УДК 004.056.55:004.312.2

В. М. Рудницький[1], *д.т.н., професор,*
e-mail: rvn_2008@ukr.net
С. В. Сисоєнко[1], *аспірант,*
О. Г. Мельник[2], *к.т.н., ст. наук. співробітник,*
М. О. Пустовіт[2], *здобувач*
[1] Черкаський державний технологічний університет
б-р Шевченка, 460, м. Черкаси, 18006, Україна
[2] Черкаський інститут пожежної безпеки імені Героїв Чорнобиля
Національного університету цивільного захисту України
вул. Онопрієнка, 8, м. Черкаси, 18034, Україна

ДОСЛІДЖЕННЯ МЕТОДУ ПІДВИЩЕННЯ СТІЙКОСТІ КОМП'ЮТЕРНИХ КРИПТОГРАФІЧНИХ АЛГОРИТМІВ

У статті розглянуто питання щодо можливості використання для криптографії алгоритму криптографічного перетворення інформації двох блоків змінних; проведено аналіз надлишковості алгоритму побудови псевдовипадкової послідовності. Розроблено алгоритм побудови псевдовипадкових послідовностей на основі використання операцій криптоперетворення та алгоритмів криптографічного перетворення двох блоків змінних.

Наведено приклади обробки двох блоків змінних перетворення за допомогою алгоритму криптографічного перетворення інформації, знайдено обернене матричне криптографічне перетворення на основі методу синтезу операцій оберненого криптоперетворення.

Доведено, що для побудови результуючої послідовності на основі групових операцій криптографічного перетворення достатньо будувати лише ті елементи первинного перетворення, які використовуються в груповій операції. Даний підхід забезпечує побудову результуючої послідовності, а також зменшує в два рази складність розрахунку елементів первинного перетворення.

Ключові слова: *криптографічний алгоритм, стійкість, псевдовипадкова послідовність, матричне перетворення, результуюча послідовність.*

Постановка проблеми. На більшість важливих рішень, що приймаються на різних рівнях: від глави держави до пересічного громадянина, впливає якість, достовірність та оперативність інформації, що обробляється в автоматизованих системах. Тому нормальне життя суспільства залежить саме від правильності функціонування таких інформаційних систем [1]. Але все частіше дані системи стають об'єктами для атак. Остання масштабна кібератака, що сталася влітку 2017 року, вплинула на роботу багатьох приватних і державних закладів та установ.

На сьогодні актуальними задачами є підвищення якості та ефективності систем інформаційної безпеки за допомогою криптографічних методів і засобів захисту інформації [2].

Питання оцінки криптостійкості систем захисту інформації є досить актуальним в наш час, адже існує велика кількість криптоалгоритмів [3], і постає задача для удосконалення існуючих та побудови нових ефективних систем захисту інформації й підвищення загального рівня конфіденційності інформації, що передається.

Аналіз останніх досліджень. Серед останніх досліджень і публікацій варто виділити: [4], в якій проведено обґрунтування вимог, побудову та аналіз перспективних симетричних криптоперетворень на основі блочних шифрів. У роботі [5] розглянуто питання удосконалення та аналізу стійкості алгоритму симетричного шифрування ФБШ (блокового шифру на основі перетворення Фейстеля).

В роботі [6] доведено, що використання матричних операцій криптографічного перетворення в поєднанні з груповими операціями криптографічного перетворення забезпечує підвищення якості шифрування (отриманої псевдовипадкової послідовності), а також забезпечує можливість розшифрування інформації, оскільки забезпечує використання умови отримання невиродженого перетворення.

Проте в даних дослідженнях не вивчалося питання щодо можливості використання для криптографії алгоритму криптографічного перетворення інформації двох блоків змінних; не проводився аналіз надлишковості алгоритму побудови псевдовипадкової послідовності.

Формулювання цілей статті. Метою даної роботи є дослідження методу підвищення стійкості комп'ютерних криптографічних алгоритмів на основі використання операцій криптоперетворення та алгоритмів криптографічного перетворення двох блоків змінних.

Виклад основного матеріалу. В роботах [7-10] було доведено, що при кодуванні інформації кількома випадковими невиродженими операціями криптографічного перетворення інформації з подальшим додаванням результатів кодування за модулем 2 підвищується якість псевдовипадкової послідовності за рахунок того, що результат додавання буде виродженим.

Для використання даного результату в криптоперетвореннях скористалися заміною операції додавання за модулем операціями матричного криптоперетворення, що включають в себе додавання за модулем. Дослідження проводилося на основі використання операцій криптоперетворення (табл. 1) та алгоритмів криптографічного перетворення двох блоків змінних (табл. 2).

В роботі [6] було запропоновано, формалізовано та доведено коректність етапів та кроків побудови псевдовипадкових послідовностей на основі операцій криптографічного перетворення інформації двох блоків змінних та алгоритмів криптографічного перетворення двох блоків змінних, які наведено в табл. 3.

Таблиця 1

Операції криптографічного перетворення інформації двох блоків змінних

Номер операції	Модель операції	
	Модель операції прямого перетворення	Модель операції оберненого перетворення
1	$F_{6,5}^{k}=\begin{bmatrix} z_1 \oplus z_2 \\ z_2 \end{bmatrix}$	$F_{6,5}^{d}=\begin{bmatrix} w_1 \oplus w_2 \\ w_2 \end{bmatrix}$
2	$F_{3,6}^{k}=\begin{bmatrix} z_1 \\ z_1 \oplus z_2 \end{bmatrix}$	$F_{3,6}^{d}=\begin{bmatrix} w_1 \\ w_1 \oplus w_2 \end{bmatrix}$
3	$F_{5,6}^{k}=\begin{bmatrix} z_2 \\ z_1 \oplus z_2 \end{bmatrix}$	$F_{6,3}^{d}=\begin{bmatrix} w_1 \oplus w_2 \\ w_1 \end{bmatrix}$
4	$F_{6,3}^{k}=\begin{bmatrix} z_1 \oplus z_2 \\ z_1 \end{bmatrix}$	$F_{5,6}^{d}=\begin{bmatrix} w_2 \\ w_1 \oplus w_2 \end{bmatrix}$

Таблиця 2

Алгоритм криптографічного перетворення двох блоків змінних

Номер алгоритму	Алгоритми криптографічного перетворення	
	Алгоритм прямого перетворення	Алгоритм оберненого перетворення
1	$G_{6,5}^{k}=\begin{bmatrix} F_1 \oplus F_2 \\ F_2 \end{bmatrix}$	$G_{6,5}^{d}=\begin{bmatrix} F_1 \oplus F_2 \\ F_2 \end{bmatrix}$
2	$G_{3,6}^{k}=\begin{bmatrix} F_1 \\ F_1 \oplus F_2 \end{bmatrix}$	$G_{3,6}^{d}=\begin{bmatrix} F_1 \\ F_1 \oplus F_2 \end{bmatrix}$
3	$G_{5,6}^{k}=\begin{bmatrix} F_2 \\ F_1 \oplus F_2 \end{bmatrix}$	$G_{6,3}^{d}=\begin{bmatrix} F_1 \oplus F_2 \\ F_1 \end{bmatrix}$
4	$G_{6,3}^{k}=\begin{bmatrix} F_1 \oplus F_2 \\ F_1 \end{bmatrix}$	$G_{5,6}^{d}=\begin{bmatrix} F_2 \\ F_1 \oplus F_2 \end{bmatrix}$

Таблиця 3

Таблиця алгоритму побудови псевдовипадкової послідовності

Етапи реалізації алгоритму	Кроки алгоритму побудови псевдовипадкових послідовностей				
	1	2	3	4	5
Побудова перших операндів	$F_{1;1}^{k}(z_1)$	$F_{1;2}^{k}(z_2)$	$F_{1;3}^{k}(z_3)$	$F_{1;4}^{k}(z_4)$	$F_{1;5}^{k}(z_5)$
Побудова других операндів	$F_{2;1}^{k}(z_1)$	$F_{2;2}^{k}(z_2)$	$F_{2;3}^{k}(z_3)$	$F_{2;4}^{k}(z_4)$	$F_{2;5}^{k}(z_5)$
Побудова результуючої послідовності	$G_1^k(F_1,F_2)$		$G_2^k(F_1,F_2)$		$G_3^k(F_1,F_2)$

Розглянемо обробку перших двох блоків змінних перетворення за допомогою першого алгоритму криптографічного перетворення інформації $G_{6,5}^{k}=\begin{bmatrix} F_1 \oplus F_2 \\ F_2 \end{bmatrix}$.

Позначимо F_1 через $F_{1;1}^{k}(z_1)$, тоді $F_1 = F_{1;1}^{k}(z_1) = F_{6,5}^{k}(z_1) = \begin{bmatrix} z_{1.1} \oplus z_{1.2} \\ z_{1.2} \end{bmatrix}$.

Представимо F_2 через $F_{2;2}^{k}(z_2)$, тоді $F_2 = F_{2;2}^{k}(z_2) = F_{6,3}^{k}(z_2) = \begin{bmatrix} z_{2.1} \oplus z_{2.2} \\ z_{2.1} \end{bmatrix}$.

Перший алгоритм криптографічного перетворення інформації двох блоків змінних буде наступним:

$$G_{6,5}^{k}=\begin{bmatrix} F_1 \oplus F_2 \\ F_2 \end{bmatrix}=\begin{bmatrix} F_{1;1}^{k}(z_1) \oplus F_{2;2}^{k}(z_2) \\ F_{2;2}^{k}(z_2) \end{bmatrix}=$$

$$=\begin{bmatrix} F_{6,5}^{k}(z_1) \oplus F_{6,3}^{k}(z_2) \\ F_{6,3}^{k}(z_2) \end{bmatrix}=\begin{bmatrix} z_{1.1} \oplus z_{1.2} \oplus z_{2.1} \oplus z_{2.2} \\ z_{1.2} \oplus z_{2.1} \\ z_{2.1} \oplus z_{2.2} \\ z_{2.1} \end{bmatrix}$$

Перевіримо можливість використання даного перетворення для криптографії. Для цього необхідне існування оберненого перетворення.

Обернене матричне криптографічне перетворення знайдемо на основі методу синтезу операцій оберненого криптоперетворення, наведеного в [2].

Використавши даний метод, отримаємо: $G_{6,5}^{d}=\begin{bmatrix} w_{1.1} \oplus w_{1.2} \oplus w_{2.1} \oplus w_{2.2} \\ w_{1.2} \oplus w_{2.2} \\ w_{2.2} \\ w_{2.1} \oplus w_{2.2} \end{bmatrix}$.

Перевіримо коректність отриманої операції оберненого перетворення.

$$G_{6,5}^{d}=\begin{bmatrix} w_{1.1} \oplus w_{1.2} \oplus w_{2.1} \oplus w_{2.2} \\ w_{1.2} \oplus w_{2.2} \\ w_{2.2} \\ w_{2.1} \oplus w_{2.2} \end{bmatrix}=$$

$$=\begin{bmatrix} z_{1.1} \oplus z_{1.2} \oplus z_{2.1} \oplus z_{2.2} \oplus z_{1.2} \oplus z_{2.1} \oplus z_{2.1} \oplus z_{2.2} \oplus z_{2.1} \\ z_{1.2} \oplus z_{2.1} \oplus z_{2.1} \\ z_{2.1} \\ z_{2.1} \oplus z_{2.2} \oplus z_{2.1} \end{bmatrix}=\begin{bmatrix} z_{1.1} \\ z_{1.2} \\ z_{2.1} \\ z_{2.2} \end{bmatrix}$$

Отримано коректну операцію оберненого криптографічного перетворення. При реалізації даної операції були задіяні обидві псевдовипадкові послідовності, а це призводить до підвищення якості загального результату перетворення.

Проведемо аналіз надлишковості алгоритму побудови псевдовипадкової послідовності (табл. 3). В результаті дослідження було встановлено наступне:

1. Для побудови коректного групового перетворення

$$G_i^k = \left(F_{1,2i-1}^{k}, F_{2,2i}^{k}\right),$$
$$G_i^k = \left(F_{2,2i}^{k}, F_{1,2i-1}^{k}\right)$$

необхідно знайти $F_{1,2i-1}^{k}$ та $F_{2,2i}^{k}$. Знаходити результати перетворення $F_{1,2i}^{k}$ та $F_{2,2i-1}^{k}$ не потрібно, так як вони в побудові групових операцій не використовуються.

2. Для побудови коректного групового перетворення

$$G_i^k = \left(F_{1,2i}^{k}, F_{2,2i-1}^{k}\right),$$
$$G_i^k = \left(F_{2,2i-1}^{k}, F_{1,2i}^{k}\right)$$

необхідно знайти $F_{1,2i}^{k}$ та $F_{2,2i-1}^{k}$. Знаходити результати перетворення $F_{1,2i-1}^{k}$ та $F_{2,2i}^{k}$ не потрібно, так як вони не використовуються.

Виходячи з наведених результатів, можна зробити висновок, що для побудови результуючої послідовності на основі групових операцій криптографічного перетворення достатньо будувати лише ті елементи первинного перетворення, які використовуються в груповій операції. Даний підхід забезпечує побудову результуючої послідовності, а також зменшує в два рази складність розрахунку елементів первинного перетворення, тому що інші елементи не використовуються.

Список літератури

1. Василюк В. Я., Климчук С. О. Інформаційна безпека держави: курс лекцій. Київ: КНТ, Видавничий дім «Скіф», 2008. 136 с.
2. Рудницкий В. Н., Мильчевич В. Я., Бабенко В. Г., Мельник Р. П., Рудницкий С. В., Мельник О. Г. Криптографическое кодирование: методы и средства реализации (часть 2): монография. Краснодар, 2014. 224 с.
3. Мао В. Современная криптография: теория и практика. М.: Издательский дом «Вильямс», 2005. 768 с.

4. Кузнецов О. О., Олійников Р. В., Горбенко Ю. І., Пушкарьов А. І., Дирда О. В., Горбенко І. Д. Обґрунтування вимог, побудування та аналіз перспективних симетричних криптоперетворень на основі блочних шифрів. *Вісник Національного університету «Львівська політехніка». Комп'ютерні системи та мережі*. 2014. № 806. С. 124–141.
5. Лагун А., Поліщук О. Удосконалення та аналіз стійкості алгоритму симетричного шифрування ФБШ. Захист інформації і безпека інформаційних систем: мат-ли I Міжнар. наук.-техн. конф., 31 трав. – 01 черв. 2012 р. Львів, 2012. С. 104–106.
6. Наукоемкие технологии в инфокоммуникациях: обработка информации, кибербезопасность, информационная борьба: монография / под общей редакцией В. М. Безрука, В. В. Баранника. Х.: Издательство «Лидер», 2017. 600 с.
7. Ланських Є. В., Сисоєнко С. В., Пустовіт М. О. Оцінка якості псевдовипадкових послідовностей на основі використання операцій додавання за модулем два. *Наука і техніка Повітряних Сил Збройних Сил України.* 2015. № 4 (21). С. 147–150. URL: http://nbuv.gov.ua/UJRN/ Nitps_2015_4_36.
8. Фауре Е. В., Сисоєнко С. В., Миронюк Т. В. Синтез і аналіз псевдовипадкових послідовностей на основі операцій криптографічного перетворення. *Системи управління, навігації та зв'язку*. Полтава: ПНТУ, 2015. № 4 (36). С. 85–87.
9. Рудницький В. М., Фауре Е. В., Сисоєнко С. В. Оцінка якості псевдовипадкових послідовностей на основі додавання за модулем. *Вісник інженерної академії України.* Київ, 2016. № 3. С. 219–221.
10. Фауре Е. В., Сисоєнко С. В. Метод підвищення стійкості псевдовипадкових послідовностей до лінійного криптоаналізу. *Науковий прогрес та процес розвитку країни в аспекті євроінтеграції: зб. наук. праць «ЛОГОС». Спецвипуск*. 2016. Т.1. С. 119–122.

References

1. Vasylyuk, V. Y. and Klymchuk, S. O. (2008) Information security of the state: a course of lectures. Kyiv: Vydavnychyy dim «Skif», 136 p. [in Ukrainian].
2. Rudnytskyy, V. N., Mylchevych, V. Y., Babenko, V. G., Melnyk, R. P., Rudnytskyy, S. V. and Melnyk, O. G. (2014) Cryptographic coding: methods and means of realization (part 2): monograph. Krasnodar, 224 p. [in Russian].
3. Venbo, Mao (2005) Modern cryptography: theory and practice. Moscow: Izdatelskyi dom «Williams», 768 p. [in Russian].
4. Kuznetsov, O. O., Oliynykov, R. V., Horbenko, Y. I., Pushkar'ov, A. I., Dyrda, O. V. and Horbenko, I. D. (2014) Substantiation of requirements, construction and analysis of perspective symmetric cryptographic transformations based on block ciphers. *Visnyk Nacionalnogo universytetu «Lvivska politechnika». Kompjuterni systemy ta mereži*, No. 806, pp. 124–141 [in Ukrainian].
5. Lahun, A. and Polishchuk, O. (2012) Improvement and analysis of the stability of the algorithm of symmetric encryption of FBS. *Zakhyst informatsiyi i bezpeka informatsiynykh system: mat-ly I Mizhnar. nauk.-tekhn. konf, 31 trav. – 01 cherv. 2012 r. Lviv, pp. 104–106* [in Ukrainian].
6. High technology in infocommunications: information processing, cybersecurity, information struggle: monograph / pod obshchey redaktsyey V. M. Bezruka, V. V. Barannyka. Kh.: Yzdatelstvo «Lyder», 2017, 600 p. [in Russian].
7. Lanskykh, Ye. V., Sysoyenko, S. V. and Pustovit, M. O. (2015) Assessing the quality of pseudorandom sequences based on the use of adding operations by module two. *Nauka i tekhnika Povitryanykh Syl Zbroynykh Syl Ukrayiny*, No. 4 (21), pp. 147–150 [in Ukrainian].
8. Faure, E. V., Sysoyenko, S. V. and Myronyuk, T. V. (2015) Synthesis and analysis of pseudorandom sequences based on cryptographic transformation operations. *Systemy upravlinnya, navihatsiyi ta zvyazku*, No. 4 (36), pp. 85–87 [in Ukrainian].
9. Rudnytskyy, V. M., Faure, E. V. and Sysoyenko, S. V. (2016) Assessing the quality of pseudorandom sequences based on the addition of a module. *Visnyk inzhenernoyi akademiyi Ukrayiny*, No. 3, pp. 219–221 [in Ukrainian].
10. Faure, E. V. and Sysoyenko, S. V. (2016) Method of increasing the stability of pseudorandom sequences to linear cryptanalysis. *Naukovyy prohres ta protses rozvytku krayiny v aspekti yevrointehratsiyi*, V. 1, pp. 119–122 [in Ukrainian].

V. M. Rudnitsky[1], *Dr.Tech.Sc., professor,*
e-mail: rvn_2008@ukr.net
S. V. Sysoyenko[1], *Ph.D. student,*
O. G. Melnyk[2], *Ph.D., Senior Researcher,*
M. O. Pustovit[2], *Applicant*
[1] Cherkasy State Technological University
Shevchenko blvd., 460, Cherkasy, 18006, Ukraine
[2] Cherkasy Institute of Fire Safety named after Chornobyl Heroes of National University
of Civil Defense of Ukraine, Onoprienko Str., 8, Cherkasy, 18034, Ukraine

STUDYING METHOD FOR STABILITY IMPROVEMENT OF COMPUTER CRYPTOGRAPHIC ALGORITHM

The article considers the possibility of using cryptographic algorithm for cryptographic information transformation of two blocks of variables; the analysis of the redundancy of the pseudorandom sequence algorithm is carried out. An algorithm for constructing pseudorandom sequences based on the use of cryptographic transformation operations and algorithms for cryptographic transformation of two blocks of variables is developed.

Examples of processing two blocks of transformation variables using cryptographic information transformation algorithm are found; the inverse matrix cryptographic transformation is found on the basis of the synthesis method of inverse cryptographic transformation operations.

It is proved that to construct a resultant sequence on the basis of group operations of cryptographic transformation it is enough to build only those elements of the primary transformation used in the group operation. This approach provides the construction of the resulting sequence, as well as reduces by half the elements calculation complexity of the primary transformation.

Keywords: *cryptographic algorithm, stability, pseudorandom sequence, matrix transformation, resultant sequence.*

Статтю представляє В. М. Рудницький, д.т.н., професор.