схемасын қолданылды. Нәтижесінде, табылған мұрын қуысындағы жылдамдық және температура профильдері белгілі сандық есептеу нәтижелерімен тексерілді. Сандық модельдеу нәтижелері адам мұрын арқылы қалыпты тыныс алған кезінде ауаның альвеолярлық қалыпқа жетуге жеткілікті уақыт бар екенін көрсетеді. Мұрын қуысының ішкі құрлысы ауаның жылу және ылғалдандыру үдерістеріне себептеседі.

Түйінді сөздер: адам тыныс алу жүйесінің ауа ағынының, альвеолярлы қалып, екі өлшемді компьютерлік моделдеу, мұрын қуысындағы жылуалмасу, Навье-Стокс теңдеулері, аралық көлемдер әдісі.

A. Issakhov, A.M. Yessenkozha

Numerical simulation of air flow in the human respiratory system

Symmary. Nasal inspiration is important for maintaining the internal milieu of the lung, since ambient air is conditioned to nearly alveolar conditions (body temperature and fully saturated with water vapor) on reaching the nasopharynx. We conducted a two-dimensional computational study of transport phenomena in model transverse cross sections of the nasal cavity of normal human noses based on the Navier-Stokes equation. For solution of the Navier-Stokes equations applied projection method. The results suggest that during breathing via the normal human nose there is ample time for heat and water exchange to enable equilibration to near intraalveolar conditions. A normal nose can maintain this equilibrium under extreme environments. The turbinates increase the rate of local heat and moisture transport by narrowing the passageways for air and by induction of laminar swirls downstream of the turbinate wall.

Keywords: Respiratory air conditioning, alveolar condition, 2D modeling, heat transfer, Navier-Stokes equations, finite volume method

УДК 004.056.5

С. Е. Нысанбаева, М. М. Магзом
(Институт информационных и вычислительных технологий КН МОН РК,
Алматы, Республика Казахстан, magzomxzn@gmail.com)

МОДЕЛЬ НЕТРАДИЦИОННОГО АЛГОРИТМА ШИФРОВАНИЯ НА ОСНОВЕ ВЛОЖЕННЫХ СЕТЕЙ ФЕЙСТЕЛЯ

Аннотация. Цель исследования – изучение возможностей практического применения алгоритма шифрования на базе непозиционных полиномиальных систем счисления с использованием схемы вложенных сетей Фейстеля. В данной работе рассмотрена математическая модель нетрадиционного алгоритма шифрования с рекурсивной структурой сети Фейстеля и режимом шифрования.

Ключевые слова: криптографическая система, алгоритм шифрования, модулярная арифметика, сеть Фейстеля, режимы шифрования.

ВВЕДЕНИЕ

Увеличение масштабов современных информационных систем повышает потребность в стойких и эффективных средствах, обеспечивающих информационную безопасность при хранении и передачи данных. Наибольший интерес сегодня вызывают такие направления теоретических и прикладных исследований, как создание и анализ надежности криптографических алгоритмов и протоколов.

Описываемая в данной статье система шифрования применяет нетрадиционный алгебраический метод, который основывается на теории непозиционных полиномиальных систем счисления (НПСС) в остаточных классах. Синонимами НПСС является полиномиальная система остаточных классов, модулярная арифметика.

Классическая модулярная арифметика базируется на «Китайской теореме об остатках», которая гласит, что любое число может быть представлено своими остатками (вычетами) от деления на систему оснований, в качестве которой выбираются попарно простые числа [1]. Отличие предлагаемого метода от классических систем в остаточных классах заключается в том, в полиномиальных системах счисления в остаточных классах основаниями служат не простые числа, а неприводимые многочлены над полем GF(2).

Нетрадиционный подход, основанный на применении непозиционных полиномиальных систем счисления, позволяет повысить надежность алгоритма шифрования и увеличить скорость

шифрования, т.к. в соответствии с правилами НПСС все арифметические операции могут выполняться параллельно по модулям оснований НПСС.

Нетрадиционный алгоритм шифрования на базе НПСС

Для шифрования электронного сообщения длиной N бит формируется НПСС: из множества всех неприводимых многочленов степени не выше значения N выбираются рабочие основания

$$p_1(x), p_2(x),\ldots,p_S(x)\cdot \tag{1}$$

Выбранные полиномы (1) составляют одну систему оснований, в которой также важен порядок их расположения. Рабочий диапазон данной системы определяется многочленом $P(x)=p_1(x)\,p_2(x)\cdots p_S(x)$ степени m:

$$m=\sum_{i=1}^{S} m_i,$$

где S – число выбранных рабочих оснований, а m_i – степень соответствующего основания $p_i(x)$.

Все выбираемые основания (1) должны отличаться друг от друга, то есть быть уникальными для этой системы. Тогда, согласно условиям китайской теоремы об остатках, в данной системе любой многочлен степени меньше m имеет единственное представление в виде последовательности остатков (вычетов) от деления его на основания (1).

После формирования системы оснований, блок открытого текста длиной N бит может быть представлен в виде последовательности вычетов $\alpha_1(x),\alpha_2(x),\ldots,\alpha_S(x)$ от деления некоторого многочлена $F(x)$ на рабочие основания $p_1(x), p_2(x),\ldots, p_S(x)$:

$$F(x)=(\alpha_1(x),\alpha_2(x),\ldots,\alpha_S(x)), \tag{2}$$

где $F(x)\equiv\alpha_i(x)\big(mod\ p_i(x)\big), i=\overline{1,S}$.

Таки же образом интерпретируется секретный ключ длины N бит в построенной НПСС. Он представляется как система вычетов $\beta_1(x),\beta_2(x),\ldots,\beta_S(x)$ но от деления некоторого другого многочлена $G(x)$ по тем же рабочим основаниям системы:

$$G(x)=(\beta_1(x),\beta_2(x),\ldots,\beta_S(x)), \tag{3}$$

где $G(x)\equiv\beta_i(x)\big(mod\ p_i(x)\big), i=\overline{1,S}$.

Процедура нетрадиционного шифрования рассматривается как некоторая функция $H(F(x),G(x))$ от представлений (2) открытого текста и (3) секретного ключа. Полученная криптограмма также записывается в виде непозиционного представления - последовательности вычетов $\omega_1(x),\omega_2(x),...,\omega_S(x))$:

$$H(x)=(\omega_1(x),\omega_2(x),...,\omega_S(x)), \tag{4}$$

где $H(x)\equiv\omega_i(x)(\mathrm{mod}\ p_i(x)), i=\overline{1,S}$.

Криптостойкость этого алгоритма шифрования определяется полным секретным ключом, который включает систему рабочих оснований (1) и секретный ключ (3).

Моделирование нетрадиционного алгоритма шифрования

Для построения (разработки) модели нетрадиционного блочного шифрования применяется схема Фейстеля, которая приобрела широкую популярность при разработке симметричных блочных шифров. Схема Фейстеля является методом смешивания подблоков входного текста в шифре посредством повторяющегося применения зависящих от раундовых ключей нелинейных функций, называемых F-функциями и выполнения перестановок подблоков [3,4]. В стандартной сети Фейстеля открытый текст разбивается на два равных подблока. В общем случае, сеть Фейстеля может разбивать входной блок на $n \geq 2$ подблоков. Далее подразумевается, что все подблоки имеют

одинаковую длину, так что каждый подблок может участвовать в транспозиции с любым другим подблоком. Обобщенная схема обмена является перестановкой $n \geq 2$ подблоков в одном раунде. Сети Фейстеля были широко изучены в силу их широкого использования при разработке алгоритмов шифрования.

В ходе разработки непозиционного алгоритма шифрования были рассмотрены несколько моделей схемы Фейстеля. Модели отличаются структурой сети, количеством подблоков и числом раундов.

В работе [5] были описаны модификации нетрадиционного алгоритма шифрования с испольщованием сети Фейстеля в качестве пред- и постобработки блока шифруемых данных.

В отличии от традиционной сети Фейстеля, где входными данными является открытый текст сообщения, в модели с постобработкой на вход подаётся битовая последовательность шифротекста, получаемая при шифровании нетрадиционным алгоритмом.

В модели с предобработкой блок открытого текста предварительно шифруется по классической схеме Фейстеля, после чего преобразуется нетрадиционным методом шифрования.

Шифрование в разрабатываемой модели с использованием вложенной сети Фейстеля выполняется по следующей схеме, показанной на рисунке 1.

Входной блок делиться на две равные части L_0 и R_0. Правая часть R_0 проходит через функцию преобразования G, которая является вложенной сетью Фейстеля. В результате преобразованный подблок R_0 умножается по модулю 2 с левым подблоком L_0 и становится правой частью R_1 входного блока для следующего раунда сети Фейстеля, а неизмененный подблок R_0 переставляется на место левого блока подблока L_1 в следующей итерации.

Функция преобразования G также представляет собой сеть Фейстеля. Входной блок данных, полученный из узла сети верхнего уровня делиться на две равные части L'_0 и R'_0.

Подблок R'_0 кодируется процедурой нетрадиционного шифрования (4) с использованием раундового ключа K_i. Согласно (2), правая сторона подблока R'_0 представляется в виде последовательности вычетов $\alpha_1(x), \alpha_2(x), \ldots, \alpha_S(x)$, а раундовый ключ KI представляется в виде системы вычетов $\beta_1(x), \beta_2(x), \ldots, \beta_S(x)$, в соответствии с (3). Тогда зашифрованный подблок получается в виде операции

$$F(x)G(x) \equiv H(x)\big(mod\, P(x)\big),$$

т.е. представлен как система остатков от деления произведений $\alpha_i(x)\beta_i(x)$ на соответствующие основания $p_i(x)$, $\overline{1,S}$.

Бинарная последовательность полученного шифра подблока R'_0 умножается по модулю 2 с бинарной последовательностью левого подблока L'_0 и становится правой частью R'_1, а исходный подблок R'_0 становится левой частью L'_1 входного блока для следующего раунда вложенной сети Фейстеля.

В процессе расшифровывания шифротекста $H(x)$ по известному ключу $G(x)$ для каждого значения $\beta_i(x)$ вычисляется обратный (инверсный) многочлен $\beta_i^{-1}(x)$ из условия выполнения следующего сравнения

$$\beta_i(x)\beta_i^{-1}(x) \equiv 1\big(mod\ p_i(x)\big), i = 1,2,\ldots,S. \quad (5)$$

В результате получается многочлен, инверсный к многочлену $G(x)$. Тогда исходное сообщение восстанавливается по сравнению:

$$F(x) \equiv G^{-1}(x)H(x)\big(mod\, P(x)\big). \quad (6)$$

Применение вложенной, или рекурсивной, схемы сети Фейстеля позволяет существенно затруднить криптоанализ [6].

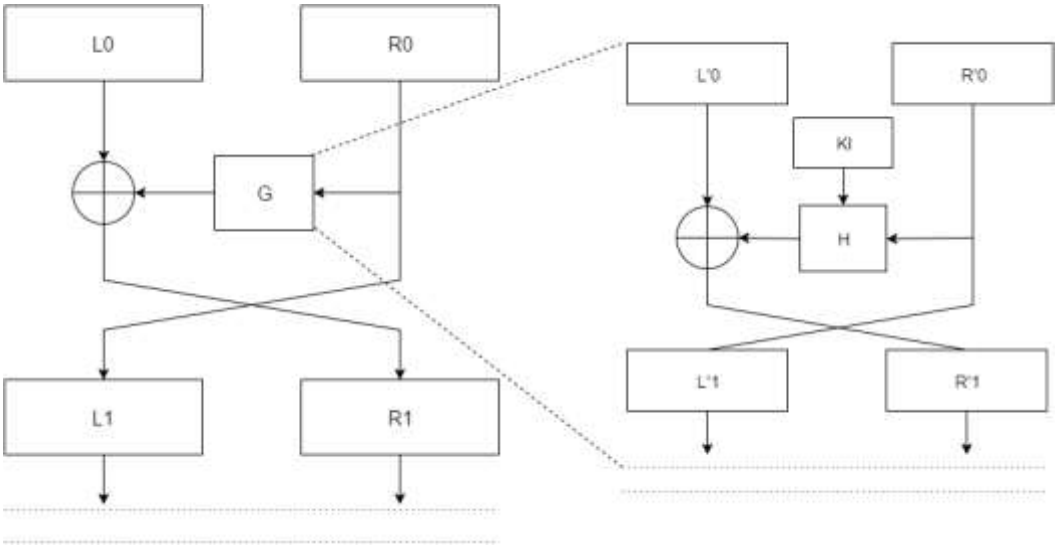

Рис. 1. Схема применения вложенной сети Фейстеля

В процессе моделирования алгоритма шифрования количество раундовых ключей на каждом из уровней и способы их генерации могут быть различными. В связи с этим, возможно построение различных моделей разрабатываемой системы шифрования с использованием нетрадиционного шифрования и вложенных сетей Фейстеля.

В разрабатываемой модели вложенная сеть включает в себя шестнадцать раундов, а сеть Фейстеля верхнего уровня состоит из четырёх раундов. В предлагаемом алгоритме шестнадцать раундовых ключей получаются путём сдвига битовой последовательности ключа K на переменное количество разрядов, которое определяется степенью *i*-го многочлена в системе оснований. Здесь также могут использоваться и другие секретные параметры, определяющиеся в полном ключе. В алгоритме шифрования, основанном на НПСС, полный секретный ключ зависит не только от длины ключевой последовательности, но и от выбранной системы полиномиальных оснований, а также от порядка расположения оснований в системе. Применение этих свойств алгоритма при генерации раундовых ключей приводит к неравномерному изменению внутренних свойств сети, что усложняет анализ свойств шифра.

Чем больше длина входного блока, тем больше вариантов выбора систем рабочих оснований. Поэтому криптостойкость предложенного алгоритма шифрования с использованием НПСС существенно возрастает с увеличением длины электронного сообщения. В данной модели используется входной блок длиною в 512 бит. В этом случае длина подблока вложенной сети Фейстеля, для которого формируется НПСС, равняется 128 битам. Это даёт большой выбор неприводимых многочленов для построения системы рабочих оснований [5,7].

В данной модели для улучшения статистических свойств получаемых криптограмм используется режим шифрования. Режимы шифрования используются для модификации процесса шифрования так, чтобы результат шифрования каждого блока был уникальным вне зависимости от шифруемых данных и не позволял сделать какие-либо выводы об их структуре. Это обусловлено, прежде всего, тем, что блочные шифры шифруют данные блоками фиксированного размера, и поэтому существует потенциальная возможность утечки информации о повторяющихся частях данных шифруемых на одном и том же ключе.

В данной модели применяется режим Chipher Block Chaining [8] – режим сцепления блоков шифра. Преобразование выполняется следующим образом: каждый блок открытого текста складывается по модулю 2 с результатом шифрования предыдущего блока. Таким образом, результаты шифрования предыдущих блоков влияют на шифрование следующих блоков.

При этом в начале шифрования используется вектор инициализации для того, чтобы любое сообщение было уникальным. В связи с этим вектор инициализации должен быть случайным числом. Его не обязательно хранить в секрете, можно передавать его вместе с сообщением.

Для проверки эффективности и надежности предлагаемой модели нетрадиционного шифрования разрабатывается алгоритм ее компьютерной реализации. .Тестирование алгоритма

проводится путем зашифрования и расшифрования файлов различных форматов. Использование файлов похожих форматов позволяет оценить эффективность алгоритма шифрования при работе с данными с явной повторяющейся структурой. Анализ статистических характеристик получаемых шифртекстов будет проведен путем использования набора статистическим тестов [9].

ЗАКЛЮЧЕНИЕ

Было проведено моделирование алгоритма шифрования на базе НПСС с применением рекурсивной схемы Фейстеля. Данный подход позволяет скрыть структурные особенности блока исходного текста, что при дополнительном использовании режима шифрования значительно улучшает статистические характеристики всего щифротекста.

Проводимые исследования направлены на разработку рекомендаций по практическому применению нетрадиционного алгоритма шифрования. Полученные результаты данного исследования будут использованы также в работе по построению и исследованию других моделей нетрадиционного алгоритма шифрования.

ЛИТЕРАТУРА

[1] M. Pohst and H. Zassenhaus, Eds., Algorithmic algebraic number theory. New York, NY, USA: Cambridge University Press, 1989, ch. 2.2.5.

[2] Бияшев Р.Г., Нысанбаева С.Е. Алгоритм формирования элек¬тронной цифровой подписи с возможностью обнаружения и исправления ошибки // Кибернетика и системный анализ. – 2012 г. – Т. 48, № 4. – С. 14-23.

[3] H. Feistel. Cryptography and Computer Privacy, H. Feistel // Scientific American. – 1973. V. 228, N. 5.P. 15-23.

[4] Bassham L., Burr W., Dworkin M., Foti J., Roback E., Report on the Development of the Advanced Encryption Standard (AES) , Computer Security Division, Information Technology Laboratory; NIST: Technology Administration; U.S. Department of Commerce, 116 p. (2000).

[5] R. G. Biyashev, S. E. Nyssanbayeva, Ye. Ye. Begimbayeva, M. M. Magzom, Building modified modular cryptographic systems, International Journal of Applied Mathematics and Informatics, Volume 9 2015, P103-109.

[6] Mitsuru Matsui and Toshio Tokita. MISTY, KASUMI and Camellia Cipher Algorithm Development. Mitsubishi Electric Advance. Vol. 100/December 2002 Mitsubishi Electric.

[7] N. A. Kapalova, S. E. Nyssanbayeva, R. A. Khakimov, “Irreducible polynomials over the field GF (2n),” Proceedings of Scientific and Technical Society "KAKHAK" , Almaty, Kazakhstan, № 1. P. 17-28, 2013.

[8] Recommendation for Block Cipher Modes of Operation. NIST Special Publication 800-38A. Technology Administration U.S. Department of Commerce. 2001 Edition.

[9] A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications /A. Rukhin, J. Soto at al. // NIST Special Publication 800.-22, 2001, 154 p.

[10] B. Schneier, J. Kelsey. Unbalanced Feistel Networks and Block-Cipher Design // Fast Software Encryption, Third International Workshop Proceedings (February 1996), Springer-Verlag, 1996, pp. 121-144.

С.Е. Нысанбаева, М.М. Мағзом

Позициялы емес шифрлеу алгоритмінің ендірілген Фейстель желісіне негізделген моделі

Түйіндеме. Позициялы емес полиномды санау жүйесі негізінде құралған шифрлеу алгоритмнің моделі ұсынылады. Фейстель желісін және шифрлеу режимдерін қолдана отырып ұсынылған моделді жетілдіру мүмкіндігі қарастырылды. Ұсынылған криптографикалық алгоритмнің моделі алынатын шифрленген мәтіндердің статистикалық сипаттамаларын жетілдіруге мүмкіндік береді.

Негізгі сөздер. Криптографикалық жүйе, шифрлеу алгоритмі, модулярлық арифметика, Фейстель желісі, шифрлеу режимдері.

S.E. Nyssanbayeva, M.M. Magzom

Model of nonpositional encryption algorithm based on nested Feistel network

Summary. The purpose of research - studying the possibilities of practical application of the encryption algorithm based on nonpositional polynomial notations using nested Feistel network. In this paper, a mathematical model of non-conventional encryption algorithm with recursive Feistel network and the encryption mode is described.

Keywords. Cryptographic system, encryption algorithm, modular arithmetic, Feistel scheme, encryption mode.