УДК 004.056: 061.068

ШИФРОВАНИЕ ДАННЫХ НА ОСНОВЕ ДИСКРЕТНЫХ ХАОТИЧЕСКИХ СИСТЕМ И ОТОБРАЖЕНИЙ

А.В. СИДОРЕНКО, К.С. МУЛЯРЧИК

Белорусский государственный университет,
пр. Независимости, 4, 220050, Минск, Беларусь

Поступила в редакцию 1 ноября 2012

Рассматривается алгоритм шифрования данных, имеющий в своей основе обобщенную схему блочного симметричного алгоритма шифрования и использующий дискретные хаотические системы и отображения. Сравнительный анализ зашифрованных последовательностей методом задержанной координаты и построением фазовых диаграмм с известными алгоритмами шифрования на основе динамического хаоса позволяет выделить его преимущества: повышение степени защищенности информации, скорости и эффективности обработки данных, расширение функциональных способностей при решении криптографических задач. Рассматриваются особенности программной и аппаратной реализации предложенного алгоритма.

Ключевые слова: шифрование, информация, алгоритм, дискретное отображение, хаос.

Введение

Информационные технологии проникают практически во все сферы деятельности человека. Стремительный рост объемов и ценности информации способствует разработке новых методов и средств ее защиты. Важнейшим средством обеспечения конфиденциальности передаваемой информации является шифрование.

В настоящее время получили широкое распространение блочные симметричные алгоритмы шифрования. Среди них наиболее известны AES [1], ГОСТ 28147-89 [2], DES [3] и др. В Республике Беларусь разработан и принят в качестве стандарта алгоритм шифрования BelT [4]. Вместе с тем, во всем мире постоянно ведутся исследования по разработке новых алгоритмов шифрования [5, 6].

Одним из перспективных направлений в современной криптографии является разработка и исследование алгоритмов шифрования на основе динамического хаоса [7, 8]. Применение методов хаотической динамики для шифрования данных обладает большим потенциалом, что обусловлено общностью фундаментальных свойств хаоса и криптографии. Среди таких свойств выделяются: высокая чувствительность к начальным условиям, случайность траекторий, рассеивание и запутывание.

Развитие теории дискретного хаоса привело к появлению новых криптографических алгоритмов и примитивов. Тем не менее, большинство из них, в частности [9–12], имеет низкую степень защищенности информации, невысокую скорость и эффективность шифрования.

В предлагаемой работе рассматривается алгоритм шифрования на основе дискретных хаотических систем и отображений, представлены результаты анализа алгоритма и его преимущества, описана программно-аппаратная реализация рассматриваемого алгоритма.

Элементы обобщенной схемы блочного симметричного алгоритма шифрования

Для рассматриваемого блочного алгоритма шифрования характерным является использование прямого и обратного преобразования (зашифрования и расшифрования). При этом об-

Библиотека БГУИР

ратное преобразование (расшифрование) зашифрованного текста в открытый текст аналогично по своей структуре и свойствам прямому преобразованию – зашифрованию [6]. В процессе реализации шифрования осуществляется разбиение обрабатываемого текста на блоки фиксированной длины и их последовательная обработка.

Открытый текст произвольного объема X, подлежащий обработке, разбивается на блоки фиксированной длины ($X_1, X_2, ..., X_N$). В результате последовательной обработки каждого блока X_i на выходе формируются блоки Y_i, входящие в состав выходного текста Y. Для обеспечения взаимосвязи блоков текста используются внутренние вспомогательные блоки A и B. Типичными размерами входных и выходных блоков текста для современных блочных алгоритмов являются: 64, 128, 192 или 256 бит. Непосредственное преобразование блоков текста осуществляется функциональным компонентом, определяемым как блок «основной шаг», внутренняя структура которого приведена на рисунке.

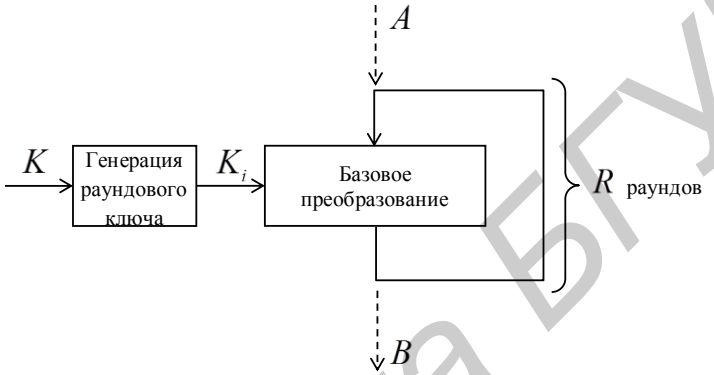


Рис. 1. Внутренняя структура функционального блока «основной шаг»

В функциональном блоке «основной шаг» к блоку текста многократно (R раундов) последовательно применяется базовое преобразование, управляемое раундовым ключом K_i, который генерируется из ключа шифрования K. A и B обозначают направления внутренних вспомогательных блоков взаимосвязи текста. Использование нескольких раундов обусловлено необходимостью обеспечения перемешивающих свойств алгоритма шифрования. Количество раундов шифрования определяется в зависимости от используемого базового преобразования и должно быть достаточным для обеспечения требуемой степени защищенности информации [13]. Указанный блок является «ядром» алгоритма шифрования и определяет его криптографические и вычислительные свойства. На данном уровне устанавливают: конкретный вид процедуры генерации раундового ключа; конкретный вид базового преобразования, в т.ч. длину входного и выходного блоков текста; длину раундового ключа K_i; конкретное количество раундов базового преобразования.

Алгоритм шифрования, его анализ и сравнение с аналогами

Анализ алгоритмов шифрования на основе динамического хаоса показывает, что основными задачами, решаемыми в процессе разработки новых алгоритмов, являются: повышение криптостойкости алгоритма и степени защищенности информации; повышение скорости и эффективности работы; расширение функциональных возможностей.

В основу разрабатываемого алгоритма шифрования положена обобщенная схема блочного симметричного алгоритма шифрования. В функциональном компоненте алгоритма, определяемом как «основной шаг», в качестве базового преобразования используется сеть Фейстеля, в которой в качестве нелинейного элемента применяется дискретное хаотическое отображение. Анализ степени хаотичности выходных (зашифрованных) последовательностей проводится построением фазовых диаграмм и использованием метода задержанной координаты. Это позволило определить необходимое количество раундов базового преобразования и оценить степень криптостойкости алгоритма по параметрам корреляционной размерности и энтропии

Библиотека БГУИР

Колмогорова. Допустимые режимы работы алгоритма, при которых достигается приемлемый уровень защищенности информации, – CBC и CFB.

Сеть Фейстеля относится к хорошо изученной структуре базового преобразования, основными преимуществами которой являются [14, 15]: использование одной структуры базового преобразования и для зашифровывания, и для расшифровывания; применение необратимой нелинейной функции; однородное перемешивание в обрабатываемом блоке (т. е. все байты блока в равной степени участвуют в преобразовании); простота аппаратно-программной реализации.

Использование сети Фейстеля, в отличие, например, от алгоритма Kocarev et al., описанного в работе [9], позволяет повысить скорость и эффективность работы алгоритма путем снижения структурной сложности и потребности в вычислительных ресурсах. В качестве нелинейного преобразования в алгоритме шифрования применяется дискретное хаотическое отображение. Использование хаотического отображения, в отличие от таблиц подстановки в алгоритме Kocarev et al., для обеспечения свойства перемешивания позволяет: отказаться от построения и подбора таблиц подстановки; получать различные нелинейные преобразования путем варьирования параметрами хаотического отображения.

Важной особенностью дискретных хаотических систем является то, что указанные системы определяются на множестве целых чисел, что устраняет недостаток, заключающийся в использовании арифметики с плавающей запятой и процедуры дискретизации непрерывного хаотического отображения, которые присущи ряду алгоритмов шифрования на основе динамического хаоса [9–12]. К тому же, применение целочисленной арифметики является необходимым условием в криптографии.

Исследования открытого текста и полученных описанным алгоритмом зашифрованных текстов проводились путем визуальной оценки фазовых диаграмм и оценки значений корреляционной размерности и энтропии Колмогорова входных и выходных последовательностей. Результаты анализа позволили оценить криптостойкость алгоритма в сравнении с известными алгоритмами, а также оценить минимальное необходимое количество раундов базового преобразования, что обеспечивает более высокий уровень защищенности информации.

На рис. 2, 3 изображены графики зависимости корреляционной размерности и энтропии Колмогорова от количества раундов базового преобразования для открытого текста (1), алгоритма шифрования Kocarev et al. (2) и разрабатываемого алгоритма шифрования (3). Как видно из графиков (рис. 2, 3), приведенных для режима работы CBC, разрабатываемый алгоритм при определенных условиях обладает более предпочтительными характеристиками. Количество итераций определено в промежутке 64–256 для режима CBC.

На рис. 4 изображена фазовая диаграмма открытого текста. На рис. 5 изображены фазовые диаграммы зашифрованных текстов, соответствующих данному открытому тексту, полученные разрабатываемым алгоритмом и алгоритмом Kocarev et al. На основании визуального анализа представленных фазовых диаграмм можно сделать вывод о том, что при использовании разрабатываемого алгоритма траектории максимально заполняют фазовое пространство, что говорит об их значительной расходимости, и, следовательно, о надежной защите шифруемой информации.

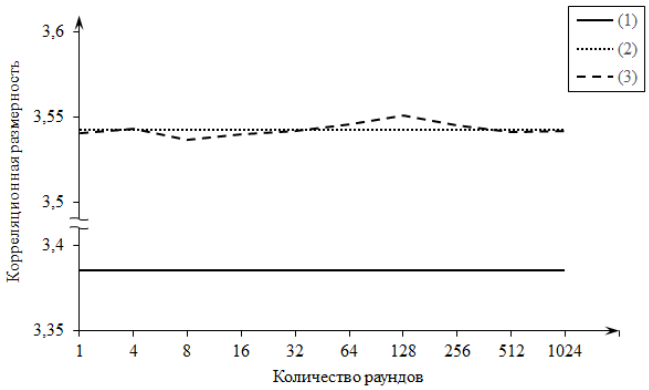


Рис. 2. Зависимость корреляционной размерности от количества раундов базового преобразования в режиме работы CBC

Библиотека БГУИР

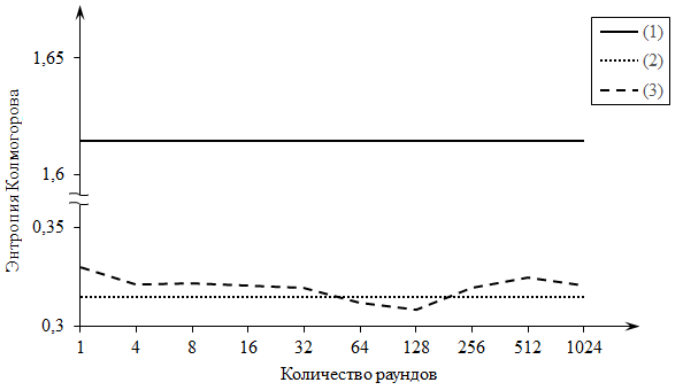


Рис. 3. Зависимость энтропии Колмогорова от количества раундов базового преобразования в режиме работы CBC

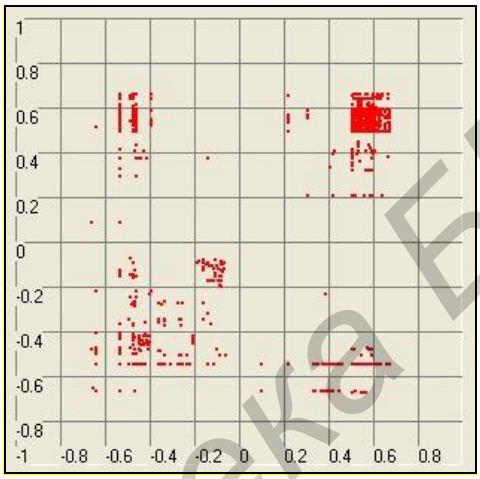
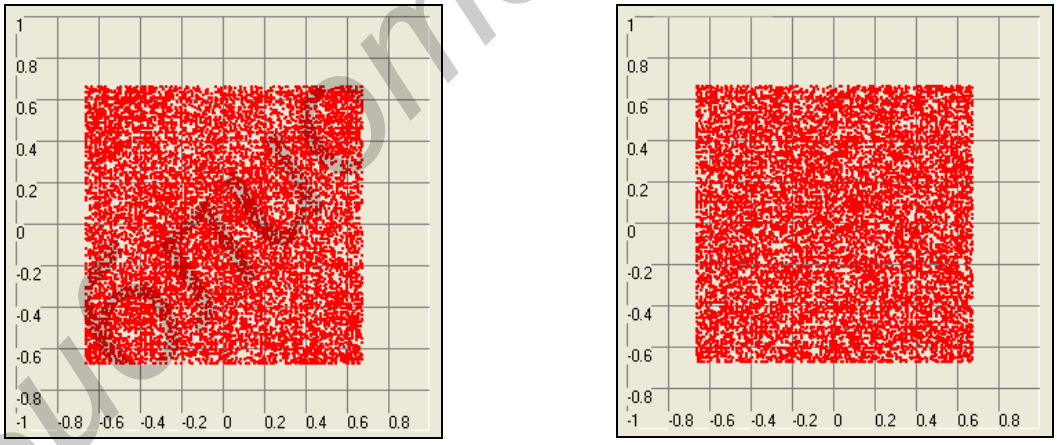


Рис. 4. Фазовая диаграмма открытого текста



а *б*

Рис. 5. Фазовые диаграммы зашифрованных последовательностей, полученных в режиме CBC: *а* – разрабатываемым алгоритмом; *б* – алгоритмом Kocarev et al.

Таким образом, в сравнении с известными алгоритмами шифрования на основе динамического хаоса [9–12], предложенный в данной статье работе алгоритм позволяет повысить степень защищенности информации, скорость и эффективность шифрования. Разрабатываемый алгоритм позволяет также расширить функциональные возможности при решении криптографических задач за счет применения дискретных хаотических отображений [16].

Библиотека БГУИР

Программно-аппаратная реализация алгоритма шифрования

Программная реализация алгоритма шифрования, выполненная при использовании компьютерных средств, в ряде случаев способна обеспечить большую скорость обработки информации. Среди достоинств аппаратных шифраторов, выполненных на базе узкоспециализированных микроконтроллеров, следует выделить [14]: аппаратную реализацию алгоритма гарантирует его целостность; шифрование и хранение ключей осуществляются в самой плате шифратора, а не в оперативной памяти компьютера; аппаратный датчик случайных чисел создает действительно случайные числа для формирования надежных ключей шифрования и векторов инициализации; на базе аппаратных шифраторов можно создавать системы защиты информации от несанкционированного доступа и разграничения доступа к компьютеру.

Аппаратная реализация алгоритма шифрования выполнена на базе сверхширокополосных приемопередатчиков ППС-40А, использующих в своей основе RISC-микроконтроллер Atmel серии ATmega. Она осуществлена путем модификации основного программного кода прошивки микроконтроллера, что позволило выполнить следующие функции:

– зашифрование подготовленного к отправке пакета данных;

– расшифрование принятого пакета данных;

– конфигурирование криптографических параметров.

В качестве среды разработки программного кода алгоритма шифрования использован пакет Atmel AVR Studio 5.0. Для обеспечения совместимости исходного программного кода прошивки микроконтроллера и реализуемых модификаций в качестве языка программирования выбран язык AVR RISC ассемблер. При этом набор возможных инструкций определяется моделью микроконтроллера.

Для проверки работы сверхширокополосных приемопередатчиков со встроенным алгоритмом шифрования развернута опытная сеть передачи данных, схематично изображенная на рисунке.

Рис. 6. Схема опытной сети передачи данных

Сверхширокополосный приемопередатчик ПП1 запрограммирован на работу в автономном режиме, ПП2 – на работу в режиме координатора сети. Приемопередатчик ПП1 регистрирует данные с подключенного к нему сенсора через заданный интервал времени, формирует пакет данных и отправляет его в зашифрованном виде в эфир. Сверхширокополосный приемопередатчик ПП2 прослушивает эфир, принимает пакет данных, расшифровывает его и отправляет для дальнейшей обработки в ПК.

В результате проведенных исследований установлено, что аппаратная реализация алгоритма шифрования обладает следующими характеристиками:

– объем программного кода – 625 байт;

– объем памяти для хранения переменных – 255 байт;

– скорость обработки данных (при частоте процессора 2 ГГц) в режиме СВС – 8,6 Мбит/с.

Реализация алгоритма на программно-аппаратной платформе позволит использовать алгоритм шифрования в различных практических приложениях: смарт-карты, электронные ключи и другие средства защиты информации.

Заключение

Предложен алгоритм шифрования, в основе которого лежат схема блочного симметричного алгоритма шифрования и дискретные хаотические отображения.

Проведен сравнительный анализ выходных последовательностей зашифрованного текста с использованием построения фазовых диаграмм и метода задержанной координаты.

Библиотека БГУИР

Установлено, что предложенный алгоритм повышает степень защищенности шифруемой информации, скорость и эффективность обработки данных, а также расширяет функциональные возможности при решении криптографических задач благодаря особым свойствам хаотических отображений.

Выполнена реализация предложенного алгоритма шифрования на программно-аппаратной платформе, что позволяет его использовать в различных практических приложениях.

THE DATA ENCRYPTION BASED ON DISCRETE CHAOTIC SYSTEMS AND MAPS

A.V. SIDORENKO, K.S. MULYARCHIK

Abstract

The encryption algorithm based on scheme of block symmetric encryption algorithm and used the discrete chaotic systems and maps is presented. Comparative analysis of encryption sets by delayed coordinate method and construction of phase diagrams with famous encryption algorithms based on dynamic chaos is allowed to revealed it's preferences: increasing of degree defence information, speed and effectiveness of date processing, spreading of functional possibilities in decision cryptography problems. The peculiarities of software and apparatus realization of algorithm are considered.

Список литературы

1. FIPS Publication 197. Specification for the Advanced Encryption Standard. [Электронный ресурс]. – Режим доступа: http://www.csrc.nist.gov. – Дата доступа: 1.07.2012.
2. ГОСТ 28147-89. Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования.
3. FIPS 46-3. Data Encryption Standard (DES). [Электронный ресурс]. – Режим доступа: http: www.csrc.nist.gov. – Дата доступа: 1.07.2012.
4. СТБ 34.101.31-2011. Информационные технологии. Защита информации. Криптографические алгоритмы шифрования и контроля целостности.
5. *Guodong Ye, Kwok-Wo Wong* // Nonlinear dynamics. 2012. № 4 (69). P. 2079–2087.
6. *Satyaki Roy, Navajit Maitra, Shalabh Agarwal et. al.* // International Journal of Modern Education and Computer Science. 2012. № 7 (4). P. 50–56.
7. *Kocarev L.* // IEEE Circuits and Systems Magazine. 2001. № 1. P. 6–21.
8. *Сидоренко А.В., Мулярчик К.С.* // Информатика. 2011. №1. С. 95-106.
9. Патент США US007106864B2. Chaos-based data protection using time-discrete dynamical systems / L. Kocarev, G. Jakimoski, G. Rizzotto, P. Amato.
10. Патент США US005696826A. Method and apparatus for encrypting and decrypting information using a digital chaos signal / Z. Gao.
11. Патент США US005751811A. 32N+D bit key encryption-decryption system using chaos / J. Magnotti, L. Nelson.
12. Патент США 5048086. Encryption system based on chaos theory / M. Bianko, D. Reed.
13. *Шемякина О.В.* // Дискретная математика. 2011. № 2 (23). С. 32–40.
14. Панасенко, С.П. Алгоритмы шифрования / С.П. Панасенко // Специальный справочник. – СПб.: БХВ-Петербург, 2009. – С. 564
15. *Котегов М.Г., Трунов И.Л., Серогодский Д.И.* // Современные наукоемкие технологии. 2008. № 3. С. 51–52.
16. *Sidorenko A.V., Mulyarchik K.S.* // Nonlinear Phenomena in Complex Systems. 2012. № 1 (15). P. 95–104.

Библиотека БГУИР