УДК 004.056.55:004.312.2

СПОСОБ ПАРАЛЛЕЛЬНОЙ РЕАЛИЗАЦИИ ОПЕРАЦИЙ МАТРИЧНОГО КРИПТОГРАФИЧЕСКОГО ПРЕОБРАЗОВАНИЯ

В.Н. Рудницкий, доктор технических наук, профессор кафедры системного программирования
Черкасский государственный технологический университет, Черкассы (Украина)
Е.В. Козлов, кандидат физико-математических наук, доцент
Самарский государственный университет путей сообщения, Самара (Россия)
В.Г. Бабенко, докторант
Одесская национальная академия связи им. А.С. Попова, Одесса (Украина)

Ключевые слова: операция криптографического преобразования; матрица; параллельное выполнение; скорость шифрования; криптостойкость; коэффициент быстродействия.

Аннотация: В работе предложен способ повышения быстродействия реализации метода защиты информации на основе операций матричного криптографического преобразования за счет распараллеливания процесса выполнения операции матричного криптографического преобразования. Проведен анализ коэффициента быстродействия, который подтверждает эффективность применения алгоритма параллельной реализации.

Одними из самых распространенных и высокоэффективных средств защиты информации являются средства построены на базе криптографических методов, которые позволяют решать важные задачи защищенной автоматизированной обработки и передачи информации (конфиденциальности и целостности). Основным достоинством таких методов считают их гибкость, потому что реализовать их можно как на аппаратном так и на программном уровне.

Процесс разработки аппаратных или аппаратно-программных средств криптографической защиты информации на основе криптографических алгоритмов [1], непосредственно связан с необходимостью реализации арифметических операций, лежащих в основе алгоритмов. Большинство таких операций связано с обработкой относительно больших объемов информации, что ведет к необходимости выбора элементной базы с повышенной производительностью. Но использование высокопроизводительных элементов, например процессоров, для выполнения криптографических операций в аппаратных средствах зачастую не позволяет обеспечить нужную скорость работы. Поэтому важной задачей считается разработка и реализация быстродействующих программных средств выполнения криптографических операций.

Наиболее перспективным и динамичным направлением увеличения скорости работы программных средств для систем защиты информации является широкое внедрение идей параллелизма при создании алгоритмов выполнения криптографических преобразований.

Основной целью данной статьи является разработка алгоритма параллельного выполнения синтезированных операций криптографического преобразования на основе сложения по модулю два для повышения скорости шифрования данных.

Синтез матричных операций обратного криптографического преобразования на основе известной операции криптографического прямого преобразования без учета группы операций инверсии описан в [2].

В [3] описан метод синтеза матричных операций криптографического взаимного преобразования, использование которого позволяет обеспечить повышение оперативности доступа к конфиденциальным информационным ресурсам за счет замены процесса повторного преобразования.

Разработанные методы синтеза матричных операций [2, 3] позволили реализовать метод защиты информационных ресурсов на основе матричных операций криптографического преобразования, алгоритм работы которого представлен в [4].

С целью оценки эффективности применения матричных операций криптографического преобразования для защиты информации было создано программное обеспечение, которое реализует алгоритм работы предложенного метода защиты информации на основе вышеуказанных операций.

С помощью пакета тестов NIST STS произведено тестирование результатов криптографического преобразования. Пакет NIST STS содержит 15 статистических тестов, какие разработаны для проверки гипотезы относительной случайности двоичных последовательностей произвольной длины [5].

Тестирование проводилось с такими параметрами: длина последовательности, которая тестируется, $n=10^6$ бит; количество последовательностей, которые тестируются, $m=100$; уровень значимости $\alpha=0{,}01$; количество тестов $q=189$. Таким образом, объем выборки, которая тестируется, составлял $N=10^6\times100=10^8$ бит, количество тестов (q) для разной длинны $q=189$, а статистический портрет генератора содержит 18 900 значений вероятности P.

Метод защиты информационных ресурсов на основе матричных операций криптографического преобразования был применен для улучшения характеристик псевдослучайных последовательностей (ПСП) [4], которые генерируются с помощью стандартной функции random. Проведено тестирование статистических свойств последовательностей, полученных в результате применения операций матричного криптографического преобразования. Статический портрет программной реализации матричного генератора изображен на рис. 1.

Сводные результаты тестирования матричного генератора (на основе random) программным пакетом NIST-STS представлены в табл. 1.

Как видно из результатов, генератор ПСП, реализованный на базе матричного генератора на основе стандартной функции random, прошел комплексный контроль по методике NIST STS.

Разработан алгоритм формирования ПСП на основе операций матричного преобразования числовой или текстовой информации. Сводные результаты тестирования

матричного преобразования неслучайной монотонно возрастающей последовательности с циклом повторения 64 байта и 256 байт программным пакетом NIST-STS представлены в табл. 2.

Исследуемая последовательность с циклом повторения 256 байт не прошла комплексный контроль по методике NIST STS, так как был не пройден 1 тест: NonOverlappingTemplate; P-VALUE=0.213309; PROPORTION=0.9500.

Осуществлена модификация алгоритма криптографического матричного преобразования с помощью добавления блока криптографического преобразования группой операций инверсии результатов матричного преобразования. Статический портрет программной реализации алгоритма модифицированного матричного преобразования неслучайной монотонно возрастающей последовательности с циклом повторения 256 байт показан на рис. 2, а сводные результаты тестирования, представленные в табл. 3, подтверждают прохождение комплексного контроля по методике NIST-STS.

Осуществлена проверка статистических свойств результатов матричного криптографического преобразования текстовой информации на примере электронных информационных ресурсов, а именно художественной литературы в текстовом формате. Статистический портрет программной реализации алгоритма матричного криптографического преобразования текстового файла изображен на рис. 3 [5].

Обобщённые результаты тестирования модифицированного матричного криптографического преобразования текстового файла программным пакетом NIST STS представлены в табл. 4 подтверждаю прохождение пакета тестов.

Таблица 1. *Сводные результаты тестирования матричного генератора*

Генератор	Количество тестов, в которых тестирование прошло	
	99% послед.	96% послед.
Матричный генератор на основе random	150 (79,4%)	189 (100%)

Таблица 2. *Сводные результати тестирования матричного преобразования*

Генератор	Количество тестов, в которых тестирование прошло	
	99% послед.	96% послед.
Матричное криптографическое преобразование (с циклом 64 байта)	129 (68,3%)	189 (100%)
Матричное криптографическое преобразование (с циклом 256 байт)	136 (71,9%)	188 (99,5%)

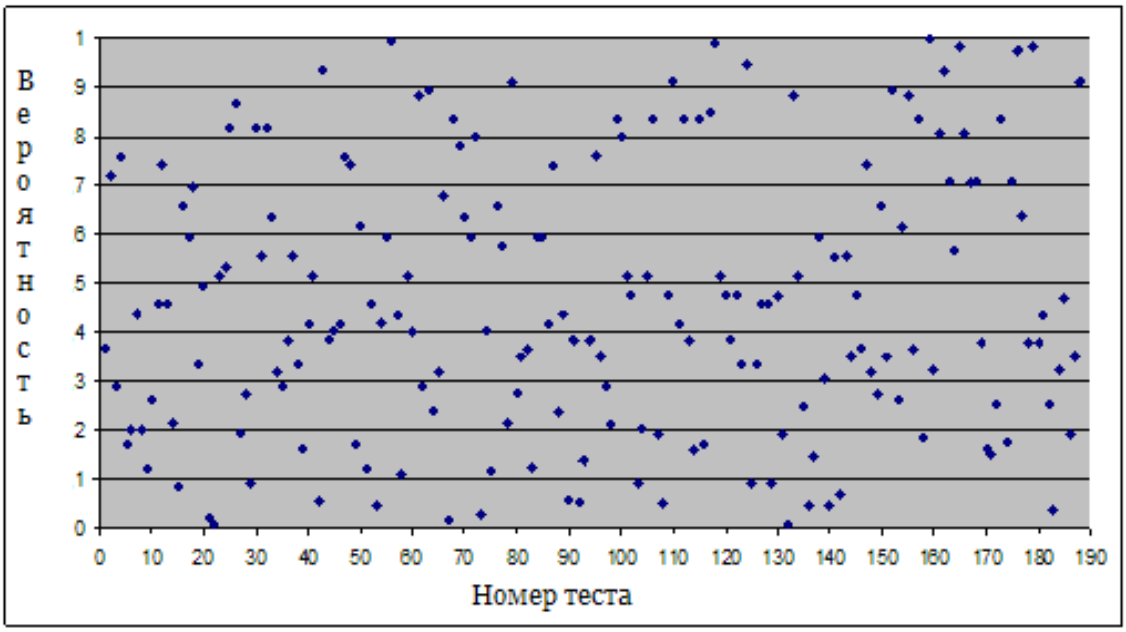


Рис. 1. *Статистический портрет программной реализации матричного генератора*

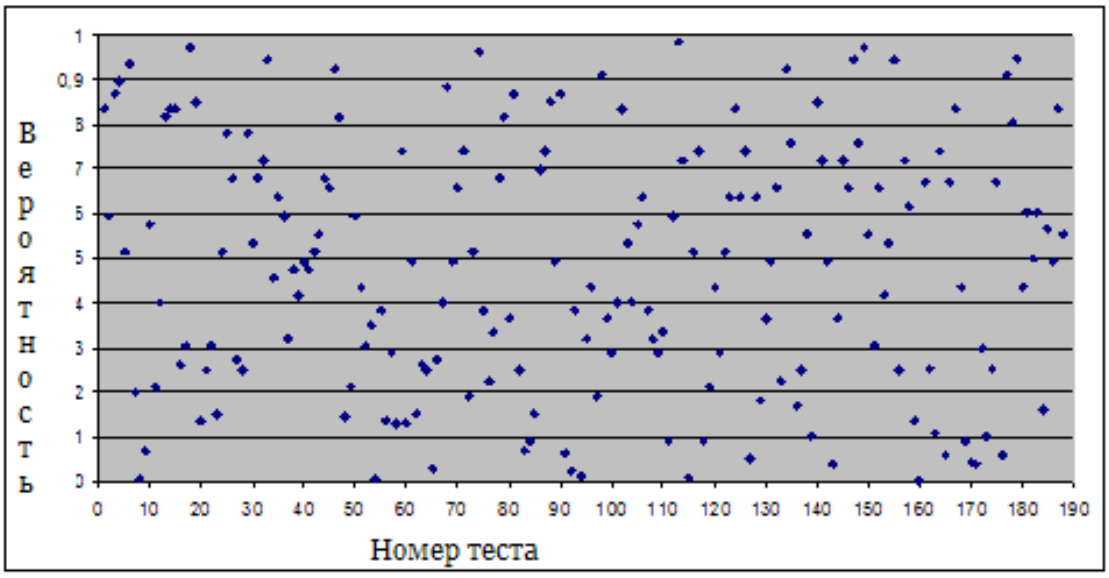


Рис. 2. *Статистический портрет программной реализации алгоритма модифицированного матричного преобразования неслучайной монотонно возрастающей последовательности с циклом повторения 256 байт*

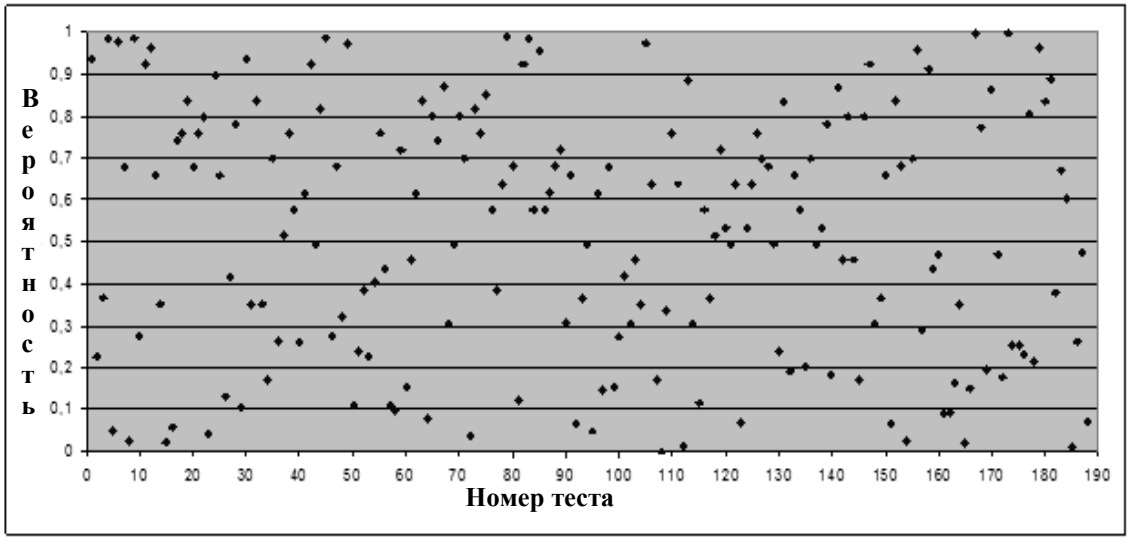


Рис. 3. *Статистический портрет программной реализации алгоритма матричного криптографического преобразования текстового файла*

Таблица 3. *Сводные результати тестирования модифицированным алгоритмом*

Генератор	Количество тестов, в которых тестирование прошло	
	99% послед.	96% послед.
Модифицированное матричное криптографическое преобразование	132 (69,8%)	189 (100%)

Таблица 4. *Обобщённые результаты тестирования данных*

Генератор	Количество тестов, в которых тестирование прошло	
	99% послед.	96% послед.
Модифицированное матричное криптографическое преобразование	129 (68,3 %)	189 (100 %)

Повысить скорость работы системы защиты информации на основе матричных операций криптографического преобразования по модулю два можно за счет распараллеливания процесса выполнения преобразования над данными. Для осуществления данного предложения применим основную идею подхода, основанного на параллелизме данных, которая заключается в том, что одна операция выполняется сразу над всеми элементами массива данных. В нашем случае такой операцией будет элементарная операция матричного криптографического преобразования. Различные фрагменты такого массива обрабатываются на векторном процессоре или на разных процессорах параллельной машины [6]. Задачу распределения данных между процессорами нужно реализовывать программно.

Один из вариантов реализации алгоритма параллельного выполнения матричного криптографического преобразования изображен на рис. 4.

Анализ результатов расчета коэффициента быстродействия при использовании три и четырехразрядных матричных преобразований [7] изображен на рис 5, где n_k – разрядность команды выполнения последовательностей операций криптопреобразования соответственно

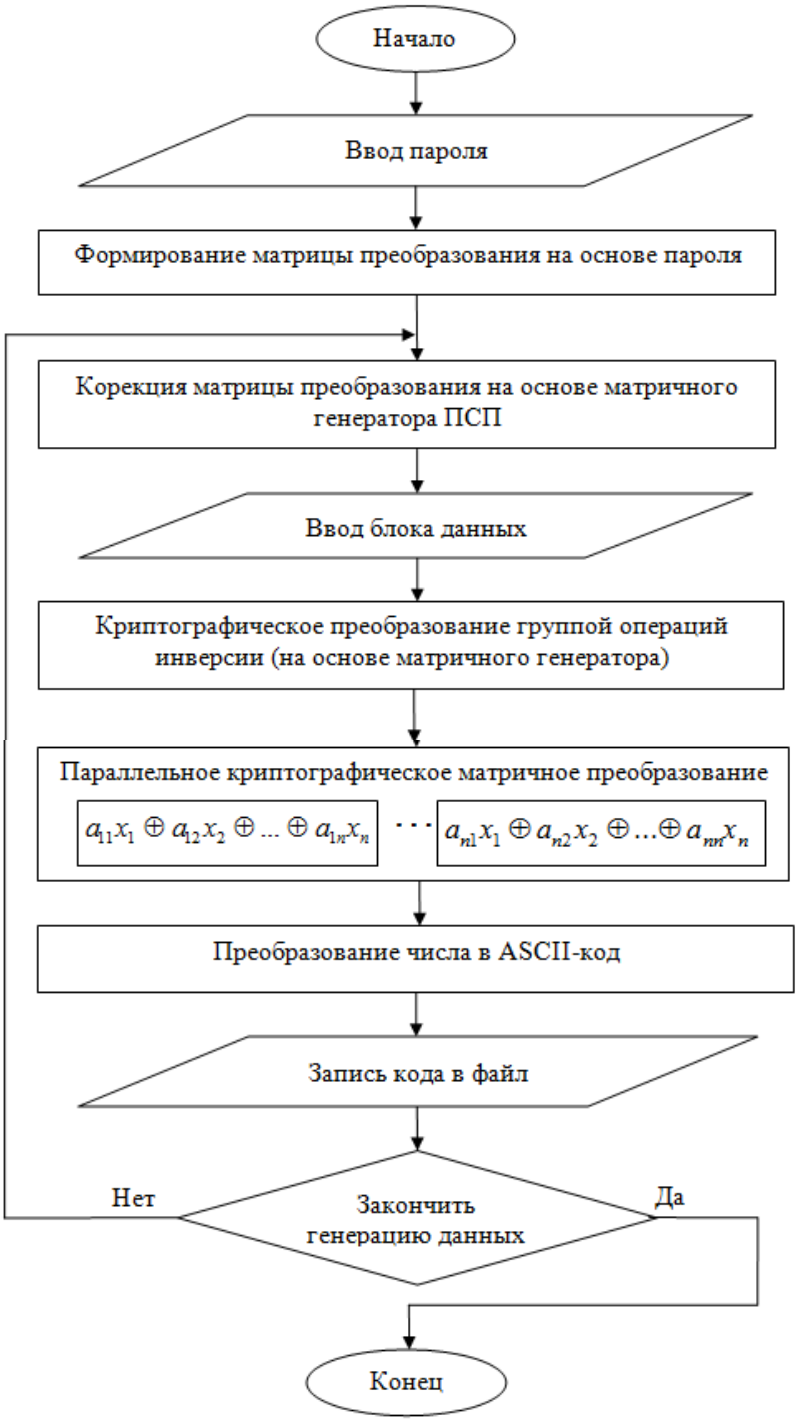
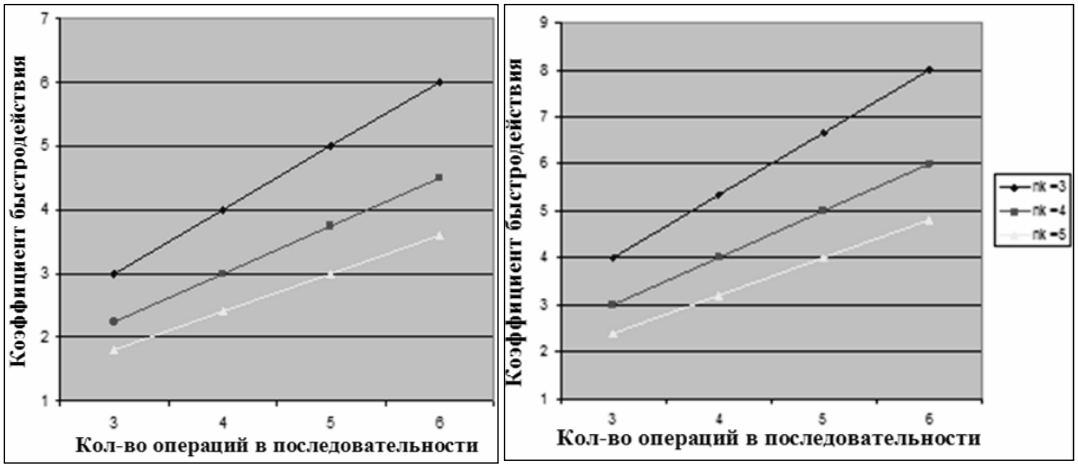


Рис. 4. *Алгоритм с параллельным выполнением операции матричного криптографического преобразования*



а) б)

Рис. 5. *Результаты расчета коэффициента быстродействия: а) трехразрядные матричные преобразования; б) четырехразрядные матричные преобразования*

Использование разработанного способа параллельного выполнения операций криптографического преобразования обеспечивает повышение показателей быстродействия системы защиты информационных ресурсов, а также дает возможность гибкого управления необходимыми значениями скорости шифрования и криптостойкости за счет увеличения аппаратной и программной сложности реализации системы криптографической защиты информации.

Работа частично поддержана ФЦП «Научные и научно-педагогические кадры инновационной России» на 2009–2013 годы (соглашение № 14.B37.21.1934).

СПИСОК ЛИТЕРАТУРЫ

1. Б. Шнайер. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си. Издательство ТРИУМФ, М., 2002. – 816 с.
2. Рудницький В.М. Метод синтезу матричних моделей операцій криптографічного кодування та декодування інформації / В.М. Рудницький, В.Г. Бабенко, С.В. Рудницький // Збірник наукових праць Харківського університету повітряних сил. – Вип. 4 (33). – Х.: ХУПС ім. І. Кожедуба, 2012. – С. 198–200.
3. Рудницький В.М. Метод синтезу матричних моделей операцій криптографічного перекодування інформації / В.М. Рудницький, В.Г. Бабенко, С.В. Рудницький // Захист інформації : наук.-практ. журн. – № 3 (56). – К.: НАУ, 2012. – С. 50–56.
4. Бабенко В.Г. Реалізація методу захисту інформації на основі матричних операцій криптографічного перетворення / В.Г. Бабенко, С.В. Рудницький // Системи обробки інформації: зб. наук. праць. – № 9 (107). – Х.: ХУПС імені. І. Кожедуба, 2012. – С. 163–168.
5. Потій А.В. Статистичне тестування генераторів випадкових і псевдовипадкових чисел з використанням набору статистичних тестів NIST STS [Електронний ресурс] / А.В. Потій, С.Ю. Орлова, Т.А. Гриненко. – Режим доступу: //www.kiev-security.org.ua
6. Мельников Б.Ф. Принятие решений в прикладних задачах с применением динамически подобранных фунцкий риска / Б.Ф. Мельников, С.В. Пивнева // Вестник транспорта Поволжья. – 2010.– № 3. С. 28–33.
7. Рудницкий С.В. Криптографическое преобразование информации на основе трехразрядных логических функций / С.В. Рудницкий, Р.П. Мельник, В.В. Веретельник // Вектор науки Тольяттинского государственного университета. – 2012. – № 4 (22). С. 119–122.

METHOD OF PARALLEL IMPLEMENTATION OF THE MATRIX OPERATIONS OF CRYPTOGRAPHIC TRANSFORMATIONS

V.N. Rudnicki, doctor of technical sciences, professor of systems programming
Cherkasy State Technological University, Cherkassy (Ukraine)
E.V. Kozlov, candidate of physical and mathematical sciences, associate professor
Samara State University of Railway Transport, Samara (Russia)
V.G. Babenko, doctoral candidate
Odessa National Academy of Telecommunications named after O.S. Popov, Odessa (Ukraine)

Keywords: operation of cryptographic transformation; the matrix; parallel execution, encryption speed; cryptographic strength, coefficient of performance.

Annotation: In the work we propose a way to increase the speed of the method of information security based on cryptographic transformation matrix operations by parallelizing the process of the operation of cryptographic transformation matrix. The analysis of the coefficient of speed confirms the efficiency of the parallel implementation of the algorithm.