УДК 004.056.55:003.26

С.В. Сисоєнко,
старший викладач
Черкаського державного технологічного університету, м. Черкаси, Україна,
ORCID ID 0000-0002-0009-337X
І.В. Миронець,
кандидат технічних наук, доцент,
доцент Черкаського державного технологічного університету,
м. Черкаси, Україна,
ORCID ID 0000-0003-2007-9943,
В.Г. Бабенко,
кандидат технічних наук, доцент, професор Університету митної справи
та фінансів, м. Дніпро, Україна,
ORCID ID 0000-0003-2039-2841

ПОБУДОВА УЗАГАЛЬНЕНОЇ МАТЕМАТИЧНОЇ МОДЕЛІ ГРУПОВОГО МАТРИЧНОГО КРИПТОГРАФІЧНОГО ПЕРЕТВОРЕННЯ

Показано удосконалену модель побудови криптоперетворення на основі використання двохоперандних операцій, шляхом впровадження ієрархічної структури групового перетворення та встановлення нових взаємозв'язків між прямими та оберненими операціями для підвищення стійкості результатів шифрування. Розроблено метод підвищення швидкості реалізації групового матричного криптографічного перетворення на основі запропонованої узагальненої математичної моделі групового матричного криптографічного перетворення. На основі математичного апарату блочних матриць було проведено перевірку коректності узагальненої математичної моделі побудови оберненого групового матричного криптоперетворення.

Ключові слова: *псевдовипадкова послідовність, операції додавання за модулем, криптографічне перетворення інформації, групові операції, відносна швидкість шифрування.*

Показана усовершенствованная модель построения криптопреобразования на основе использования двухоперандных операций, путем внедрения иерархической структуры группового преобразования и определения новых взаимосвязей между прямыми и обратными операциями для повышения результатов шифрования. Разработан метод повышения скорости реализации группового матричного криптографического преобразования на основе предложенной обобщенной математической модели группового матричного криптографического преобразования, за счет уменьшения сложности построения и реализации обратного преобразования, что обеспечило уменьшение математической сложности и скорости криптографического преобразования. На основе математического аппарата блочных матриц была проведена проверка корректности обобщенной математической модели построения обратного группового матричного криптопреобразования.

Ключевые слова: *псевдослучайная последовательность, операции сложения по модулю, криптографическое преобразование информации, групповые операции, относительная скорость шифрования.*

Постановка проблеми. Забезпечення захисту конфіденційної інформації про соціальний, політичний, економічний, військовий та науково-технологічний стан держави та персональної інформації громадян є вкрай важливою задачею. В

умовах наростання кількості загроз виникає необхідність розробки нових та вдосконалення існуючих систем захисту інформації. У сфері захисту інформації криптографічний захист є одним із перспективних напрямів наукових досліджень як у нашій державі, так і за її межами.

Аналіз останніх досліджень та публікацій. Значний внесок у вдосконалення існуючих та розробку нових методів і засобів криптографічного захисту інформації зробили такі зарубіжні та вітчизняні вчені: C.E. Shannon, B. Schneier, G. Brassard, J.L. Massey, W. Diffie, M.E. Hellman, R.L. Rivest, A. Shamir, N. Koblitz, О.А. Молдовян, М.А. Молдовян, І.Д. Горбенко, В.К. Задірака, М.А. Іванов, А.Н. Фіонов, В.В. Ященко, О.О. Логачов, Б.Я. Рябко, А.М. Олексійчук, Л.В. Ковальчук, А.Я. Білецький, О.Г. Корченко та інші.

Проте у зв'язку з розвитком комп'ютерних систем завжди були і будуть залишатися невирішеними задачі підвищення рівня захисту інформації та зменшення часу шифрування. Основними характеристиками криптографічних систем є стійкість, швидкість та надійність криптоперетворення, які необхідно постійно підвищувати. На сьогодні не вичерпані всі можливості підвищення стійкості криптографічних систем на основі використання логічних операцій криптографічного перетворення, вагомий внесок у розвиток яких зробили: К.Г. Самофалов, В.А. Лужецький, О.В. Дмитришин, О.М. Романкевич, Р.П. Мельник, І.В. Миронець та інші. Тому виникає потреба у проведенні додаткових досліджень, спрямованих на розробку методів підвищення якості псевдовипадкових послідовностей, а також підвищення якості криптопримітивів для потокового та блокового шифрування. Залишається невирішеною, зокрема, задача підвищення швидкості та стійкості матричного криптографічного перетворення інформації на основі застосування групових перетворень.

Мета статті. Дослідження та перевірка коректності узагальненої математичної моделі групового матричного криптографічного перетворення.

Виклад основного матеріалу. За результатами попередніх досліджень [1; 2; 3] була отримана коректна модель двохоперандного групового криптографічного перетворення, що дозволяє зробити припущення про можливість побудови узагальнених моделей (1) прямого групового криптографічного перетворення та (2) оберненого групового криптографічного перетворення.

$$\text{Якщо } G^k = \begin{bmatrix} a_{11}F_1^k(z_1) \oplus a_{12}F_2^k(z_2) \oplus \ldots \oplus a_{1n}F_n^k(z_n) \\ a_{21}F_1^k(z_1) \oplus a_{22}F_2^k(z_2) \oplus \ldots \oplus a_{2n}F_n^k(z_n) \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ a_{n1}F_1^k(z_1) \oplus a_{n2}F_2^k(z_2) \oplus \ldots \oplus a_{nn}F_n^k(z_n) \end{bmatrix}, \quad (1)$$

де $a_{ij} \in [0,1]$ – коефіцієнти матриці прямого групового криптографічного перетворення, F_i^k – операції не групових двохоперандних криптографічних перетворень, $\oplus$ – операція "сума за mod 2". z_i – вхідні дані для прямого перетворення, w_i – вхідні дані (результати прямого перетворення) для оберненого перетворення.

$$\text{Тоді } G^d = \begin{bmatrix} b_{11}F_1^d(w_1) \oplus b_{12}F_1^d(w_2) \oplus \ldots \oplus b_{1n}F_1^d(w_n) \\ b_{21}F_2^d(w_1) \oplus b_{22}F_2^d(w_2) \oplus \ldots \oplus b_{2n}F_2^d(w_n) \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ b_{n1}F_n^d(w_1) \oplus b_{n2}F_n^d(w_2) \oplus \ldots \oplus b_{nn}F_n^d(w_n) \end{bmatrix}, \quad (2)$$

де $b_{ij} \in [0,1]$ – коефіцієнти матриці оберненого групового криптографічного перетворення, F_i^d – операції обернених не групових двохоперандних криптографічних перетворень.

Запропоновані математичні моделі (1, 2) за своєю сутністю представляють метод підвищення швидкості групового матричного криптографічного перетворення.

Перевіримо коректність розробленого методу та моделей підвищення швидкості і стійкості групового матричного криптографічного перетворення.

Для побудови оберненого групового чотирьохоперандного криптографічного перетворення використаємо відомі [4] прямі та обернені негрупові двохоперандні операції перетворення.

Нехай
$$G^k = G^k_{x,x,x,x} == \begin{bmatrix} F^k_1(z_1) \oplus F^k_3(z_3) \\ F^k_2(z_2) \oplus F^k_4(z_4) \\ F^k_1(z_1) \oplus F^k_2(z_2) \oplus F^k_4(z_4) \\ F^k_3(z_3) \oplus F^k_4(z_4) \end{bmatrix}$$

$$F^k_1(z_1) = F^k_{1(6,5)} = \begin{bmatrix} z_1 \oplus z_2 \\ z_2 \end{bmatrix},\ F^k_2(z_2) = F^k_{2(6,3)} = \begin{bmatrix} z_3 \oplus z_4 \\ z_3 \end{bmatrix},\ F^k_3(z_3) = F^k_{3(3,6)} = \begin{bmatrix} z_5 \\ z_5 \oplus z_6 \end{bmatrix},$$

$$F^k_4(z_4) = F^k_{4(5,6)} = \begin{bmatrix} z_8 \\ z_7 \oplus z_8 \end{bmatrix}.$$

Тоді
$$G^k_{x,x,x,x} = \begin{bmatrix} F^k_{1(6,5)}(z_1) \oplus F^k_{3(3,6)}(z_3) \\ F^k_{2(6,3)}(z_2) \oplus F^k_{4(5,6)}(z_4) \\ F^k_{1(6,5)}(z_1) \oplus F^k_{2(6,3)}(z_2) \oplus F^k_{4(5,6)}(z_4) \\ F^k_{3(3,6)}(z_3) \oplus F^k_{4(5,6)}(z_4) \end{bmatrix} = \begin{bmatrix} z_1 \oplus z_2 \oplus z_5 \\ z_2 \oplus z_5 \oplus z_6 \\ z_3 \oplus z_4 \oplus z_8 \\ z_3 \oplus z_7 \oplus z_8 \\ z_1 \oplus z_2 \oplus z_3 \oplus z_4 \oplus z_8 \\ z_2 \oplus z_3 \oplus z_7 \oplus z_8 \\ z_5 \oplus z_8 \\ z_5 \oplus z_6 \oplus z_7 \oplus z_8 \end{bmatrix}$$

$$G^k = G^k_{x,x,x,x} = A_{x,x,x,x} = \begin{bmatrix} 1 & 1 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{bmatrix}$$

Знайдемо обернену матрицю згідно із запропонованою моделлю (2) за умови:

$$F^k_{1(6,5)} \to F^d_{1(6,5)} = \begin{bmatrix} w_1 \oplus w_2 \\ w_2 \end{bmatrix},\ F^k_{2(6,3)} \to F^d_{2(5,6)} = \begin{bmatrix} w_4 \\ w_3 \oplus w_4 \end{bmatrix},\ F^k_{3(3,6)} \to F^d_{3(3,6)} = \begin{bmatrix} w_5 \\ w_5 \oplus w_6 \end{bmatrix}$$

$$F^k_{4(5,6)} \to F^d_{4(6,3)} = \begin{bmatrix} w_7 \oplus w_8 \\ w_7 \end{bmatrix}.$$

Оскільки

$$G^k_{x,x,x,x} \to G^d_{x,x,x,x} = \begin{bmatrix} F^d_{1(6,5)}(w_2) \oplus F^d_{1(6,5)}(w_3) \\ F^d_{2(5,6)}(w_1) \oplus F^d_{2(5,6)}(w_3) \oplus F^d_{2(5,6)}(w_4) \\ F^d_{3(3,6)}(w_1) \oplus F^d_{3(3,6)}(w_2) \oplus F^d_{3(3,6)}(w_3) \\ F^d_{4(6,3)}(w_1) \oplus F^d_{4(6,3)}(w_2) \oplus F_{4(6,3)}(w_3) \oplus F^d_{4(6,3)}(w_4) \end{bmatrix} =$$

$$= \begin{bmatrix} w_3 \oplus w_4 \oplus w_5 \oplus w_6 \\ w_4 \oplus w_6 \\ w_2 \oplus w_6 \oplus w_8 \\ w_1 \oplus w_2 \oplus w_5 \oplus w_6 \oplus w_7 \oplus w_8 \\ w_1 \oplus w_3 \oplus w_5 \\ w_1 \oplus w_2 \oplus w_3 \oplus w_4 \oplus w_5 \oplus w_6 \\ w_1 \oplus w_2 \oplus w_3 \oplus w_4 \oplus w_5 \oplus w_6 \oplus w_7 \oplus w_8 \\ w_1 \oplus w_3 \oplus w_5 \oplus w_7 \end{bmatrix}$$

Матриця $A_{x,x,x,x}{}^{-1}$ набуде такого вигляду:

$$G^d_{x,x,x,x} = A_{x,x,x,x}{}^{-1} = \begin{bmatrix} 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 0 & 1 \\ 1 & 1 & 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \end{bmatrix}.$$

Провівши відповідні математичні обчислення, перевіримо правильність отриманого результату, використавши формулу Фробеніуса [5].

$$A_{x,x,x,x}A_{x,x,x,x}{}^{-1} = A_{x,x,x,x}{}^{-1}A_{x,x,x,x} = \begin{bmatrix} E & 0 \\ 0 & E \end{bmatrix} =$$

$$= \begin{bmatrix} 1&1&0&0&1&0&0&0 \\ 0&1&0&0&1&1&0&0 \\ 0&0&1&1&0&0&0&1 \\ 0&0&1&0&0&0&1&1 \\ 1&1&1&1&0&0&0&1 \\ 0&1&1&0&0&0&1&1 \\ 0&0&0&0&1&0&0&1 \\ 0&0&0&0&1&1&1&1 \end{bmatrix} \times \begin{bmatrix} 0&0&1&1&1&1&0&0 \\ 0&0&0&1&0&1&0&0 \\ 0&1&0&0&0&1&0&1 \\ 1&1&0&0&1&1&1&1 \\ 1&0&1&0&1&0&0&0 \\ 1&1&1&1&1&1&0&0 \\ 1&1&1&1&1&1&1&1 \\ 1&0&1&0&1&0&1&0 \end{bmatrix} = \begin{bmatrix} 1&0&0&0&0&0&0&0 \\ 0&1&0&0&0&0&0&0 \\ 0&0&1&0&0&0&0&0 \\ 0&0&0&1&0&0&0&0 \\ 0&0&0&0&1&0&0&0 \\ 0&0&0&0&0&1&0&0 \\ 0&0&0&0&0&0&1&0 \\ 0&0&0&0&0&0&0&1 \end{bmatrix}$$

Цей результат показав правильність знаходження оберненої матриці за допомогою запропонованої моделі (2).

Розроблений метод забезпечує підвищення стійкості результатів шифрування, тому що базується на матричних операціях додавання по модулю два, які забезпечують часткову реалізацію додавання декількох псевдовипадкових послідовностей.

За результатами моделювання та практичного впровадження встановлено, що зменшення складності реалізації математичної моделі групового матричного криптографічного перетворення становить від 8 до 33 разів залежно від розрядності матриць, а також забезпечено збільшення швидкості реалізації на 6–8 % за результатами практичного впровадження [6; 7].

Висновки. У статті вперше розроблено метод підвищення швидкості реалізації групового матричного криптографічного перетворення на основі запропонованої узагальненої математичної моделі групового матричного криптографічного перетворення, за рахунок зменшення складності побудови та реалізації оберненого перетворення, що забезпечило зменшення математичної складності та швидкості криптографічного перетворення.

На основі дослідження математичної моделі двохоперандного групового матричного криптографічного перетворення запропоновано узагальнену (по кількості операндів) математичну модель групового матричного криптографічного перетворення та перевірено її коректність.

На основі узагальненої математичної моделі групового матричного криптографічного перетворення розроблено метод підвищення швидкості групового матричного криптографічного перетворення.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. *Сисоєнко С.В., Мельник О.Г.* Дослідження операцій оберненого групового матричного криптографічного перетворення інформації. Наука у контексті сучасних глобалізаційних процесів: матеріали Міжнародної наук.-практ. конф. “Європейська наукова платформа” (м. Полтава, 19 листопада 2017 р.): зб. наук. праць “ЛjГОУ” / відп. за вип. Голденблат М.А. Одеса: Друкарик, 2017. Т. 10. С. 44–46.

2. *Ланських Є.В., Сисоєнко С.В.* Дослідження математичної моделі двохоперандного групового матричного криптографічного перетворення. Вісник Черкаського державного технологічного університету. Серія: Технічні науки. Черкаси: ЧДТУ, 2018. Вип. 1. С. 67–74.

3. *Рудницький В.М., Сисоєнко С.В., Мельник О.Г.* та ін. Дослідження методу підвищення стійкості комп'ютерних криптографічних алгоритмів. Вісник Черкаського державного технологічного університету. Серія: Технічні науки. Черкаси: ЧДТУ, 2017. Вип. 3. С. 5–10.

4. *Рудницкий В.Н., Мильчевич В.Я., Бабенко В.Г.* та ін. Криптографическое кодирование: методы и средства реализации (часть 2): монография. Харьков: ООО «Щедрая усадьба плюс», 2014. 224 с.

5. *Наконечний С.І., Терещенко Т.О., Романюк Т.П.* Економетрія: підручник. Вид. 3-тє, доп. та перероб. Київ: КНЕУ, 2004. 520 с.

6. *Сисоєнко С.В.* Оцінка швидкості реалізації групового матричного криптографічного перетворення. Системи управління, навігації та зв'язку: зб. наук. праць. Вип. 1(47). Полтава: Полтавськ. техн. ун-т ім. Юрія Кондратюка, 2018. С. 141–145.

7. *Сисоєнко С.В., Сисоєнко А.А.* Математична модель синтезу операцій оберненого групового матричного криптографічного перетворення. Проблеми інформатизації: тези доповідей п'ятої Міжнародної наук.-техн. конф. (13–15 листопада 2017 р.). Черкаси: ЧДТУ; Баку: ВА ЗС АР; Бельсько-Бяла, Польща: УТіГН; Полтава: ПНТУ ім. Юрія Кондратюка, 2017. С. 18.

REFERENCES

1. *Sysoyenko S.V., Melnyk O.H.* (2017). Doslidzhennia operatsiy obernenoho hrupovoho matrychnoho kryptohrafichnoho peretvorennia informatsii. Nauka u konteksti suchasnykh hlobalizatsiynykh protsesiv: materialy Mizhnarodnoi nauk.-prakt. konf. "Yevropeyska naukova platforma" "Investigation of operations of inverse group matrix cryptographic information transformation". Science in the Context of Modern Globalization Processes: International Science Materials. conf. "European Scientific Platform" (Poltava, November 19, 2017): Sob. sciences works "LOGOU" / rep. for the issue Goldenblatt MA Odessa: Drukaruk. T. 10. P. 44–46. [in Ukrainian].

2. *Lanskykh Ye.V., Sysoyenko S.V.* (2018). Doslidzhennia matematychnoyi modeli dvokhoperandnoho hrupovoho matrychnoho kryptohrafichnoho peretvorennia. Visnyk Cherkaskoho derzhavnoho tekhnolohichnoho universytetu. "The study of the mathematical model of a two-operand group matrix cryptographic transformation". Bulletin of Cherkasy State Technological University. Series: Engineering. Cherkasy: ChSTU. Iss. 1. P. 67–74 [in Ukrainian].

3. *Rudnytskyi V.M., Sysoienko S.V., Melnyk O.H.* ta in. (2017). Doslidzhennia metodu pidvyshchennia stiykosti kompiuternykh kryptohrafichnykh alhorytmiv. "Research of the method of increasing the stability of computer cryptographic algorithms". Bulletin of Cherkasy State Technological University. Series: Engineering. Cherkasy: ChSTU. Iss. 3. P. 5–10. [in Ukrainian].

4. *Rudnitsky V.N., Milchevich V.Ya., Babenko V.G.* та нп. (2014). Kriptohraficheskoye kodirovaniye: metody i sredstva realizatsii (chast 2): monohrafiya. "Cryptographic coding: methods and means of realization (part 2): monograph". Kharkiv: LLC "Generous Estate Plus". 224 p. [in Russian].

5. *Nakonechnyi S.I., Tereshchenko T.O., Romaniuk T.P.* (2004). Ekonometriia: pidruchnyk. "Econometrics": textbook. Kind. 3rd, add. and processing". Kyiv: KNEU. 520 p. [in Ukrainian].

6. *Sysoienko S.V.* (2018). Otsinka shvydkosti realizatsii hrupovoho matrychnoho kryptohrafichnoho peretvorennia. Systemy upravlinnia, navihatsii ta zviazku: zb. nauk. prats. "Estimation of the implementation speed of group matrix cryptographic transformation". Systems of control, navigation and communication: Sb. sciences works. Iss. 1(47). Poltava: Poltava. tech Un-t them. Yuri Kondratyuk. P.141–145. [in Ukrainian].

7. *Sysoienko S.V., Sysoienko A.A.* (2017). Matematychna model syntezu operatsiy obernenoho hrupovoho matrychnoho kryptohrafichnoho peretvorennia. Problemy informatyzatsii: tezy dopovidey piatoi Mizhnarodnoi nauk.-tekhn. Konf. "Mathematical model of the synthesis of operations of inverse group matrix cryptographic transformation. Problems of informatization: theses of reports of the fifth international sciences. Conf". (November 13–15, 2017). Cherkasy: ChTTU; Baku: UAA AR; Bielsko-Biala, Poland: UTiGN; Poltava: PNTU them. Yuri Kondratyuk. 18 p. [in Ukrainian].

UDC 004.056.55:003.26

S.V. Sysoienko,
Senior Lecturer, Cherkasy State Technological University,
Cherkasy,Ukraine,
ORCID ID 0000-0002-0009-337X,
I.V. Myronets,
Candidate of Technical Sciences, Docent,
Associate Professor, Cherkasy State Technological University,
Cherkasy, Ukraine,
ORCID ID 0000-0003-2007-9943,
V.H. Babenko,
Candidate of Technical Sciences, Docent, Professor,
University of Customs and Finance, Dnipro, Ukraine,
ORCID ID 0000-0003-2039-2841

GENERAL CONSTRUCTION OF MATHEMATICAL MODEL OF GROUP MATRIX CRYPTOGRAPHIC TRANSFORMATION

In the process of conducting this scientific research, the model for constructing a cryptographic transformation based on the use of two-operand operations has been improved by implementing hierarchical group transformation, and finding the new relationships between the direct and inverse operations to improve the encryption results. It is proposed to apply the method of increasing the stability of pseudo-random sequences to improve the quality of cryptographic transformation based on the hierarchical application of two-operand information transformation operations. The model of cryptographic transformation has been improved based on the use of two-operand operations, by implementing a hierarchical structure of the transformation to increase the results stability. A method has been developed for increasing the speed of implementation of a group matrix cryptographic transformation based on the proposed generalized mathematical model of a matrix of group cryptographic transformation by reducing the complexity of the construction and implementation of the inverse transform, which provided a reduction of mathematical complexity and speed cryptographic transformation. Based on the study of the mathematical model of two-operand group matrix cryptographic transformations, a generalized (by the number of operands) mathematical model of the matrix of group cryptographic transformation is proposed and its correctness is verified. Based on the generalized mathematical model of the matrix of group cryptographic transformation, a method is developed for increasing the speed of group matrix cryptographic transformation. According to the results of modeling and practical implementation of the developed method, quantitative characteristics of the decrease in complexity and increase in the speed of implementation of the mathematical model of the matrix of group cryptographic transformation were determined which depend on matrices of arbitrary dimension. On the basis of the mathematical apparatus of block matrices, the correctness of the generalized mathematical

model for constructing the inverse group matrix cryptographic transformation was verified.

Keywords: pseudo-random sequence, modulo addition operations, cryptographic transformation of information, group operations, relative encryption speed.

Отримано 30.11.2018
Рецензент Рибальський О.В., д.т.н., проф.