УДК 004.056.55:004.312.2

ПАРАЛЛЕЛЬНАЯ РЕАЛИЗАЦИЯ НЕЛИНЕЙНОГО РАСШИРЕННОГО МАТРИЧНОГО КРИПТОГРАФИЧЕСКОГО ПРЕОБРАЗОВАНИЯ

В.Г. Бабенко, кандидат технических наук, докторант
Одесская национальная академия связи им. А.С. Попова, Одесса (Украина)
С.В. Пивнева, кандидат педагогических наук, доцент,
доцент кафедры «Высшая математика и математическое моделирование».
Тольяттинский государственный университет, Тольятти (Россия)
О.Г. Мельник, кандидат технических наук, доцент кафедры строительных конструкций
Р.П. Мельник, кандидат технических наук, доцент кафедры пожарно-профилактической работы
Черкасский институт пожарной безопасности им. Героев Чернобыля НУГЗ Украины, Черкассы (Украина)

Ключевые слова: защита информации; криптографическое преобразование; матричные операции, расширенные матричные операции; параллельная реализация.

Аннотация: В данной работе на основе полученных результатов исследования и проведенной на их основе классификации основных элементарных функций осуществлена параллельная реализация нелинейного расширенного матричного криптографического преобразования.

Расширенное матричное преобразование позволяет увеличить количество операций криптографического преобразования и, как следствие, повысить криптостойкость систем защиты информации, так как операции матричного и расширенного матричного преобразования по результатам исследования не образуют одной группы.

Криптографическое кодирование на основе расширенного матричного преобразования может осуществляться параллельно как над матрицами, так и над тремя разрядами одновременно.

В работе представлен алгоритм параллельной реализации операций расширенного матричного криптографического преобразования.

Результаты программной реализации операций расширенного матричного преобразования были оценены на основе статистических тестов NIST STS.

Реализация операций расширенного матричного криптографического преобразования соответствует требованиям программного пакета статистического тестирования NIST STS.

Практическое использование операций расширенного матричного криптографического преобразования на основании проведенных исследований проводится на основе гаммирующей последовательности.

Поскольку операции криптопреобразования могут выполняться параллельно, то время криптопреобразования будет определяться только временем формирования n_k разрядов гаммирующей последовательности. Тогда увеличение скорости криптографического преобразования информации будет определяться отношением разрядности информации, которая шифруется на основе операций расширенного матричного преобразования под управлением гаммирующей последовательности, к количеству разрядов, над которыми выполнено гаммирование.

Нелинейное расширенное матричное криптографическое преобразование в зависимости от параметров n_k и K_{on} позволяет увеличить криптостойкость от 10^{32} до 10^{150} раз пропорционально относительно потокового шифрования при уменьшении времени шифрования в 1,5–6 раз.

Учитывая то, что сегодня объем данных, который подлежит одновременному преобразованию, довольно громоздкий, то особое внимание уделяется быстродействию аппаратного обеспечения, которое непосредственно реализует преобразование информации. Это же касается и криптографического преобразования.

Криптографическое преобразование может осуществляться над одним, двумя, тремя и более разрядами одновременно, в зависимости от применяемого алгоритма и набора схемотехнических элементов, доступных разработчику.

Криптографическая защита информации развивается в двух направлениях: шифрование и кодирование. Сочетание этих направлений возможно на основе использования логических операций криптографического преобразования информации.

В статье [1] предложена классификация основных элементарных функций для криптографического преобразования, которые были получены и формализованы в результате проведенного вычислительного эксперимента. В результате классификации определено, что группа элементарных функций, которые были названы как функции расширенного матричного преобразования, ранее не исследовалась.

Одним из вариантов использования расширенного матричного представления могут быть дополнения матричного представления [2; 3] расширенным матричным представлением [4].

$$\vec{F}_k = \begin{bmatrix} a_{11}x_1 \oplus a_{12}x_2 \oplus \ldots \oplus a_{1n}x_n \\ a_{21}x_1 \oplus a_{22}x_2 \oplus \ldots \oplus a_{2n}x_n \\ \ldots \\ a_{n1}x_1 \oplus a_{n2}x_2 \oplus \ldots \oplus a_{nn}x_n \end{bmatrix} \oplus \begin{bmatrix} b_1^1 \\ b_2^1 \\ \ldots \\ b_n^1 \end{bmatrix} \oplus \begin{bmatrix} d_1(x_1 \oplus (\tilde{x}_i \cdot \tilde{x}_j)) \\ d_2(x_2 \oplus (\tilde{x}_i \cdot \tilde{x}_j)) \\ \ldots \\ d_n(x_n \oplus (\tilde{x}_i \cdot \tilde{x}_j)) \end{bmatrix} \oplus \begin{bmatrix} d_1 b_1^2 \\ d_2 b_2^2 \\ \ldots \\ d_n b_n^2 \end{bmatrix}$$

Данное расширенное матричное представление позволяет увеличить количество операций криптографического преобразования информации. При использовании только одного расширенного матричного представления – это три разряда – общее количество операций криптографического преобразования информации (N) увеличится в 2016 раз: $N = N_б \cdot N_n \cdot N_i = 42 \cdot 6 \cdot 8 = 2016$, где $N_б$ – базовые операции, N_n – операции перестановки, N_i – операции инверсии.

Расширенное матричное преобразование позволяет увеличить количество операций криптографического преобразования и, как следствие, повысить криптостойкость систем защиты информации, так как операции матричного и расширенного матричного преобразования по результатам исследования не образуют одной группы.

Криптографическое кодирование на основе расширенного матричного преобразования может осуществляться параллельно как над матрицами, так и над тремя разрядами одновременно.

Алгоритм параллельной реализации операций расширенного матричного криптографического преобразования представлен на рис. 1.

Результаты программной реализации операций расширенного матричного преобразования были оценены на основе статистических тестов NIST STS.

Результаты преобразования псевдослучайной последовательности генератора RANDOM, неслучайной монотонно возрастающей последовательности с циклом повторения 64 байта и преобразования текстового файла представлены в табл. 1.

Реализация операций расширенного матричного криптографического преобразования соответствует требованиям программного пакета статистического тестирования NIST STS.

Практическое использование операций расширенного матричного криптографического преобразования

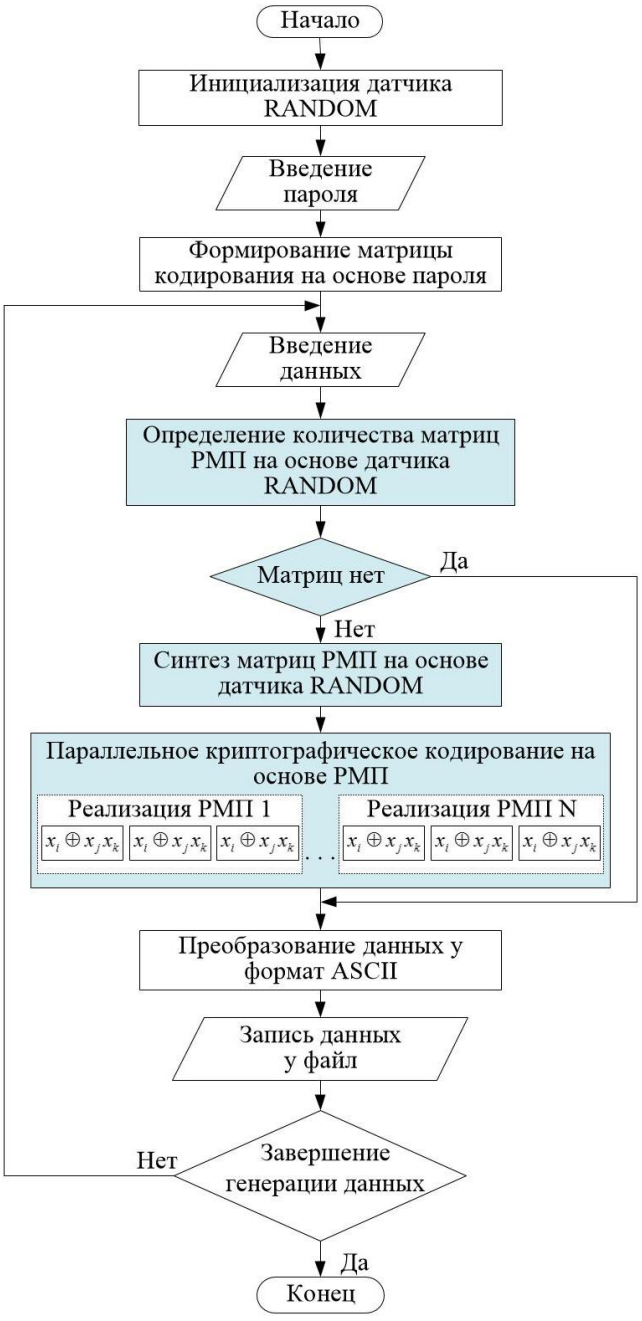

Рис. 1. *Алгоритм параллельной реализации операций расширенного матричного криптографического преобразования*

Таблица 1. *Оценка параллельной программной реализации операций расширенного матричного преобразования*

Объекты тестирования	Количество тестов, у которых тестирование прошли больше 99 % последовательностей	Количество тестов, у которых тестирование прошли больше 96 % последовательностей
Генератор RANDOM-РМП	127 (68 %)	189 (100 %)
Криптографическое преобразование неслучайной монотонно возрастающей последовательности с циклом повторения 64 байта на основе операций РМП	132 (70 %)	189 (100 %)
Криптографическое преобразование текстового файла на основе операций РМП	127 (68 %)	189 (100 %)

на основании проведенных исследований проводится на основе гаммирующей последовательности.

Применим метод повышения скорости шифрования, сущность которого заключается в использовании гаммирующей последовательности как последовательного набора команд выполнения случайно выбранного подмножества операций криптопреобразования. Необходимо отметить, что криптостойкость (z) использования этого метода определяется как $z = z_г \cdot z_o$, где $z_г$ – криптостойкость гаммирующей последовательности, z_o – криптостойкость последовательностей операций криптопреобразования.

Криптостойкость и скорость шифрования определяются параметрами: n_k – разрядность команды выполнения последовательностей операций криптопреобразования, K_{on} – количество операций в последовательности, которая реализует команду.

Подмножество случайно выбранных операций для реализации метода определяется как $П_o = 2^{n_k} \cdot K_{on}$. Практическая криптостойкость зависит от разрядности пароля $R_П = (2^{n_k} \cdot K_{on}) \log_2 2016$ и будет пропорциональной величине $z_o = 2^{R_П}$.

Например, если $n_k = 4$, а $K_{on} = 4$, тогда $П_o = 64$, $R_П = 64 \cdot \log_2 2016 = 704$ и $z_o = 2^{704}$, что является приемлемым значением, так как общая криптостойкость увеличится в 2^{704} раз пропорционально.

Поскольку операции криптопреобразования могут выполняться параллельно, то время криптопреобразования будет определяться только временем формирования n_k разрядов гаммирующей последовательности. Тогда увеличение скорости криптографического преобразования информации будет определяться отношением разрядности информации, которая шифруется на основе операций расширенного матричного преобразования под управлением гаммирующей последовательности, к количеству разрядов, над которыми выполнено гаммирование. Для нашего примера коэффициент увеличения скорости шифрования будет определяться как $k_v = \frac{3 \cdot K_{on}}{n_k} = 3$. Выбор параметров n_k и K_{on} дает возможность обеспечить необходимые значения скорости шифрования и криптостойкости.

Выводы: нелинейное расширенное матричное криптографическое преобразование в зависимости от параметров n_k и K_{on} позволяет увеличить криптостойкость от 10^{32} до 10^{150} раз пропорционально относительно потокового шифрования при уменьшении времени шифрования в 1,5–6 раз.

СПИСОК ЛИТЕРАТУРЫ

1. Бабенко В.Г., Мельник О.Г., Мельник Р.П. Класифікація трирозрядних елементарних функцій для криптографічного перетворення інформації // Безпека інформації. Київ, 2013. С. 56–59.
2. Рудницький В.М., Бабенко В.Г., Рудницький С.В. Метод синтезу матричних моделей операцій криптографічного кодування та декодування інформації // Збірник наукових праць Харківського університету Повітряних Сил. 2012. № 4. С. 198–200.
3. Рудницкий С.В., Мельник Р.П., Веретельник В.В. Криптографическое преобразование информации на основе трехразрядных логических функций // Вектор науки Тольяттинского государственного университета. 2012. № 4. С. 119–122.
4. Мельник Р.П. Застосування операцій розширеного матричного криптографічного перетворення для захисту інформації // Системи обробки інформації. 2012. № 9. С. 145–147.

PARALLEL IMPLEMENTATION OF NONLINEAR EXTENDED MATRIX CRYPTOGRAPHICAL TRANSFORMATION

V.G. Babenko, candidate of technical sciences
Odessa National Academy of Telecommunications named after A.S. Popov, Odessa (Ukraine)
S.V. Pivneva, candidate of pedagogic sciences,
Assistant Professor of the Department «Higher Mathematics and Mathematic Modeling»
Togliatti State University, Tolyatti (Russia)
O.G. Melnyk, candidate of technical sciences,
Assistant Professor of the Department of Engineering Structures
R.P. Melnyk, candidate of technical sciences,
Assistant Professor of the Department of Fire Prevention Activities
Academy of Fire Safety n. a. Heroes of Chernobyl, Cherkassy (Ukraine)

Keywords: information safety; cryptographical transformation; matrix operations; extended matrix operations; parallel implementation.

Annotation: In this investigation, parallel implementation of nonlinear extended matrix cryptographical transformation is carried out on the base of research results and classification of basic elementary functions.

The extended matrix transformation allows to increase the number of operations of cryptographical transformation and, as a consequent, to improve cryptosecurity of information safety systems. The research proved that it is caused by the fact that the operations of matrix and extended matrix transformation do not form single group.

Cryptographic coding on the base of extended matrix transformation may be carried out both over matrices and over three bits simultaneously.

The article presents an algorithm of parallel implementation of extended matrix cryptographical transformation.

The results of program implementation of extended matrix transformation were evaluated on the base of statistical tests NIST STS.

The implementation of extended matrix cryptographic transformation meets the requirements of program package of statistical tests NIST STS.

The research proved that practical application of the operation of extended matrix cryptographic transformation is carried out on the base of gamma-sequence.

As the cryptographical transformations may be carried out simultaneously the time of cryptographical transformation will be determined only by the time of forming of gamma-sequence n_k bits. In that case, the increase of cryptographical transformation speed will be determined by ratio of information size coded on the base of operations of extended matrix transformation under control of gamma-sequence to the number of bits subjected to the gamma-process.

Nonlinear extended matrix cryptographical transformation depending on n_k and K_{on} parameters allows to improve cryptosecurity from 10^{32} to 10^{150} times proportionally against the stream coding when reducing time of coding in 1,5–6 times.