УДК 004.056 **doi: 10.26906/SUNZ.2022.3.093**

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

Центральноукраїнський національний технічний університет, Кропивницький, Україна

ДОСЛІДЖЕННЯ СТІЙКОСТІ ДО ДИФЕРЕНЦІАЛЬНОГО 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** є дослідження стійкості до диференціального криптоаналізу запропонованої функції гешування удосконаленого модуля криптографічного захисту в інформаційно-комунікаційних системах. **Мета роботи** полягає в дослідженні стійкості до диференціального 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 диференціального криптоаналізу запропонованої функції гешування удосконаленого модуля криптографічного захисту в інформаційно-комунікаційних системах. Проведене експериментальне дослідження підтвердило криптостійкість удосконаленого алгоритму до диференціального 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 та можуть бути використані криптоалгоритми, стійкі до лінійного, диференціального, алгебраїчного, квантового та інших відомих видів криптоаналізу. Проведено дослідження стійкості до диференціального криптоаналізу запропонованої функції гешування удосконаленого модуля криптографічного захисту в інформаційно-комунікаційних системах. Проведене експериментальне дослідження підтвердило криптостійкість удосконаленого алгоритму до диференціального криптоаналізу.

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

Вступ

Початок 2022 року в України ознаменувався рядом кібератак на хмарні ресурси державних установ. Так під час масованої кібератаки, яка почалася у ніч з 13-го на 14 січня, постраждали 22 сайти органів державної влади. Шести сайтам було завдано значної шкоди, 70 – відключено за вказівкою Держспецзв'язку та Служби безпеки України [1]. Починаючи з другої половини дня 15 лютого 2022 року спостерігалась потужна 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]. Таким чином очевидно, що на сучасному етапі розвитку хмарних технологій, існує завдання захисту даних, які зберігаються у відповідних інформаційно-комунікаційних системах.

Останні події, пов'язані з атаками на різні хмарні сервіси потребують 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 наступні 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) і кросплатформеність (КП), показав, 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 та його порядковий номер, а також 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} та гешування F_{hash}, а також 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. У подальшому планується зосередити увагу на дослідженнях удосконаленого модуля криптографічного захисту інформації з використанням різних методів шифрування і гешування, зокрема тих, що були запропоновані авторами у своїх попередніх дослідженнях. Областю застосування запропонованих підходів є хмарні системи які описані у [19, 20].

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

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 наступні дані: повідомлення M, інформацію про ідентифікатор користувача та ідентифікатор сесії S, інформацію про час відправлення і довжину повідомлення ID та порядковий номер повідомлення PD. На виході тільки отримуємо $mHash$ – геш значення DB ($DB = (S, ID, M)$) та $EncP$ – 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}.

Схеми шифрування та дешифрування удосконаленого модуля криптографічного захисту в інформаційно-комунікаційних системах наведені на рис. 1, 2.

У схемах використовуються такі позначення:

– $K_0 \dots K_{t-1}$, – масив розширених ключів;

– *i, j, A, B, C* і *D* – тимчасові змінні, їх початкові значення дорівнюють нулю;

– $Ft()$ і $Fu()$ – функції раундового перетворення алгоритму;

– *RC*[] – перемішування в колонках (RoundColumns);

– *IRC*[] – зворотнє до *RC*[] перемішування в колонках (InvRoundColumns);

– *відкритий текст* – блок даних розміром 128 бітів (16 байтів), що підлягає зашифровуванню, а також блок даних того ж розміру після розшифровування (розміри відкритого тексту й шифротексту збігаються);

– *шифротекст* – блок даних розміром 128 бітів (16 байтів) після зашифровування, або цей же блок даних, що підлягає розшифруванню (розміри відкритого тексту й шифротексту збігаються);

– *ключ шифрування (секретний ключ, K)* – блок даних розміром 128 бітів (16 байтів), 256 бітів (32 байтів), 512 бітів (64 байтів), що використовується в якості встановлюваного секретного параметра в процедурі зашифрування або розшифрування;

– *процедура розширення підключів* – алгоритм формування із ключа шифрування − підключів, для виконання раундових перетворень;

– *підключ* (K_i) – блок даних розміром 32 біти (4 байта), що отриманий із ключа шифрування в результаті виконання процедури розширення підключів;

– *раунд* – інтерактивна процедура, що здійснює перетворення робочого стану на вході процедури в поточний стан на її виході із застосуванням відповідних підключів;

– *кількість раундів (r)*–кількість цифрових перетворень при шифруванні;

– *таблиця підстановки* – таблиця заміни (підстановки) байтових значень, що реалізує нелінійне перетворення;

– <<</>>> – циклічний побітний зсув вліво/ вправо;

– <</>> – по бітний зсув вліво/ вправо;

– $\oplus$ – додавання за модулем 2;

– [+] – додавання за модулем 2^{32};

– [*] – множення за модулем 2^{32}.

Процедура зашифрування. На вхід процедури подаються підключі K_i і відкритий текст, який розбивається на підблоки *A, B, C, D*. Спочатку виконується повне початкове відбілювання (рандомізація) підблоків *A, B, C* і *D*. Потім виконуються *r* раундових перетворень. Далі виконується повне кінцеве відбілювання підблоків *A, B, C* і *D*. Отримані у результаті зашифрування підблоки об'єднують у шифротекст.

Процедура розшифрування. При розшифруванні підключі використовуються в зворотному порядку, накладання підключів замість додавання по модулю 2^n виконується відніманням, зрушення субблоків виконується на початку раунду і у зворотний бік, а також замість процедури *RoundColumns* використовується зворотня до неї – *InvRoundColumns*. Перетворення *f()* не зазнало змін.

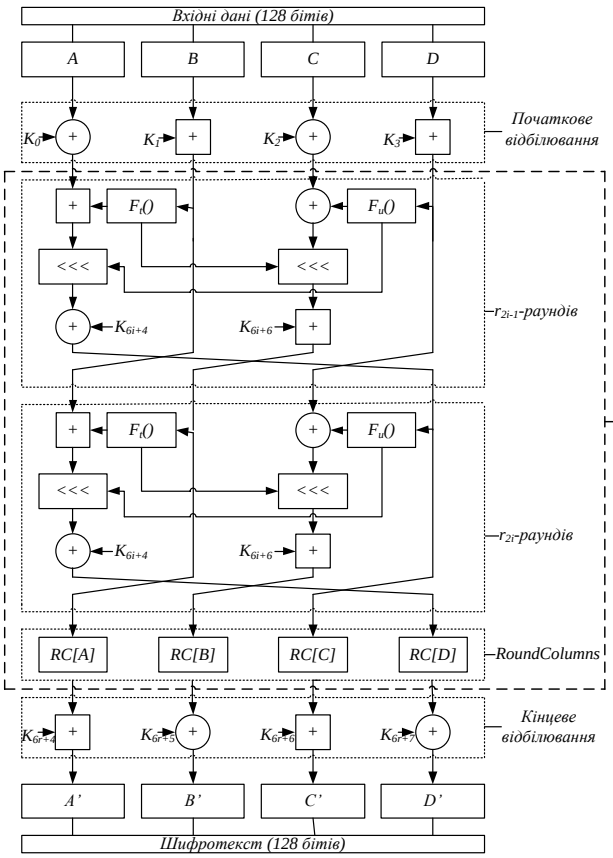

Рис. 1. Загальна схема роботи процедури зашифрування (**Fig. 1.** General scheme of encryption procedure)

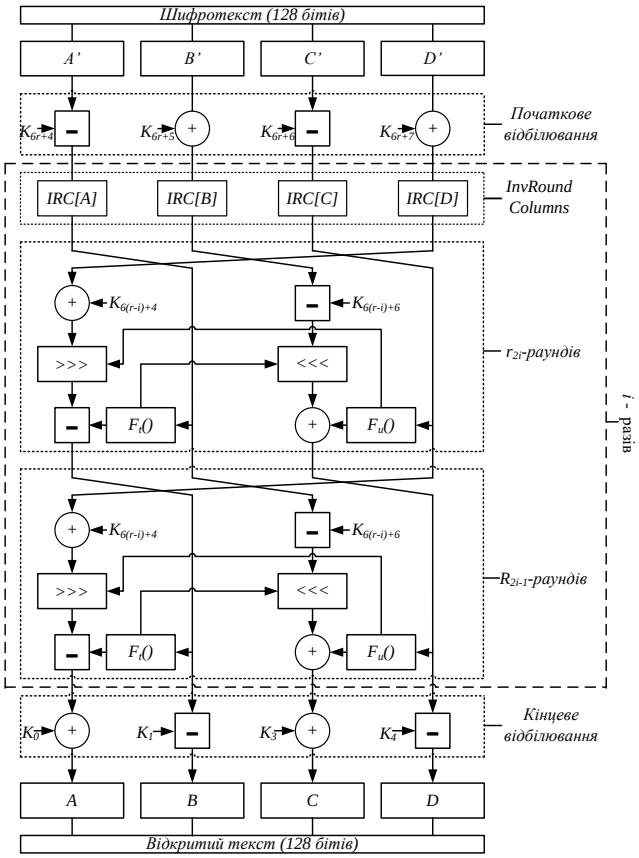

Рис. 2. Загальна схема роботи процедури розшифрування (**Fig. 2.** General scheme of decryption procedure)

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 такі етапи досліджень:

– лінійних перетворень;
– стійкості до диференціального криптоаналізу;
– стійкості до лінійного криптоаналізу;
–статистичної стійкості;
– 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 визначену кількість раз. 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. Саме стійкість до диференціального криптоаналізу розглянута у даній роботі.

Дослідження стійкості до лінійного криптоаналізу. Лінійний криптоаналіз 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 детальніше 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 порівняння швидкостей прототипу (оригіналу криптоалгоритму) та удосконаленого методу перетворення інформації береться програмне забезпечення криптоалгоритму та створюється програмне забезпечення його модифікації. А для проведення порівняльного аналізу швидкостей 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 диференціального криптоаналізу запропонованої функції гешування удосконаленого модуля криптографічного захисту в інформаційно-комунікаційних системах

Диференційний метод криптоаналізу був запропонований Е.Біхамом й А.Шаміром в 1990 р. Диференціальний криптоаналіз – це спроба розкриття секретного ключа блокових шифрів, які засновані на повторному застосуванні криптографічно слабкої цифрової операції шифрування *r* раз. 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.

Успіх таких спроб розкриття *r*-циклічного шифру залежить від існування диференціалів (*r*-1)-го циклу, які мають велику ймовірність. Диференціал *i*-го циклу визначається як пара $(a,b)_i$така, що пари різних відкритих текстів *x, x'* с різницею a може привести до пари вихідних текстів *y, y'* після *i*-ого циклу, що мають різницю b (для відповідного поняття різниці). Ймовірність *i*-циклового диференціала $(a,b)_i$- це умовна ймовірність $P\left(D_{y(i)} = b \mid D_x = a\right)$ того, що різниця $D_{y(i)}$ пари шифротекстів (y,y') після *i*-ого циклу дорівнює b за умови, що пара текстів (x,x') має різницю $D_x = a$; відкритий текст *x* і підключи циклів $k^{(1)}$, $k^{(2)}$,..., $k^{(i)}$ незалежні і рівно ймовірні.

Для блокових симетричних алгоритмів використовується диференціальний криптоаналіз, як один з найбільш універсальних та потужних видів атак на криптографічні шифри.

Для вираження результату проведення диференційного криптоаналізу використовується так званий критерій стійкості, який для *r*-циклічного SPN – шифру може бути представлений у вигляді такої нерівності:

$$P_{ДХ}^{(r-1)} \le 2^{-n}$$

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

Опишемо традиційний підхід до оцінки стійкості БСШ до диференціального криптоаналізу:

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 диференціальної характеристики. Для цього використовується два параметри:

a. кількість активних підстановок;

b. максимальна імовірність проходження ненульової різниці.

Через підстановку відбувається піднесення другого параметру до ступеня першого, тобто:

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

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

Розрахунок параметра підстановки $P_{D_{max}}$ проводиться за таким алгоритмом:

1. Побудова таблиці залежності вихідних різниць b від вхідних різниць a.

Таблиця різниці складається із значень:

$$e_s(a,b) = \#\{x \in GF(2^n) | S(x \oplus a) \oplus S(x) = b\}$$

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

– a – різниця між вхідними даними;

– b – різниця між даними після проходження *S*-блоків;

– x – змінна, що розраховує кількість разів коли рівність ставала істиною ($x \in GF(2^n)$, тобто приймає значення від 0 до 255);

– *S()* – блок підстановок.

2. Розрахунок максимальної імовірності проходження різниці, через підстановку $P_{D_{max}}$ розраховується за формулою:

$$P_{D_{max}} = \frac{\max\limits_{a \ne 0; b} e_s(a,b)}{2^n}$$

Провівши аналіз *S*-блоку алгоритму NRC21, побудована таблиця залежностей вихідних різниць b від вхідних різниць a (залежність b від a в *S*-блоці).

За таблицею залежностей вихідних різниць b від вхідних різниць a встановлено, що для всіх підстановок, які використовуються у шифрі NRC21 $P_{D_{max}} = 0{,}0234375$.

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

У табл. 1 виділені осередки, які визначають число циклів, при якому ймовірність диференціальної характеристики знаходиться нижче граничного значення. Дані, що представлені в табл. 1, дозволяють зробити висновок про стійкість до диференціального криптоаналізу шифру NRC21 з 128-бітним блоком, що містить 5 і більше циклів (10 і більше раундів).

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

Розмір блоку, біти	Число циклів							
	1	2	3	4	5	6	7	8
128	2^{-5}	2^{-41}	2^{-50}	2^{-121}	2^{-126}	2^{-162}	2^{-171}	2^{-243}

Висновки

У даній роботі наведено удосконалений 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 процесами. Для ефективного використання цього модуля важливим є вибір криптостійких методів шифрування 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 диференціального криптоаналізу запропонованої функції гешування удосконаленого модуля криптографічного захисту в інформаційно-комунікаційних системах. Проведене експериментальне дослідження підтвердило криптостійкість удосконаленого алгоритму до диференціального 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 Int. 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.

REFERENCES

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. Smirnova T.V., Hnatiuk S.O., Berdybaiev R.Sh., Burmak Yu.A., Ospanova D.M., «Udoskonalenyi modul kryptohrafich-noho zakhystu informatsii v suchasnykh informatsiino-komunikatsiinykh systemakh ta merezhakh». Kiberbezpeka: osvita, nauka, tekhnika. № 2(14). P. 176-185. 2021.
17. Smirnova T.V., Polishchuk L.I., Smirnov O.A., K.O. Buravchenko, A.O.Makevnin, «Doslidzhennia khmarnykh tekhnolohii yak servisiv», Kiberbezpeka: osvita, nauka, tekhnika. № 3(7). P. 43-62. 2020.
18. Smirnova T.V., Solovykh Ye.K., Smirnov O.A., Drieiev O.M., «Pobudova khmarnykh informatsiinykh tekhnolohii optymizatsii tekhnolohichnoho protsesu vidnovlennia ta zmitsnennia poverkhon detalei», Tsentralnoukrainskyi naukovyi visnyk. Te-khnichni nauky. № 1(32). P. 184-194, 2019
19. Smirnova, T.V., Smirnov, S.A., Mynailenko, R.M., Dorenskyi, O.P., Sysoienko S.V. «Khmarna avtomatyzovana systema intelektualnoi pidtrymky pryiniattia rishen dlia tekhnolohichnykh protsesiv». Visnyk Cherkaskoho derzhavnoho tekhnolo-hichnoho universytetu. Tekhnichni nauky. №4, 2020, P. 84-92.
20. Smirnova T.V., Buravchenko K.O., Kravchenko S.S., Horbov V.O., Smirnov O.A. «Khmarna systema pidtrymky pryiniattia rishen tekhnolohichnoho protsesu vidnovlennia poverkhon konstruktsii i detalei mashyn». Suchasni informatsiini systemy. 2021. T. 5, № 4. P. 79-95.

Received (Надійшла) 22.02.2022
Accepted for publication (Прийнята до друку) 11.05.2022

Investigation of resistance to differential cryptanalysis of the proposed hashing function of a perfect cryptographic protection module in information and communication systems

Tetiana Smirnova, Nataliia Yakymenko, Serhii Smirnov, Liudmyla Polishchuk, Oleksii Smirnov

Abstract. The object of the study is to ensure the confidentiality of data in information and communication systems for managing technological processes based on cloud technologies. **The subject** is the study of resistance to differential 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 differential cryptanalysis of the proposed hashing function of an improved cryptographic protection module 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, the study of resistance to differential cryptanalysis of the proposed function of hashing of the improved module of cryptographic protection in information and communication systems has been carried out. The conducted experimental study confirmed the cryptographic stability of the improved algorithm against differential 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 methods of encryption and hashing, 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 was made of the resistance to differential cryptanalysis of the proposed hashing function of an improved cryptographic protection module in information and communication systems. The conducted experimental study confirmed the cryptographic stability of the improved algorithm against differential cryptanalysis.

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