КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 3 (27), 2025
ISSN 2663 - 4023
DOI 10.28925/2663-4023.2025.27.752
УДК 004.056

Корнієць Віктор Анатолійович
Інститут проблем математичних машин і систем
Національної академії наук України, Київ, Україна
ORCID ID: 0000-0002-4967-8395
viktorkorniets@email.com

ОЦІНКА КРИПТОГРАФІЧНИХ ЯКОСТЕЙ МОДЕЛІ АВТЕНТИФІКАЦІЇ ДЖЕРЕЛА ДАНИХ НА ОСНОВІ ПОТОКОВОГО ШИФРУ

Анотація. У статті розглянуто проблеми і актуальні задачі застосування методики побудови на основі бітового потоку псевдовипадкових даних швидкісного імітостійкого шифру багато алфавітної заміни з одночасним формуванням коду автентифікації MAC. Вивчені питання оцінки достатності рівня безпеки його застосування у випадках реалізації загроз проведення зловмисником основних типів криптоаналітичних атак. Зокрема, проаналізована криптографічна стійкість щодо методів частотного аналізу, лінійного та диференціального аналізу, а також щодо атаки «зустріч посередині». На сформульоване питання надана доказово позитивна відповідь. Досліджуючи криптографічні властивості запропонованої моделі відмічене, що найбільш придатними для побудови вузлу накладання шифру є підстановки заміни, які мають певні структурні характеристики. На основі запропонованої криптографічної моделі побудовано захищений протокол реалізації процедури ідентифікацій «свій-чужий» (IFF) для мобільних об’єктів, включаючи роботизовані системи. Протокол враховує потенційну загрозу проведення криптоаналітичних атак типу «man in the middle» (MIM), для цього в рамках протоколу як додатковий фактор перевірки справжності ідентифікаційної інформації використовуються дані геолокації. Актуальність запропонованого рішення постійно зростає, що обумовлено широким застосуванням роботизованих систем в умовах воєнного часу та можливістю присутності в районах розташування об’єктів критичної інфраструктури «дружніх» БПЛА, які виконують різноманітні технічні функції. Окремим напрямом подальших досліджень в плані вдосконалення запропонованої криптографічної моделі є розв’язок задачі оцінки розподілу структурних характеристик випадкових підстановок заміни.

Ключові слова: код автентифікації повідомлення; MAC; кібербезпека; загроза; захист інформації; шифрування; конфіденційність; цілісність; імітостійкість; роботизована система; мережа зв’язку.

ВСТУП

Підтвердження справжності джерела походження даних і забезпечення їхньої цілісності та конфіденційності у процесі цифрового інформаційного обміну на об’єктах критичної інфраструктури може забезпечуватись різними методами. Найбільш поширеними механізмами, що реалізують відповідні функції та використовуються в системах кіберзахисту, є цифровий підпис або коди автентифікації повідомлень (Message Authentication Code — MAC[1]) [1] разом з шифруванням.

В автоматизованих системах, що обробляють державні інформаційні ресурси, а також в банківських інформаційних системах використовується кваліфікований електронний підпис, що створюється з використанням криптографічних засобів і базується на визначеному законодавством кваліфікованому сертифікаті електронного

[1] Іноді виникає непорозуміння, оскільки в мережних технологіях абревіатура MAC також означає Media Access Control — управління доступом до середовища, як унікальний ідентифікатор — адреса, що визначається для кожного типу активного обладнання в комп'ютерних мережах.

підпису [2]. Таке рішення є майже безальтернативним, якщо політика інформаційної безпеки організації базується на концепції повної недовіри (Zero Trust) [3].

Певними недоліками процедур із застосуванням засобів криптографічного захисту інформації, які реалізують кваліфікований цифровий підпис є доволі низька швидкість асиметричних перетворень та необхідність забезпечення доступу учасників захищеного інформаційного обміну до ресурсів третьої сторони — суб'єкта управління сертифікатами відкритих ключів — надавача електронних довірчих послуг [2].

Перший недолік цього способу — невисока продуктивність — частково може бути компенсований шляхом розробки та впровадження ефективних стандартів асиметричних криптоперетворень на еліптичних кривих, застосування швидкісних процесорів та оптимізації програмних кодів [4].

Розв'язок другої проблеми — безпечного застосування цифрового підпису — значно ускладняється, якщо вимоги щодо забезпечення конфіденційності даних у мережі захищеного інформаційного обміну значно вище, ніж у надавача електронних довірчих послуг. Зокрема, якщо захист інформації з обмеженим доступом в мережі забезпечується шляхом абонентського (наскрізного) шифрування, тоді завантаження сертифікатів відкритих ключів через незахищене середовище буде суперечити політиці безпеки, яка визначена для захищеного сегменту. Навіть перенесення на фізичному носії приватного ключу електронного підпису з системи його генерації, якщо вона фізично не включена в контур захисту мережі, може вважатись потенційно небезпечною.

Алгоритми формування кодів автентифікації повідомлень (MAC) є досить важливим компонентом захищених комунікаційних протоколів для забезпечення автентичності повідомлень, якими обмінюються дві або більше сторони транзакцій. Зокрема, MAC використовуються для автентифікації даних у протоколах IPsec та TLS (Transport Layer Security).

Щодо кодів автентифікації повідомлень (MAC) слід зауважити, що їх застосовування для автентифікації джерела даних та контролю їх цілісності поширене в інформаційних системах, в яких користувачі довіряють один одному та мають спільні секретні ключі симетричних криптоперетворень.

Особливе значення у плані забезпечення високої продуктивності системи обробки та передавання інформації має той факт, що у випадку обчислення MAC за допомогою симетричних блокових шифрів (CMAC) [5] або на основі хеш-функцій стійких до колізій (HMAC) [6], порівняно з асиметричними алгоритмами, забезпечується більш висока швидкість відповідних процедур їх формування та перевірки.

При цьому забезпечується сумісність з застосованою в системі політикою конфіденційності, яка реалізується шляхом, наприклад, наскрізного шифрування даних. Це надає можливість застосовувати коди автентифікації повідомлень для управління об'єктами Інтернету речей (IoT) [7], у швидкісних системах автоматизованого управління рухомими об'єктами, включаючи системи розпізнавання об'єктів «свій — чужий» (Identification Frend or Foe, IFF) [8], [9], для виявлення активних зловмисних атак, зокрема, таких що спрямовані на нав'язування хибної інформації, а також контролю наявності випадкових відхилень у даних, що обумовлені перешкодами у каналах зв'язку.

Доцільно звернути увагу, що в сучасних умовах роботизації певних галузей суспільного виробництва та військової справи набуває актуальності саме питання автентифікації джерела даних, забезпечення гарантованого розпізнавання об'єктів IFF, розв'язання проблем, що перебувають на поточний час на стадії уточнення завдань та пошуку ефективних рішень.

В [10], [11] запропоновані певні рішення визначених завдань на основі застосування імітостійких потокових шифрів, але, зрозуміло, що виходячи з оцінки практичної стійкості криптографічних систем на основі кращого за ефективністю методу криптоаналізу, дослідження щодо підвищення безпеки їх застосування мають бути продовжені. Зокрема, в [11] сформульована задача оцінки швидкості сходження модульних сум випадкових величин на абелевих групах до рівномірного розподілу ймовірностей.

Виходячи з викладеного уявляється доцільним проаналізувати поточну ситуацію та визначити напрями покращення методів та технологій автентифікації джерел даних та забезпечення їх конфіденційності та цілісності на основі застосування швидкісних імітостійких потокових шифрів.

Постановка проблеми. Запропонована в [11] методика формування швидкісного імітостійкого шифру багато алфавітної також визначає механізм формування MAC з використанням швидкісного імітостійкого шифру, постають актуальні питання чи достатнім є рівень його безпеки проти різноманітних криптоаналітичних атак та яким чином можна застосувати запропонований криптомеханізм для розв'язку проблеми IFF для роботизованих систем.

Аналіз останніх досліджень і публікацій. Побудова криптографічної схеми, що реалізує шифр багатоалфавітної заміни (БАЗ) використовуючи алгоритм генерації підстановок заміни на базі псевдовипадкової послідовності, вперше запропонована в [15]. В роботі з метою забезпечення гарантоздатності автоматизованих систем управління безпілотними літальними апаратами також запропоновано модуль виявлення атак на криптосистему.

Подальшого розвитку пропозиція застосування шифру багатоалфавітної заміни набула в [13], де запропонована модифікація потокового криптоалгоритму A5/1 для застосування в мережах IoT на пристроях з обмеженими обчислювальними ресурсами. У запропонованому рішенні усунені основні недоліки алгоритму, а саме підвищена стійкість за рахунок збільшення довжину ключа та підвищена імітостійкість, завдяки застосування додаткового секретного параметру — блока підстановок заміни. Певним недоліком схеми є фіксоване значення блока заміни.

Запропонована в [11] методика формування швидкісного імітостійкого шифру БАЗ також визначає механізм формування MAC з використанням швидкісного імітостійкого шифру. Щодо вказаної схеми постають актуальні питання чи достатнім є рівень його безпеки проти різноманітних криптоаналітичних атак та яким чином можна застосувати запропонований криптомеханізм для розв'язку проблеми IFF для роботизованих систем.

Метою статті є формальне доведення криптографічних якостей моделі автентифікації джерела даних на основі потокового шифру та формування на її основі протоколу ідентифікації об'єктів роботизованих систем нового покоління.

МЕТОДОЛОГІЧНІ ЗАСАДИ ДОСЛІДЖЕННЯ

З метою оцінки якості шифрування даних спочатку уявляється доцільним проаналізувати ймовірнісні властивості сум випадкових величин, що приймають значення в кінцевій адитивній абелевій групі.

Для довільного натурального $n \in \{2,3,\dots\}$ позначимо адитивну групу кільця лишків за модулем n як $\boldsymbol{Z}_n = \{0,1,\dots,n-1\}$.

ISSN 2663 - 4023

Позначимо, $ax = \underbrace{x + x + \cdots + x}_{a}$, де $a, x \in \boldsymbol{Z}_n \backslash \{0\}$.

Якщо $a = 0$ або $x = 0$ тоді $ax = 0$.

Будемо називати характером групи [12] $\boldsymbol{Z}_n$ функцію $\chi_\alpha(x), \alpha, x \in \boldsymbol{Z}_n$, яка приймає значення у полі комплексних чисел $\boldsymbol{C}$ та визначається виразом:

$$\chi_\alpha(x) = e^{\frac{2\pi i \alpha x}{n}}, \text{де } i^2 = -1 . \quad (1)$$

Безпосередньо з визначення характеру (1) випливає співвідношення ортогональності:

$$\sum_{\alpha \in \boldsymbol{Z}_n} \chi_\alpha(x)\overline{\chi_\alpha(y)} = n\delta_{x,y},\ x, y \in \boldsymbol{Z}_n, \quad (2)$$

де $\overline{\chi_\alpha(y)}$ — число, яке комплексно спряжене до $\chi_\alpha(y)$, $\delta_{x,y}$ — символ Кронекера.

Для будь-якої функції $f: \boldsymbol{Z}_n \to \boldsymbol{C}$ позначимо $\hat{f}$ її дискретне перетворення Фур'є [13], [14]:

$$\hat{f}(\alpha) = \sum_{x \in \boldsymbol{Z}_n} f(x)\chi_\alpha(x),\ \alpha \in \boldsymbol{Z}_n. \quad (3)$$

Використовуючи співвідношення ортогональності (2) можна отримати обернення для перетворення Фур'є [13], [14]:

$$f(x) = n^{-1} \sum_{\alpha \in \boldsymbol{Z}_n} \hat{f}(\alpha)\overline{\chi_\alpha(x)},\ \alpha \in \boldsymbol{Z}_n. \quad (4)$$

Нехай $\xi_1, \ldots, \xi_m$ — незалежні випадкові величини що приймають значення на групі $\boldsymbol{Z}_n$ згідно законів розподілу $p_1, \ldots, p_m$ відповідно:

$$p_i(x) = Pr(\xi_i = x),\ x \in \boldsymbol{Z}_n,\ i \in \overline{1, m}. \quad (5)$$

Позначимо $\hat{p}_i$ перетворення Фур'є функції p_i. З наведених означень випливає, що $\hat{p}_i(0) = 1$, $|\hat{p}_i(\alpha)| \leq 1$ для будь-якого $\alpha \in \boldsymbol{Z}_n$.

Будемо називати розподіл p_i *прийнятним*, якщо $|\hat{p}_i(\alpha)| < 1$ для будь якого $\alpha \in \boldsymbol{Z}_n \backslash \{0\}$, $i \in \overline{1, m}$.

Позначимо

$$\theta = \max_{\substack{1 \leq i \leq m, \\ \alpha \in \boldsymbol{Z}_n \backslash \{0\}}} \{ |\hat{p}_i(\alpha)| \}. \quad (6)$$

Твердження. Для будь-якого $x \in \boldsymbol{Z}_n$ справедлива нерівність[2]:

$$|\, Pr(\xi_1 + \ldots + \xi_m = x) - n^{-1}| \leq \theta^m \quad (7)$$

Наслідок. Якщо всі розподіли ймовірностей $p_1, \ldots, p_m$ є прийнятними, то розподіл суми випадкових величин $\xi_1, \ldots, \xi_m$ збігається до рівномірного розподілу на групі $\boldsymbol{Z}_n$ при $m \to \infty$.

Доведення. Використовуючи (5) переконаємося, що виконується рівність:

$$\hat{p}(\alpha) = \hat{p}_1(\alpha) \cdots \hat{p}_m(\alpha),\ \alpha \in \boldsymbol{Z}_n. \quad (8)$$

Дійсно, за означенням перетворення Фур'є (3) та використовуючи формулу повної ймовірності отримуємо:

$$\hat{p}(\alpha) = \sum_{x \in \boldsymbol{Z}_n} p(x)\chi_\alpha(x) = \sum_{x \in \boldsymbol{Z}_n} \sum_{\substack{(x_1, \ldots, x_m) \in \boldsymbol{Z}_m^n: \\ x_1 + \ldots + x_m = x}} p_1(x_1) \cdots p_m(x_m)\chi_\alpha(x) =$$

[2] Тут операція «+» для випадкових величин позначає додавання в групі $\boldsymbol{Z}_n$.

$$= \sum_{x \in \boldsymbol{Z}_n} \sum_{\substack{(x_1,\dots,x_m) \in \boldsymbol{Z}_m^n: \\ x_1+\dots+x_m=x}} p_1(x_1) \cdots p_m(x_m)\chi_\alpha(x_1) \cdots \chi_\alpha(x_m) =$$

$$= \sum_{(x_1,\dots,x_m) \in \boldsymbol{Z}_m^n} p_1(x_1) \cdots p_m(x_m)\chi_\alpha(x_1) \cdots \chi_\alpha(x_m) = \hat{p}_1(\alpha) \cdots \hat{p}_m(\alpha),$$

тобто рівність (8) доведено.

Далі, використовуючи нерівність (7) та вираз для обернення перетворення Фур'є (4), отримаємо, що:

$$p(x) - n^{-1} = n^{-1} \sum_{\alpha \in \boldsymbol{Z}_n} \hat{p}(\alpha)\overline{\chi_\alpha(x)} - n^{-1} = n^{-1} \sum_{\alpha \in \boldsymbol{Z}_n \setminus \{0\}} \hat{p}(\alpha)\overline{\chi_\alpha(x)} =$$
$$= n^{-1} \sum_{\alpha \in \boldsymbol{Z}_n \setminus \{0\}} \hat{p}_1(\alpha) \cdots \hat{p}_m(\alpha)\overline{\chi_\alpha(x)}, x \in \boldsymbol{Z}_n.$$

Отже,

$$|p(x) - n^{-1}| \le n^{-1} \sum_{\alpha \in \boldsymbol{Z}_n \setminus \{0\}} |\hat{p}_1(\alpha)| \cdots |\hat{p}_m(\alpha)| \le n^{-1}(n-1)\theta^m \le \theta^m.$$

Твердження доведено.

Надалі, розглянемо модель вузлу накладання імітостійкого шифру з формуванням коду автентифікації повідомлення, що побудована на основі запропонованої в [11] методики побудови вузлу накладання шифру на базі методології побудови роторних систем.

Модель імітостійкого шифрування даних та генерування MAC складається з декількох раундів, що виконуються циклічно (рис. 1).

Першим кроком моделі є доповнення повідомлення для кратності 32 біти. Можливо відмітити, що вирівнювання довжин повідомлень по межам, які кратні 32 бітам, відповідає рекомендаціям [15] в плані покращення резистентності шифрування щодо атак типу визначення стану об'єкту.

Наступні кроки виконуються для векторів даних довжиною 32 біти, що розглядаються як послідовність восьми 4-х бітових чисел

$$\overline{D}_i = d_i \parallel d_{i+1} \parallel \cdots \parallel d_{i+7}, i = 1,2, \dots \quad (9)$$

де $\parallel$ — операція конкатенації 4-х бітових комбінацій.

В межах одного раунду перетворення (рис. 1, блоки 3–11) відбувається:

1. Формування за допомогою потокового шифру [17] 4×8+4×16=96 біт векторів параметрів шифрування:

$$\overline{\Lambda}_i = (\lambda_i, \lambda_{i+1}, \dots, \lambda_{i+7}) \quad (10)$$

$$\overline{\mathrm{M}}_i = (\mu_i, \mu_{i+1}, , \dots, \mu_{i+15}) \quad (11)$$

2. Шифрування вектору даних $\overline{D}_i$ (8) за допомогою 32-х біт вектору параметрів $\overline{\Lambda}_i$ (рис. 1, блок 7)**:**

$$s_{i+l} = d_{i+l} + \lambda_{i+l} \, mod \, 2^4, l = \overline{0,7} \quad (12)$$

Зауваження. Вихідна послідовність потокового шифру, який запропонований в [17], за ймовірнісно-статистичними характеристиками не відрізняється від рівномірного розподілу, а це визначатиме відповідні характеристики величин s_{i+l} в рівнянні (12).

3. Наступне перетворення вектору $\bar{S}_i = s_i \parallel s_{i+1} \parallel \cdots \parallel s_{i+7}$ описується (рис. 1, блок 9) рівнянням роторного типу за допомогою 16-ти підстановок заміни $\{X^{(0)}, X^{(1)}, \dots, X^{(15)}\}$:

$$\bar{W}_i = \prod_{j=0}^{15} C_{-\mu_{i+j}} \cdot X^{(j)} \cdot C_{\mu_{i+j}}(\bar{S}_i) \quad (13)$$

де C_μ — шифр Цезаря з параметром μ:

$$C_\mu = \begin{pmatrix} 0 & 1 & \cdots & 15 \\ 0+\mu & 1+\mu & \cdots & 15+\mu \end{pmatrix} = \begin{pmatrix} i \\ i+\mu \bmod 2^4 \end{pmatrix}_{i=\overline{0,15}}.$$

$X^{(j)}, j = \overline{0,15}$ — підстановки заміни, що можуть бути подані у наступному вигляді:

$$X^{(j)} = \begin{pmatrix} 0 & 1 & \cdots & 15 \\ 0+\delta_0^{(j)} & 1+\delta_1^{(j)} & \cdots & 15+\delta_{15}^{(j)} \end{pmatrix} = \begin{pmatrix} i \\ i+\delta_i^{(j)} \bmod 2^4 \end{pmatrix}_{i=\overline{0,15}}.$$

Якщо скористатись введеними позначеннями з урахуванням зауваження до рівняння (12) рівняння шифрування (13) може бути згідно [17] записане в еквівалентній формі для 4-х бітових чисел $\bar{s}_k, \overline{w}_k$, а саме:

$$\overline{w}_k = \bar{s}_k + \delta_\alpha^{(0)} + \delta_\beta^{(1)} + \delta_\gamma^{(2)} + \cdots + \delta_\xi^{(15)} \bmod 2^4, \qquad (14)$$

де $\alpha, \beta, \gamma, \ldots, \xi$ — випадкові значення індексів, що приймають значення на абелевій групі $\boldsymbol{Z}_{16}$.

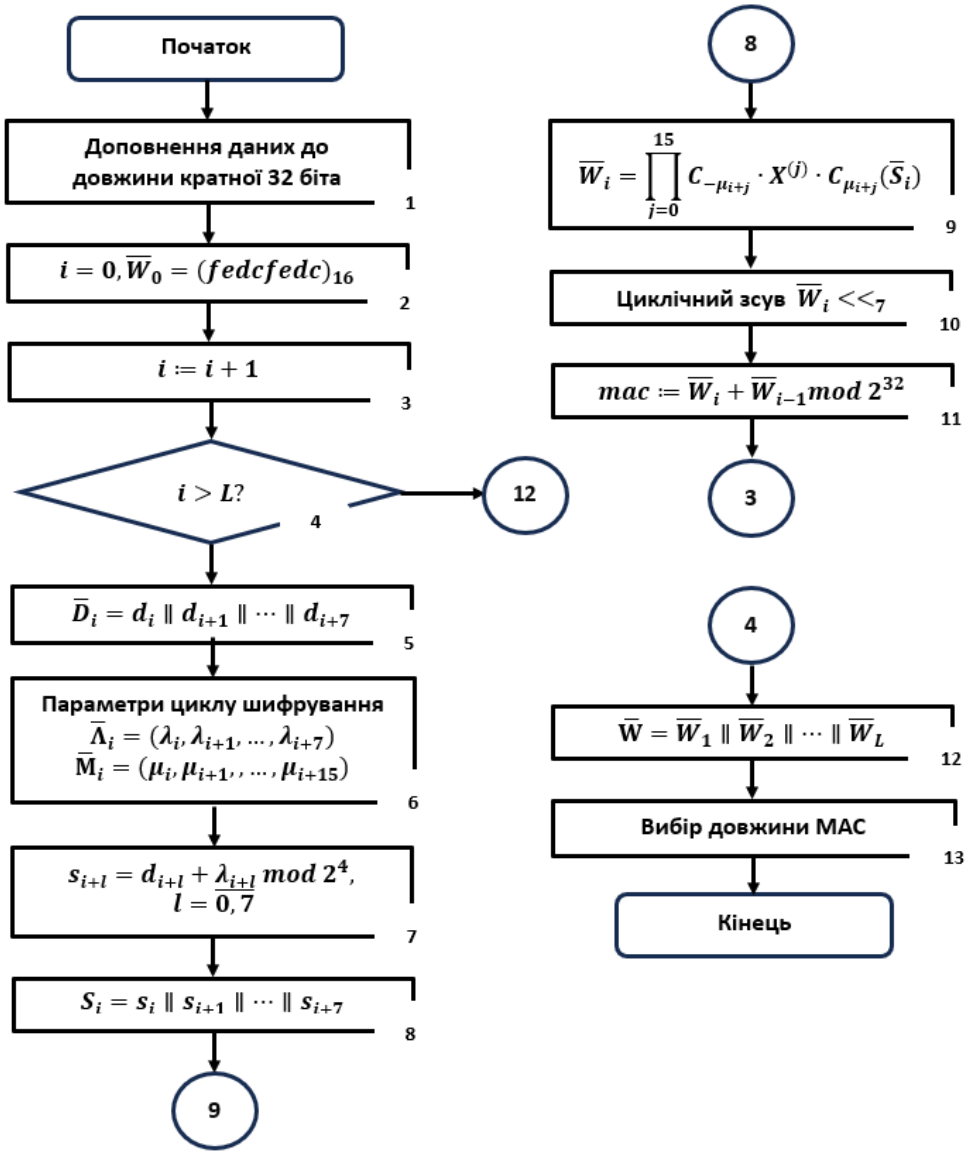

Рис. 1. Модель імітостійкого шифру та формування MAC

У визначених умовах можна скористатись висновками твердження (7) щодо наближення розподілу суми випадкових величин до рівномірного наступним чином:

$$|\,Pr(\,\delta_{\alpha}^{(0)} + \delta_{\beta}^{(1)} + \delta_{\gamma}^{(2)} \ldots + \delta_{\xi}^{(15)} = x) - 2^{-4}|\ \leq \theta^{16}. \tag{15}$$

Нескладно бачити, що у випадку для якщо всіх підстановок $\{X^{(0)}, X^{(1)}, \ldots, X^{(15)}\}$ виконується нерівність:

$$\delta_k^{(j)} \neq \delta_l^{(j)}, \text{для } k \neq l, \forall j = \overline{0,15} \tag{16}$$

тоді забезпечується максимальне розсіювання та величина θ набуває мінімального значення $\theta_{min} = 2^{-4} = 0{,}0625$.

У випадку підстановки, для якої спостерігається Q — кратний збіг:

$$\overbrace{\delta_k^{(j)} = \delta_l^{(j)} = \cdots = \delta_n^{(j)}}^{Q} \tag{17}$$

де $Q \geq 2$ та усі індекси $\{k, l, \ldots, n\}$ попарно різні, для оцінки (15) з урахуванням визначення в (6) величини θ отримуємо наступне значення:

$$\theta = Q \cdot \theta_{min} \tag{18}$$

При цьому якість розсіювання по К. Шеннону [18] погіршується. Це означає, що в запропонованій моделі імітостійкого шифрування (рис. 1) потрібно забезпечити максимальне наближення набору підстановок $\{X^{(0)}, X^{(1)}, \ldots, X^{(15)}\}$ до виконання умови (16) для уникнення атак частотного аналізу.

Слід відмітити, що підстановки з властивістю, що визначена сукупністю нерівностей (16), для деяких їх степенів взагалі не існують, а генерація підстановок з мінімальною кількістю співпадінь Q у випадку достатньо великої їх степені є доволі складною обчислювальною задачею.

Тому виникає питання яка кількість співпадінь Q (17) є припустимою для якісної у криптографічному сенсі підстановки? Проведені в цьому напряму розрахунки наведені в табл. 1.

Таблиця 1

Розрахунок максимальної імовірності θ^m залежно від значень параметрів Q, m

Значення		**Значення імовірності θ^m для кількості підстановок в системі, m**			
Q	θ	2	4	8	16
2	0.125	$1.6\cdot10^{-2}$	$2.4\cdot10^{-4}$	$6.0\cdot10^{-8}$	$3.6\cdot10^{-15}$
3	0.1875	$3.5\cdot10^{-2}$	$1.2\cdot10^{-3}$	$1.5\cdot10^{-6}$	$2.3\cdot10^{-12}$
4	0.25	$6.3\cdot10^{-2}$	$3.9\cdot10^{-3}$	$1.5\cdot10^{-5}$	$2.3\cdot10^{-10}$
5	0.3125	$9.8\cdot10^{-2}$	$9.5\cdot10^{-3}$	$9.1\cdot10^{-5}$	$8.3\cdot10^{-9}$
6	0.375	$1.4\cdot10^{-1}$	$2.0\cdot10^{-2}$	$3.9\cdot10^{-4}$	$1.5\cdot10^{-7}$
7	0.4345	$1.9\cdot10^{-1}$	$3.7\cdot10^{-2}$	$1.3\cdot10^{-3}$	$1.8\cdot10^{-6}$
8	0.5	$2.5\cdot10^{-1}$	$6.3\cdot10^{-2}$	$3.9\cdot10^{-3}$	$1.5\cdot10^{-5}$

Аналізуючи дані що наведені в табл. 1 можливо відстежити швидкість сходження розподілу сум випадкових величин до рівномірного розподілу залежно від кількості підстановок заміни в рівнянні (13). При цьому варіант $m = 16$ забезпечує достатньо високі якості порівняно з вимогами до генерації криптографічних ключів [19].

Також слід зазначити, що на підставі даних таблиці однозначно слід відхилити схеми, що включають лише 2 або 4 підстановки, як такі що не забезпечують належних характеристик вирівнювання розподілу сум випадкових величин в (14). Також з аналогічних міркувань не слід застосовувати підстановки $\{X^{(0)}, X^{(1)}, \dots, X^{(15)}\}$, для яких індекс співпадінь $Q > 4$.

Досліджуючи криптографічні властивості запропонованої моделі можливо відмітити що її особливість полягає у псевдовипадковому формуванні підстановок заміни, що їх добуток змінюється не тільки при кожній зміні секретного ключа, а й при переході від шифрування одного вектору даних до другого. Цей фактор, що блок замін випадково залежить від ключа та постійно змінюється залежно від вектору $\overline{\mathrm{M}}_i$ підвищує його резистентність щодо можливості застосування методів лінійного та диференціального криптоаналізу, які базуються на формуванні відповідних рівнянь на основі властивостей відомих фіксованих блоків заміни.

Також слід відмітити, що вибір кількості підстановок заміни $m = 16$ знижує ризик реалізації атаки типу «зустріч посередині» [1], оскільки блок замін потребує для розшифрування за допомого всіх варіантів вектору $\overline{\mathrm{M}}_i$

$$|\{(\mu_i, \mu_{i+1}, , \dots, \mu_{i+15}), \mu_{i+k} = 0{,}1\}| = 2^{64} = 10^{64 \log_{10} 2} \approx 10^{19}$$

комірок пам'яті прямого доступу для зберігання проміжних результатів. В найгіршому випадку успіх атаки зустріч посередині може дати лише інформацію про вектор $\overline{\Lambda}_i = (\lambda_i, \lambda_{i+1}, \dots, \lambda_{i+7})$ та вектор $\overline{\mathrm{M}}_i = (\mu_i, \mu_{i+1}, , \dots, \mu_{i+15})$, що визначаються секретним ключем стійкого алгоритму потокового шифрування.

4. Продовжуючи аналіз моделі імітостійкого шифру та формування MAC звернемо увагу, що заключні перетворення раунду (рис. 1, блоки 10, 11) забезпечують переміщування шляхом циклічного зсуву та розсіювання завдяки додаванню за модулем 2^{32} $(mod\ 2^{32})$ з попереднім значенням згортки для рекурсивного утворення коду автентифікації повідомлення. В якості нульового (початкового) вектору рекурсивної процедури обрана константа $\overline{W}_0 = (fedcfedc)_{16}$.

Надалі виконання раундів продовжується до завершення даних та здійснюється перехід до остаточно оформлення шифрованого повідомлення та коду автентифікації (рис. 1, блоки 12, 13).

Криптографічна стійкість створюваного коду автентифікації за методом повного перебору оцінюється по довжині коду як $O(2^{32})$, по довжині ключу шифрування $O(2^{256})$.

Таким чином маємо математичне обґрунтування резистивності запропонованої криптографічної моделі щодо атак частотного аналізу, лінійного та диференціального аналізу, а також атаки «зустріч посередині».

Хороші швидкісні характеристики та криптографічні якості запропонованої моделі надають можливість побудувати безпечний протокол ідентифікації IFF для роботизованих систем.

Безпеку протоколу доцільно забезпечити на основі спільного для учасників процедури ідентифікації секретного ключу симетричної криптографічної системи, що вище описана в рамках аналіза відповідної моделі.

Позначимо наступні елементи криптографічного протоколу:

Hello — стандартне початкове повідомлення для початку процедури ідентифікації;

$E_K(M)$ — результат зашифрування імітостійким шифром даних M за допомогою спільного секретного ключу K;

$mac_K(M)$ — код автентифікації повідомлення, створений за запропонованою схемою (рис. 1) з допомогою спільного секретного ключу;

R — випадкове число, яке використовується одноразово та щоразу генерується ініціатором процедури ідентифікації;

A — випадкове число, яке використовується одноразово та щоразу генерується відповідачем в процедурі ідентифікації;

GP_R — геолокаційні дані ініціатора процедури ідентифікації;

GP_A — геолокаційні дані відповідача в процедурі ідентифікації;

T — час (по таймеру системи) початку процедури ідентифікації.

В табл. 2 наведена покрокова загальна схема протоколу IFF з використанням моделі імітостійкого шифрування та формування MAC

Таблиця 2

Загальна схема протоколу IFF з використанням моделі імітостійкого шифрування та формування MAC

№	Ініціатор	Відповідач	№
1	Hello	Генерує A, визначає T, формує та надсилає $E_K(A \parallel T) \parallel mac_K(A \parallel T)$	1
2.	Розшифровує отримане та перевіряє $E_K(A \parallel T) \parallel mac_K(A \parallel T)$, генерує R, Формує та надсилає відповідачу $E_K(R \parallel A \parallel T) \parallel mac_K(R \parallel A \parallel T)$.	Розшифровує отримане та перевіряє $E_K(R \parallel A \parallel T) \parallel mac_K(R \parallel A \parallel T)$, формує та надсилає ініціатору $E_K(GP_A \parallel R \parallel A \parallel T) \parallel \parallel mac_K(GP_A \parallel R \parallel A \parallel T)$	2
3.	Розшифровує отримане та перевіряє $E_K(GP_A \parallel R \parallel A \parallel T) \parallel \parallel mac_K(GP_A \parallel R \parallel A \parallel T)$ Формує та надсилає відповідачу $E_K(GP_R \parallel GP_A \parallel R \parallel A \parallel T) \parallel \parallel mac_K(GP_R \parallel GP_A \parallel R \parallel A \parallel T)$	Розшифровує отримане та перевіряє $E_K(GP_R \parallel GP_A \parallel R \parallel A \parallel T) \parallel \parallel mac_K(GP_R \parallel GP_A \parallel R \parallel A \parallel T)$	3.

1. Після ініціації процесу IFF на другому кроці процедури ініціатор після отримання відповіді розшифровує її та перевіряє цілісність за допомогою коду автентифікації. Внаслідок цього він отримує випадкове число відповідача A та час початку процедури T (це важливо для попередження атак «Man In the Middle» — MIM). У відповідь він надсилає повідомлення яке додатково до попередньої інформації містить його власне випадкове число.

2. Відповідач на другому кроці процедури розшифрував та перевірив цілісність отриманого повідомлення отримує власне випадкове число та випадкове число ініціатора, що підвищує його впевненість в легітимності процедури. Далі він додає свої геолокаційні дані для перевірки їх ініціатором та нове зашифроване повідомлення надсилає ініціатору.

3. Ініціатор після отримання чергової відповіді розшифровує її, перевіряє цілісність бачить власне випадкове число та дані геолокації, які використовує для додаткової перевірки (це також важливо для попередження атак MIM). Після чого він у новому повідомленні додає власні дані геолокації та надсилає їх відповідачу на цьому він закінчує процедуру IFF. Відповідач розшифровує та перевіряє цілісність отриманого і також закінчує процедуру IFF.

Процедура, за необхідності, може включати обмін особистими ідентифікаторами об’єктів ідентифікації, що може додатково сприяти підвищенню довіри до результатів її виконання.

З урахуванням особливостей застосованих каналів зв'язку, їх швидкодії та захисту від перешкод час на відповідь може обмежуватись, що контролюється за допомогою відмітки часу початку процедури IFF.

Для виключення загрози подвійного шифрування на одному ключі кожне повідомлення шифрується із застосуванням вектору ініціалізації (синхромаркеру).

ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

У роботі розглянуті проблеми і актуальні задачі застосування запропонованої в [11] методики формування швидкісного імітостійкого шифру багато алфавітної заміни з одночасним формуванням коду автентифікації MAC на основі потокового шифру, включаючи питання оцінки достатності рівня безпеки його застосування у випадках реалізації основних типів криптоаналітичних атак. На сформульоване питання надана доказово позитивна відповідь.

З використанням запропонованої криптографічної моделі побудовано протокол реалізації процедури IFF для роботизованих систем, який враховує потенційну загрозу проведення криптоаналітичних атак типу «man in the middle».

Актуальність запропонованого рішення постійно зростає, що обумовлено широким застосуванням роботизованих систем в умовах воєнного часу.

Окремим напрямом подальших досліджень, який викликає значний інтерес в плані вдосконалення запропонованої криптографічної моделі, становить задача оцінки розподілу структурних характеристик випадкових підстановок заміни.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Horbenko, I. D, & Horbenko, Yu. I. (2012). *Applied cryptology: Theory. Practice. Application: monograph.* Kharkiv: "Fort".
2. On Electronic Trust Services, Law of Ukraine № 2155-VIII (2024) (Ukraine). https://zakon.rada.gov.ua/laws/show/2155-19#Text
3. Vorokhob, M., Kyrychok, R., Yaskevych, V., dobryshyn, y., & sydorenko, s. (2023). Modern perspectives of applying the concept of zero trust in building a corporate information security policy. *Electronic Professional Scientific Journal «Cybersecurity: Education, Science, Technique», 1(21),* 223–233. https://doi.org/10.28925/2663-4023.2023.21.223233
4. Horbenko, Yu. I. (2015). *Construction and analysis of systems, protocols and means of cryptographic information protection: monograph - Part 1: Methods of construction and analysis. standardization and application of cryptographic systems.* Kharkiv: "Fort".
5. *Information technology -- Security techniques -- Message Authentication Codes (MACs) -- Part 1: Mechanisms using a block cipher* (ISO/IEC 9797-1:2011). (2011).
6. *Information security — Message authentication codes (MACs) – Part 2: Mechanisms using a dedicated hash-function* (ISO/IEC 9797-2:2021). (2021)
7. Chernenko, R. (2023). Performance evaluation of lightweight cryptography algorithms on constrained 8-bit devices. *Electronic Professional Scientific Journal «Cybersecurity: Education, Science, Technique», 1(21).* https://doi.org/10.28925/2663-4023.2023.21.273285
8. Bowden, L. (1985). The story of IFF (identification friend or foe). *IEE Proceedings A - Physical Science, Measurement and Instrumentation, Management and Education, Reviews. 132(6),* 435–437.
9. Alferov, O. P., et al. (2001). *Fundamentals of cryptography.* Helios ARV.
10. Hulak, H. M., & Skladannyi, P. M. (2017). Ensuring the reliability of automated control and data transmission systems for unmanned aerial vehicles. *Mathematical machines and systems, 3,* 154–161.
11. Korniiets, V., & Zhdanova Y. (2024). Methodology for forming a high-speed imitator-resistant cipher for multi-alphabet substitution. *Electronic Professional Scientific Journal «Cybersecurity: Education, Science, Technique», 2(26),* 476–486. https://doi.org/10.28925/2663-4023.2024.26.723

12. Chandrasekharan, K. (2012). *Introduction to Analytic. Number Theory*. Springer-Verlag. Berlin Heidelberg New York.
13. Oleksiichuk, A. M., Koniushok, S. M. (2012). *Fourier transforms and cryptographic properties of Boolean functions.* K.: ISZZI NTUU "KPI".
14. Marks II, R. J. (2009). *Handbook of Fourier Analysis & Its Applications.* Oxford: Oxford University Press.
15. Hulak, H., Zhdanova Y., Skladannyi, P., Hulak, Y., & Korniiets, V. (2022). Vulnerabilities of short message encryption in mobile information and communication systems of critical infrastructure objects. *Electronic Professional Scientific Journal «Cybersecurity: Education, Science, Technique», 1(17),* 145–158. https://doi.org/10.28925/2663-4023.2022.17.145158
16. Korniiets, V., & Chernenko, R. (2023). Modification of the cryptographic algorithm a5/1 to ensure communication for iot devices. *Electronic Professional Scientific Journal «Cybersecurity: Education, Science, Technique», 4(20),* 253–271. https://doi.org/10.28925/2663-4023.2023.20.253271
17. Konheim, A. G. (1981). *Cryptography: A prime.* Wiley & Sons, Incorporated, New York.
18. Shannon, C. E. (1950) *Communication Theory of Secrecy Systems.* Bell Telephone Laboratories, Incorporated, New York.
19. Chernenko, R. (2023). Generation of pseudorandom sequences on microcontrollers with limited computational resources, entropy sources, and statistical properties testing. *Electronic Professional Scientific Journal «Cybersecurity: Education, Science, Technique», 2(22),* 191–203. https://doi.org/10.28925/2663-4023.2023.22.191203
20. Hulak, H. M., Zhiltsov, O. B., Kyrychok, R. V., Korshun, N. V., & Skladannyi, P. M. (2024). *Information and cyber security of the enterprise. Textbook.* Lviv: Publisher Marchenko T. V.

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 3 (27), 2025
ISSN 2663 - 4023

Viktor Korniets
Institute of Problems of Mathematical Machines and Systems of the
National Academy of Sciences of Ukraine, Kyiv, Ukraine
ORCID ID: 0000-0002-4967-8395
viktorkorniets@email.com

EVALUATION OF THE CRYPTOGRAPHIC QUALITIES OF A DATA SOURCE AUTHENTICATION MODEL BASED ON A STREAM CIPHER

Abstract. The article considers the problems and actual tasks of applying the methodology for constructing a high-speed imitation-resistant multi-alphabet substitution cipher based on a bit stream of pseudorandom data with simultaneous generation of a MAC authentication code. The issues of assessing the adequacy of the security level of its application in cases of realization of threats of the main types of cryptanalytic attacks by an attacker are studied. In particular, the cryptographic resistance to frequency analysis, linear and differential analysis, as well as to the "meeting in the middle" attack is analyzed. The question is provably answered positively. Investigating the cryptographic properties of the proposed model, it is noted that the most suitable for building a cipher overlay node are substitution substitutions that have certain structural characteristics. On the basis of the proposed cryptographic model, a secure protocol for implementing the friend-or-foe (IFF) identification procedure for mobile objects, including robotic systems, is built. The protocol takes into account the potential threat of man-in-the-middle (MIM) cryptanalytic attacks, for which purpose geolocation data is used as an additional factor in verifying the authenticity of identification information. The relevance of the proposed solution is constantly growing, due to the widespread use of robotic systems in wartime and the possibility of the presence of "friendly" UAVs performing various technical functions in the areas where critical infrastructure facilities are located. A separate direction for further research in terms of improving the proposed cryptographic model is to solve the problem of estimating the distribution of structural characteristics of random substitutions.

Keywords: message authentication code; MAC; cybersecurity; threat; information security; encryption; confidentiality; integrity; imitation resistance; robotic system; communication network.

REFERENCES (TRANSLATED AND TRANSLITERATED)

1. Horbenko, I. D, & Horbenko, Yu. I. (2012). *Applied cryptology: Theory. Practice. Application: monograph.* Kharkiv: "Fort".
2. On Electronic Trust Services, Law of Ukraine № 2155-VIII (2024) (Ukraine). https://zakon.rada.gov.ua/laws/show/2155-19#Text
3. Vorokhob, M., Kyrychok, R., Yaskevych, V., dobryshyn, y., & sydorenko, s. (2023). Modern perspectives of applying the concept of zero trust in building a corporate information security policy. *Electronic Professional Scientific Journal «Cybersecurity: Education, Science, Technique», 1(21),* 223–233. https://doi.org/10.28925/2663-4023.2023.21.223233
4. Horbenko, Yu. I. (2015). *Construction and analysis of systems, protocols and means of cryptographic information protection: monograph - Part 1: Methods of construction and analysis. standardization and application of cryptographic systems.* Kharkiv: "Fort".
5. *Information technology -- Security techniques -- Message Authentication Codes (MACs) -- Part 1: Mechanisms using a block cipher* (ISO/IEC 9797-1:2011). (2011).
6. *Information security — Message authentication codes (MACs) – Part 2: Mechanisms using a dedicated hash-function* (ISO/IEC 9797-2:2021). (2021)
7. Chernenko, R. (2023). Performance evaluation of lightweight cryptography algorithms on constrained 8-bit devices. *Electronic Professional Scientific Journal «Cybersecurity: Education, Science, Technique», 1(21).* https://doi.org/10.28925/2663-4023.2023.21.273285
8. Bowden, L. (1985). The story of IFF (identification friend or foe). *IEE Proceedings A - Physical Science, Measurement and Instrumentation, Management and Education, Reviews. 132(6),* 435–437.
9. Alferov, O. P., et al. (2001). *Fundamentals of cryptography.* Helios ARV.

10. Hulak, H. M., & Skladannyi, P. M. (2017). Ensuring the reliability of automated control and data transmission systems for unmanned aerial vehicles. *Mathematical machines and systems, 3*, 154–161.
11. Korniiets, V., & Zhdanova Y. (2024). Methodology for forming a high-speed imitator-resistant cipher for multi-alphabet substitution. *Electronic Professional Scientific Journal «Cybersecurity: Education, Science, Technique», 2(26),* 476–486. https://doi.org/10.28925/2663-4023.2024.26.723
12. Chandrasekharan, K. (2012). *Introduction to Analytic. Number Theory*. Springer-Verlag. Berlin Heidelberg New York.
13. Oleksiichuk, A. M., Koniushok, S. M. (2012). *Fourier transforms and cryptographic properties of Boolean functions.* K.: ISZZI NTUU "KPI".
14. Marks II, R. J. (2009). *Handbook of Fourier Analysis & Its Applications.* Oxford: Oxford University Press.
15. Hulak, H., Zhdanova Y., Skladannyi, P., Hulak, Y., & Korniiets, V. (2022). Vulnerabilities of short message encryption in mobile information and communication systems of critical infrastructure objects. *Electronic Professional Scientific Journal «Cybersecurity: Education, Science, Technique», 1(17),* 145–158. https://doi.org/10.28925/2663-4023.2022.17.145158
16. Korniiets, V., & Chernenko, R. (2023). Modification of the cryptographic algorithm a5/1 to ensure communication for iot devices. *Electronic Professional Scientific Journal «Cybersecurity: Education, Science, Technique», 4(20),* 253–271. https://doi.org/10.28925/2663-4023.2023.20.253271
17. Konheim, A. G. (1981). *Cryptography: A prime.* Wiley & Sons, Incorporated, New York.
18. Shannon, C. E. (1950) *Communication Theory of Secrecy Systems.* Bell Telephone Laboratories, Incorporated, New York.
19. Chernenko, R. (2023). Generation of pseudorandom sequences on microcontrollers with limited computational resources, entropy sources, and statistical properties testing. *Electronic Professional Scientific Journal «Cybersecurity: Education, Science, Technique», 2(22),* 191–203. https://doi.org/10.28925/2663-4023.2023.22.191203
20. Hulak, H. M., Zhiltsov, O. B., Kyrychok, R. V., Korshun, N. V., & Skladannyi, P. M. (2024). *Information and cyber security of the enterprise. Textbook.* Lviv: Publisher Marchenko T. V.