УДК 004.056.55:004.312.2

В. Г. Бабенко, *к.т.н., доцент*
Черкаський державний технологічний університет
б-р Шевченка, 460, м. Черкаси, 18006, Україна
zolot_verba@rambler.ru

СКЛАДНОСТІ ТА ОСОБЛИВОСТІ ПОБУДОВИ ЕФЕКТИВНИХ КРИПТОАЛГОРИТМІВ

Запропонована методологія дослідження та синтезу операцій криптографічного перетворення дозволить забезпечити розробників криптоалгоритмів новими можливостями для побудови систем захисту інформації.

Розроблені методи та засоби криптографічного перетворення з використанням запропонованої методології синтезу операцій криптографічного перетворення інформації забезпечують вирішення важливої науково-технічної задачі – підвищення якості функціонування систем захисту інформаційних ресурсів.

На основі вибраних комплексних показників якості функціонування криптографічних алгоритмів можливо здійснювати порівняльний аналіз методів та принципів, що покладені в основу структури алгоритму та синтезу і вибору операцій криптоперетворення інформації.

Ключові слова: *операції криптографічного перетворення, складність, криптостійкість, швидкість, методологія дослідження та синтезу операцій, ефективний криптографічний алгоритм.*

Постановка проблеми. Зі збільшенням ефективності застосування комунікаційних систем та комп'ютерних мереж збільшується кількість випадків несанкціонованого доступу до конфіденційної інформації. Існуючі засоби захисту недостатньо ефективні або вимагають значних економічних затрат (фінансових ресурсів) для забезпечення їх гарантованого застосування. Тому потрібно розробляти нові ефективні, економічно вигідні засоби захисту, які гарантуватимуть достатній рівень безпеки. Отже, однією з актуальних задач інформаційної безпеки є розробка ефективних, а саме швидкодіючих, криптографічно стійких і відносно недорогих апаратно-програмних засобів захисту інформації.

Отже, актуальним є пошук нових методів шифрування, які б забезпечували достатньо високий рівень криптографічної стійкості та були простими в апаратній та програмній реалізаціях, з урахуванням особливостей сучасних мікропроцесорів.

Аналіз останніх досліджень. В [1] для покращення показників стійкості криптоалгоритмів запропоновано підходи щодо побудови програмних шифрів, зокрема гнучкі шифри, що базуються на використанні декількох модифікацій алгоритму шифрування, а також шифри з псевдоймовірною вибіркою ключів, перестановкою фіксованих процедур та настройкою операцій перетворення. Крім цього, одним із відомих способів підвищення криптостійкості є багатопрохідний режим застосування алгоритму шифрування.

Серед останніх досліджень і публікацій варто виділити роботи [2, 3], де розроблено метод синтезу матричних моделей операцій криптографічного перетворення та доведено ефективність застосування матричних і розширених матричних операцій для криптографічного перетворення інформації.

Проте в цих дослідженнях не було здійснено оцінювання криптостійкості та швидкості реалізації криптографічного захисту інформації. Саме це й робить тему дослідження актуальною.

Аналіз трирозрядних елементарних функцій, проведений в [4], показав, що матричні операції криптографічного перетворення використовують лише частину елементарних функцій, представлених у таблиці. Зі збільшенням розрядності збільшується кількість елементарних функцій. Отримуються елементарні функції, які забезпечують криптографічне перетворення за принципами, відмінними від описаних та досліджених. Тому, перспективним дослідженням є виявлення нових принципів реалізації операцій криптографічного перетворення, що пов'язане з новими принципами побудови криптографічних алгоритмів та вдосконалення існуючих.

Формулювання цілей статті. Метою цього дослідження є виявлення протиріч при синтезі ефективних криптографічних алгоритмів та визначення шляхів їх подолання.

Виклад основного матеріалу. На даний момент відсутня загальна теорія синтезу криптографічних перетворень, не розглянуті в загальному вигляді проблеми підвищення криптостійкості, швидкодії та складності алгоритмів шифрування з використанням нових операцій криптоперетворення, а отже, оцінки ефективності побудови криптоалгоритмів на їх основі досі не визначені.

Методологічна основа синтезу ефективних криптографічних алгоритмів полягає в застосуванні операцій криптографічного перетворення на етапі логічного та алгоритмічного синтезу, який передбачає формалізацію алгоритму роботи криптосистеми.

Аналіз характеристик операцій криптографічного перетворення, правил застосування операцій, а також особливості протидії лінійному та нелінійному криптоаналізу показали, що ці операції забезпечують підвищення ефективності алгоритмів перетворення інформації.

На основі вищезазначеного можна здійснити формалізацію постановки наукової проблеми.

Основні характеристики криптосистеми:

1. Криптостійкість (К).
2. Складність реалізації криптографічного перетворення (С).
3. Швидкість виконання криптографічного перетворення (Ш).
4. Статистичні властивості результатів криптографічного перетворення (Н).

На основі вибраних комплексних показників якості та ефективності функціонування криптосистеми можливо проводити порівняльний аналіз методів та принципів, покладених в основу архітектури ефективних криптоалгоритмів для систем захисту інформаційних ресурсів.

Взаємозалежності ефективних криптосистем визначаються на основі описаних показників та можуть бути досягнуті за таких умов:

1. Криптостійкість $\mathrm{K} \to \max$.

$$\mathrm{K} \to \max, \text{ якщо } \begin{cases} \mathrm{C} \to \max \\ \mathrm{V} \to \min \end{cases}.$$

2. Складність $\mathrm{C} \to \min$.

$$\mathrm{C} \to \min, \text{ якщо } \begin{cases} \mathrm{V} \to \max \\ \mathrm{K} \to \min \end{cases}$$

3. Швидкість $\mathrm{V} \to \max$.

$$\mathrm{V} \to \max, \text{ якщо } \begin{cases} \mathrm{C} \to \min \\ \mathrm{K} \to \min \end{cases}$$

4. Статистичні характеристики $H \to \max$.

$$\mathrm{H} \to \max, \text{ якщо } \begin{cases} \mathrm{C} \to \max \\ \mathrm{V} \to \min \\ \mathrm{K} \to \max \end{cases}$$

Оскільки швидкість та складність виконання криптографічного алгоритму напряму залежать від швидкості та складності виконання операцій перетворення інформації, які становлять основу алгоритму $\mathrm{V_{ALG}} \to \mathrm{V(F_i)}$ і $\mathrm{C_{ALG}} \to \mathrm{C(F_i)}$, тоді швидкість виконання алгоритму напряму залежить від складності $\mathrm{V(F_i)} \to \mathrm{C(F_i)}$ і $V_{ALG} \to C_{ALG}$. Звідси, якщо зростає складність, то знижується швидкість $\uparrow C_{ALG} \Rightarrow \downarrow V_{ALG}$, і навпаки.

Отже, виникає протиріччя між складністю, криптостійкістю та швидкістю: складність алгоритму повинна бути мінімальною, показники швидкості, криптостійкості та статистичні властивості – максимальними:

$$\begin{cases} \mathrm{C} \to \min \\ \mathrm{V} \to \max \\ \mathrm{K} \to \max \\ \mathrm{H} \to \max \end{cases}.$$

Одним із шляхів вирішення виявлених протиріч може бути використання операцій криптографічного перетворення.

У процесі дослідження було побудовано методологію синтезу операцій криптографічного перетворення інформації, сутність якої полягає в такому:

– отримання елементарних функцій із заданою кількістю аргументів, набори значень яких характеризуються однаковою кількістю одиниць та нулів;

– мінімізація отриманих елементарних функцій та визначення складності їх реалізації;

– виокремлення і дослідження групи елементарних функцій приблизно однієї складності, яка не досліджувалась раніше,

для подальшого синтезу операцій криптографічного перетворення;

– розробка методів синтезу елементарних функцій цієї групи на основі різних способів запису елементарних функцій;

– визначення кількості операцій криптографічного перетворення базової групи та поєднання операцій базової групи з операціями групи перестановок та інверсії;

– розробка методів синтезу операцій криптографічного перетворення та оберненого криптографічного перетворення на основі вибраної групи елементарних функцій;

– розробка методів синтезу операцій взаємного криптографічного перетворення на основі виявлення функціональних залежностей між результатами послідовного виконання декількох операцій;

– побудова ефективних криптографічних алгоритмів на основі використання синтезованих операцій криптографічного перетворення.

Етапи реалізації цієї методології графічно зображено на рис. 1.

Запропонована методологія дослідження та синтезу операцій криптографічного перетворення дозволить забезпечити розробників криптоалгоритмів новими можливостями для побудови систем захисту інформації.

На основі реалізації цієї методології були побудовані матричні та розширені матричні операції, які забезпечують, як показали дослідження [3, 4], підвищення ефективності криптоалгоритмів.

Для забезпечення можливості оцінювання ефективності криптоалгоритмів, в яких використовуються операції криптоперетворення, необхідно сформулювати загальну методику застосування декількох різних груп операцій в одному криптоалгоритмі.

Для розробки методики виберемо криптоалгоритм, в якому використовуються операції матричного та розширеного матричного криптографічного перетворення комбіновано.

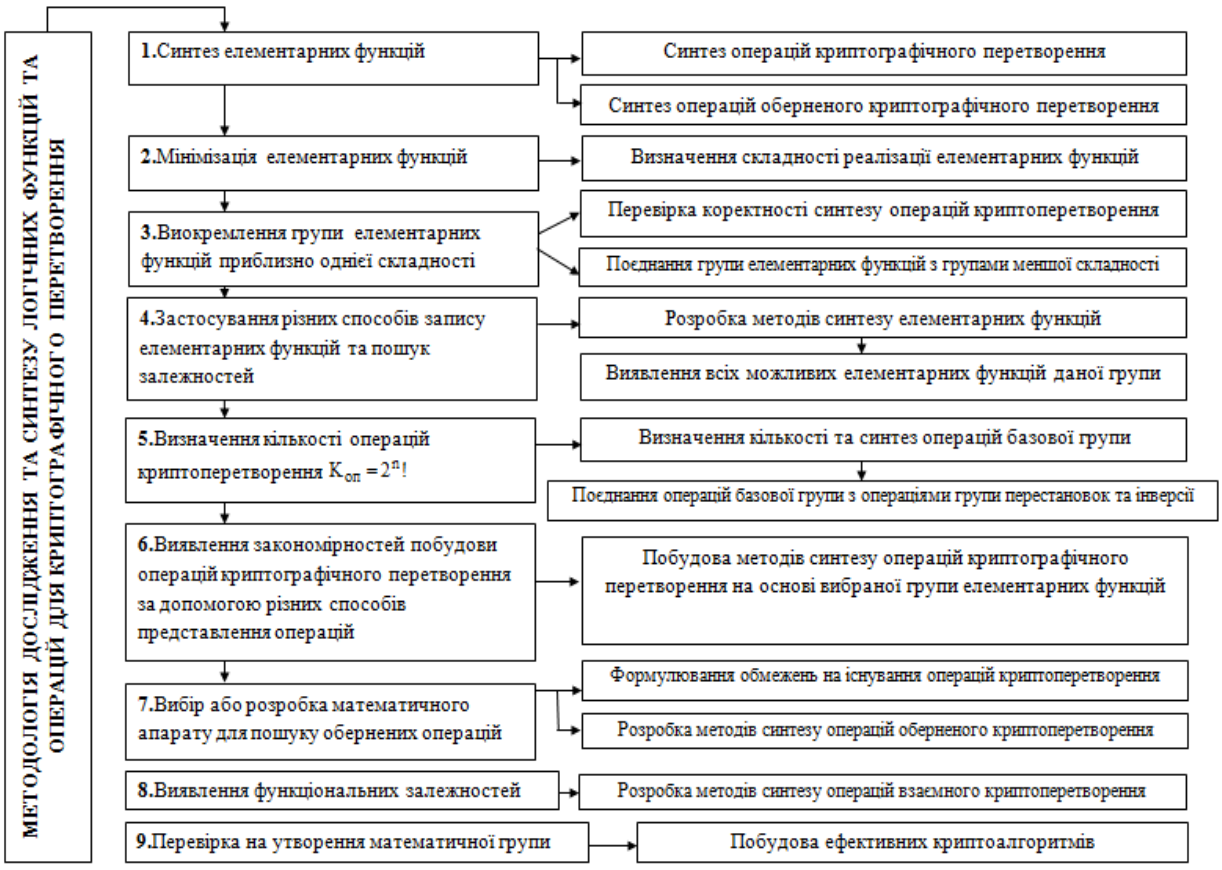

Рис. 1. Структура методології дослідження та синтезу логічних функцій та операцій для криптографічного перетворення інформації

Криптостійкість алгоритму, суть якого полягає у комбінації операцій матричного та розширеного матричного криптографічного перетворення, визначається як

$$K = K_M \cdot K_{PM},$$

де K – криптостікість алгоритму, а K_M, K_{PM} – це криптостійкість матричних та розширених матричних операцій відповідно.

Кількісна оцінка зміни криптостійкості (k) алгоритму шифрування на основі гамуючої послідовності визначається як

$$k = \frac{K_M \cdot K_{PM} \cdot K_Г}{K_Г} = K_M \cdot K_{PM},$$

де $K_Г$ – криптостійкість гамуючої послідовності.

Швидкість виконання матричних і розширених матричних операцій алгоритму криптографічного перетворення доцільніше визначати через час:

$$T_{(M+PM)} = T_{(PM+M)} = \frac{1}{T_M} + \frac{1}{T_{PM}} =$$

$$= \frac{T_M + T_{PM}}{T_M \cdot T_{PM}} = \frac{1}{3} + \frac{1}{6} = \frac{6+3}{18} = \frac{9}{18} = \frac{1}{2}.$$

Оскільки швидкість обернено пропорційна часу, тоді швидкість розраховуватиметься як

$$V_{(M+PM)} = \frac{T_M + T_{PM}}{T_M \cdot T_{PM}}.$$

Розроблені методи та засоби криптографічного перетворення з використанням запропонованої методології синтезу операцій криптографічного перетворення інформації забезпечують вирішення важливої науково-технічної задачі – підвищення якості функціонування систем захисту інформаційних ресурсів.

Висновки. На основі вибраних комплексних показників якості функціонування криптографічних алгоритмів (криптостійкість, швидкість, складність, час, статистичні властивості) можливо здійснювати порівняльний аналіз методів та принципів, що покладені в основу структури алгоритму та синтезу і вибору операцій криптоперетворення інформації.

В процесі дослідження було побудовано методологію синтезу операцій криптографічного перетворення інформації, сутність якої описано етапами реалізації, та зображено її графічну структуру.

Використання методології дослідження та синтезу операцій криптографічного перетворення спрямоване на виявлення нових операцій криптографічного перетворення, застосування яких на етапі алгоритмічного синтезу створює умови для покращення визначених показників ефективності криптографічних криптоалгоритмів.

Запропонована методологія дослідження та синтезу операцій криптографічного перетворення дозволить забезпечити розробників криптоалгоритмів новими можливостями для побудови систем захисту інформації.

Список літератури

1. Молдовян А. А. Криптография : учеб. для вузов / Молдовян А. А., Молдовян Н. А, Советов Б. Я. – СПб. : Лань, 2001. – 224 с., ил.
2. Наукоемкие технологии в инфокоммуникациях: обработка и защита информации : колл. монография / [под ред. В. М. Безрука, В. В. Баранника]. – Харьков : Компания СМИТ, 2013. – 398 с.
3. Криптографическое кодирование: методы и средства реализации : [монография / В. Н. Рудницкий, С. В. Пивнева, В. Г. Бабенко и др.] ; Тольят. гос. ун-т. – Тольятти, 2013. – 196 с.
4. Криптографическое кодирование: методы и средства реализации : [монография / В. Н. Рудницкий, В. Я. Мильчевич, В. Г. Бабенко и др.]. – Краснодар, 2014. – Ч. 2. – 224 с.

References

1. Moldovyan, A. A., Moldovyan, N. A. and Sovetov, B. Y. (2001) Cryptography. St. Petersburg: Lan', 224 p. [in Russian]
2. Science intensive technologies in information communications: data processing and security (2013). In: V. M. Bezruk, V. V. Barannik (Eds.). Kharkov: Companiya SMITH, 398 p. [in Russian]
3. Rudnicki, V. N., Pivneva, S. V., Babenko, V. G. et al. (2013) Cryptographic coding:

methods and tools for implementation. Tolyatti, 196 p. [in Russian]
4. Rudnicki, V. N., Milchevich, V. Y., Babenko, V. G. et al. (2014) Cryptographic coding: methods and tools for implementation (part 2). Krasnodar, 224 p. [in Russian]

Стаття надійшла до редакції 22.07.2014.

V. G. Babenko, *Ph.D., associate professor*
Cherkasy State Technological University,
Shevchenko blvd., 460, Cherkasy, 18006, Ukraine
zolot_verba@rambler.ru

COMPLEXITIES AND SPECIFICITIES FOR CONSTRUCTING OF EFFECTIVE CRYPTOGRAPHIC ALGORITHMS

The article presents integrated indicators of the functioning of cryptographic algorithms on which a comparative analysis of methods and principles underlying the structure and synthesis algorithm and selection operations of cryptographic transformations of information can be made.

The paper offers the methodology of research and synthesis of cryptographic transformation operations and stages of its implementation. The application of this methodology will provide developers with new capabilities of cryptographic algorithms for the construction of information security.

The development of methods and tools of cryptographic transformation using the proposed methodology for the synthesis of cryptographic transformation operations of the information provides to solve an important scientific and technical problem – improving of the quality of functioning of the systems of information resources security.

Keywords: *operations of cryptographic transformation, complexity, cryptographic strength, speed, methodology of research and synthesis operations, efficient cryptographic algorithm.*