проведення лінійного криптоаналізу аналогічно диференціальному використовується критерій стійкості до лінійного криптоаналізу, який для *r*-циклічного SPN – шифру може бути представлений у вигляді такої нерівності:

$$P_{\text{ДХ}}^{(r-1)} \le 2^{\frac{-n}{2}},$$

де: число раундів; n – розмір блоку в бітах; $P_{\text{ДХ}}^{(r)}$ – верхня границя імовірності r-циклічної лінійної характеристики.

Традиційний підхід до оцінки стійкості БСШ до лінійного криптоаналізу схожий на стійкості БСШ до диференційного криптоаналізу і складається з таких дій:

1. Розраховується таке мінімальне число активних підстановок у диференціальній характеристиці, яке буде покривати потрібне для організації ефективної атаки число циклів.
2. Обчислюється верхня границя імовірності лінійної характеристики. Для цього використовується два параметри:
   a. Кількість активних підстановок;
   b. Максимальна ймовірність лінійної апроксимації окремої підстановки.

Відбувається піднесення другого параметру до степеня першого, тобто:

$$P_{\text{ДХ}}^{(r)} = \left(P_{L_{max}}\right)^{a^{(r)}},$$

де $a^{(r)}$ – мінімальна кількість активних підстановок в r раундах шифру.

Параметр підстановки $P_{L_{max}}$ розраховується за таким алгоритмом:

1. Побудова таблиці лінійних апроксимацій, що складається із значень:

$$s_s(a,b) = \#\{x \in GF(2^n) | \big(W(x\&a) + W(S(x)\&b)\big) mod 2 = 0\} - 2^{n-1}$$

для всіх варіантів $a, b \in GF(2^n)$, де:

– a – різниця між вхідними даними;
– b – різниця між даними після проходження *S*-блоків;
– $\&$ – побітова кон'юнкція;
– $W(x)$ – вага Хемінга вектора x (кількість одиничних бітів у цьому векторі);
– $mod2$ – операція узяття за модулем 2.

2. Розрахунок максимальної імовірності лінійної апроксимації, $P_{L_{max}}$ визначається за формулою:

$$P_{L_{max}} = \frac{\left|\max\limits_{a\neq 0; b\neq 0} c_s(a,b)\right|}{2^{n-1}}.$$

Провівши аналіз *S*-блоку алгоритму NRC21, побудована таблиця лінійних апроксимацій.

За таблицею лінійних апроксимацій встановлено, що для всіх підстановок, які використовуються у шифрі NRC21 $P_{L_{max}} = 0{,}0234375$.

Для розрахунку верхньої границі ймовірності для багатоциклових лінійних характеристик для спрощеного шифру необхідно підставити у зазначену формулу $P_{L_{max}} = 0{,}0234375$ та $a^{(r)}$.

У табл. 1 кольором показані осередки, які визначають число циклів, при якому ймовірність диференціальної характеристики знаходиться нижче граничного значення.

Таблиця 1 -- **Визначення числа циклів, при якому ймовірність лінійної характеристики знаходиться нижче граничного значення**

Розмір блоку, біти	Число циклів							
	1	2	3	4	5	6	7	8
128	2^{-6}	2^{-50}	2^{-56}	2^{-149}	2^{-154}	2^{-198}	2^{-209}	2^{-297}

Дані, що наведені в табл. 1, дозволяють зробити висновок про стійкість до лінійного криптоаналізу шифру NRC21 з 128-бітним блоком, що містить 5 і більше циклів (10 і більше раундів).

Висновки

Удосконалено модуль криптографічного захисту інформації, який за рахунок фіксування інформації про ідентифікатор користувача, ідентифікатор сесії, час відправлення, довжину повідомлення та його порядковий номер, а також використання нової процедури формування сеансового ключа для шифрування, дозволяє забезпечити конфіденційність і цілісність даних в ІКСМ управління технологічними дуля важливим є вибір криптостійких методів шифрування процесами.

Для ефективного використання цього мо F_{enc} та гешування F_{hash}, а також синхронізація секретного ключа *authKey*. У якості функцій F_{enc} та F_{hash} можуть бути використані криптоалгоритми, стійкі до лінійного, диференціального, алгебраїчного, квантового та інших відомих видів криптоаналізу.

Проведено дослідження стійкості до лінійного криптоаналізу запропонованої функції гешування удосконаленого модуля криптографічного захисту в інформаційно-комунікаційних системах.

Проведене експериментальне дослідження підтвердило криптостійкість удосконаленого алгоритму до лінійного криптоаналізу.

СПИСОК ЛІТЕРАТУРИ

1. https://www.kmu.gov.ua/news/vid-kiberataki-14-sichnya-postrazhdali-22-derzhavnih-organi-derzhspeczvyazku
2. https://www.kmu.gov.ua/news/shchodo-kiberataki-na-sajti-vijskovih-struktur-ta-derzhavnih-bankiv
3. R. Oppliger, Cryptography 101: *From Theory to Practice*, Artech, 2021.

4. Job J, Naresh V and K. Chandrasekaran, "A modified secure version of the Telegram protocol (MTProto)", 2015 IEEE International Conference on Electronics, Computing and Communication Technologies (CONECCT), 2015, pp. 1-6,
5. Dion van Dam, Analysing the Signal Protocol. A manual and automated analysis of the Signal Protocol, 21 August 2019, 61 p.
6. TLS and SRTP for Skype Connect Technical Datasheet, 2011, 8 p.
7. Q. Wu, "A Chaos-Based Hash Function", 2015 International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery, 2015, pp. 1-4,
8. Gnatyuk S., Kinzeryavyy V., Kyrychenko K., Yubuzova Kh., Aleksander M., Odarchenko R. Secure Hash Function Constructing for Future Communication Systems and Networks, *Advances in Intelligent Systems and Computing*, Vol. 902, pp. 561-569, 2020.
9. K. Rajeshwaran and K. Anil Kumar, "Cellular Automata Based Hashing Algorithm (CABHA) for Strong Cryptographic Hash Function", *2019 IEEE International Conference on Electrical, Computer and Communication Technologies (ICECCT)*, 2019, pp. 1-6,
10. Iavich M., Iashvili G., Gnatyuk S., Tolbatov A., Mirtskhulava L. Efficient and Secure Digital Signature Scheme for Post Quantum Epoch, *Communications in Computer and Information Science*, Vol. 1486, pp. 185-193, 2021.
11. Gnatyuk S., Iavich M., Kinzeryavyy V., Okhrimenko T., Burmak Y., Goncharenko I. Improved secure stream cipher for cloud computing, *CEUR Workshop Proceedings*, Vol. 2732, pp. 183-197, 2020.
12. Gnatyuk S., Akhmetov B., Kozlovskyi V., Kinzeryavyy V., Aleksander M., Prysiazhnyi D. New Secure Block Cipher for Critical Applications: Design, Implementation, Speed and Security Analysis, *Advances in Intelligent Systems and Computing*, Vol. 1126, pp. 93-104, 2020.
13. A. Kuznetsov, I. Horkovenko, O. Maliy, N. Goncharov, T. Kuznetsova and N. Kovalenko, "Non-Binary Cryptographic Functions for Symmetric Ciphers", 2020 IEEE International Conference on Problems of Infocommunications. Science and Technology (PIC S&T), 2020, pp. 567-572, doi: 10.1109/PICST51311.2020.9467982.
14. E. Jintcharadze and M. Iavich, "Hybrid Implementation of Twofish, AES, ElGamal and RSA Cryptosystems", *2020 IEEE East-West Design & Test Symposium (EWDTS)*, 2020, pp. 1-5, doi: 10.1109/EWDTS50664.2020.9224901.
15. T. R. Lee, J. S. Teh, N. Jamil, J. L. S. Yan and J. Chen, "Lightweight Block Cipher Security Evaluation Based on Machine Learning Classifiers and Active S-Boxes", in *IEEE Access*, vol. 9, pp. 134052-134064, 2021, doi: 10.1109/ACCESS.2021.3116468.
16. Смірнова Т.В., Гнатюк С.О., Бердибаєв Р.Ш., Бурмак Ю.А., Оспанова Д.М., «Удосконалений модуль криптографічного захисту інформації в сучасних інформаційно-комунікаційних системах та мережах». *Кібербезпека: освіта, наука, техніка*. № 2(14). С. 176-185. 2021.
17. Смірнова Т.В., Поліщук Л.І., Смірнов О.А., К.О. Буравченко, А.О.Макевнін, «Дослідження хмарних технологій як сервісів», *Кібербезпека: освіта, наука, техніка*. № 3(7). С. 43-62. 2020.
18. Смірнова Т.В., Солових Є.К., Смірнов О.А., Дрєєв О.М., «Побудова хмарних інформаційних технологій оптимізації технологічного процесу відновлення та зміцнення поверхонь деталей», *Центральноукраїнський науковий вісник. Технічні науки.* № 1(32). с. 184-194, 2019.
19. Смірнова, Т.В., Смірнов, С.А., Минайленко, Р.М., Доренський, О.П., Сисоєнко С.В. «Хмарна автоматизована система інтелектуальної підтримки прийняття рішень для технологічних процесів». *Вісник Черкаського державного технологічного університету. Технічні науки.* №4, 2020, С. 84-92.
20. Смірнова Т.В., Буравченко К.О., Кравченко С.С., Горбов В.О., Смірнов О.А. «Хмарна система підтримки прийняття рішень технологічного процесу відновлення поверхонь конструкцій і деталей машин». *Сучасні інформаційні системи*. 2021. Т. 5, № 4. С. 79-95.

Received (Надійшла) 23.12.2021
Accepted for publication (Прийнята до друку) 09.02.2022

Study of resistance to linear cryptanalysis of the proposed hashing function of an improved cryptographic protection module in information and communication systems

Tetiana Smirnova, Liliia Konstantynova, Serhii Smirnov, Nataliia Yakymenko, Oleksii Smirnov

Abstract. **The object of research** is to ensure the confidentiality of data in information and communication systems for managing technological processes based on cloud technologies. **The subject of the research** is the study of resistance to linear cryptanalysis of the proposed hashing function of an improved cryptographic protection module in information and communication systems. **The purpose of the work** is to study the resistance to linear cryptanalysis of the proposed hashing function of an improved model of cryptographic protection in information and communication process control systems based on cloud technologies. **As a result of the research**, the module of cryptographic protection of information has been improved. A study of resistance to linear cryptanalysis of the proposed hashing function of an improved cryptographic protection module in information and communication systems has been carried out. The conducted experimental study confirmed the cryptographic resistance of the improved algorithm to linear cryptanalysis. **Conclusions**. The cryptographic information protection module has been improved, which, by recording information about the user ID, session ID, sending time, message length and sequence number, as well as using a new procedure for generating a session key for encryption, makes it possible to ensure the confidentiality and integrity of data in information and communication systems process control. For the effective use of this module, it is important to choose cryptographically strong encryption and hashing methods, as well as synchronization of the secret key. As functions, cryptalgorithms resistant to linear, differential, algebraic, quantum and other known types of cryptanalysis can be used. A study of the resistance to linear cryptanalysis of the proposed hashing function of an improved cryptographic protection module in information and communication systems has been carried out. The conducted experimental study confirmed the cryptographic resistance of the improved algorithm to linear cryptanalysis.

Keywords: cryptanalysis, hashing, information and communication systems, information security