УДК 62-7

Нысанбаева С.Е., Магзом М.М.
Институт информационных и вычислительных технологий МОН РК.
Алматы, Казахстан

МОДЕЛИРОВАНИЕ НЕТРАДИЦИОННОГО АЛГОРИТМА ШИФРОВАНИЯ

Аннотация: С целью исследования возможности практического применения алгоритма шифрования, разработанного на базе непозиционных полиномиальных систем счисления, рассмотрена возможность модификации разработанной модели с использованием сети Фейстеля. Предлагаемая модель позволит существенно повысить статистические характеристики криптографического алгоритма.

Учитывая значительное развитие технической базы, и увеличение масштабов современных информационных систем, возрастает необходимость в стойких и эффективных средствах, обеспечивающих информационную безопасность при хранении и передачи данных в электронной среде. Нетрадиционные методы и алгоритмы криптографии, построенные на базе непозиционных полиномиальных систем счисления, позволяют повысить надежность алгоритма шифрования.

Ключевые слова: непозиционная полиномиальная система счисления, шифрования, информационная безопасность, криптостойкость, модулярная арифметика.

Введение

Для блочных шифров одним из критериев криптостойкости является длина ключа. В разработанной системе шифрования в качестве показателя криптостойкости предложено использовать криптостойкость самого алгоритма, которая характеризуется полным секретным ключом. В его состав кроме стандартного секретного ключа входят также секретные параметры криптоалгоритма, разработанного на базе непозиционных полиномиальных систем счисления(НПСС). Синонимы НПСС – классическая система счисления остаточных классов (СОК), полиномиальная СОК и модулярная арифметика.

Классическая СОК базируется на китайской теореме об остатках, которая гласит, что любое число может быть представлено своими остатками (вычетами) от деления на систему оснований, которую образуют попарно простые числа [1,2]. В отличие от классических СОК предлагаемые криптографические процедуры рассматриваются в полиномиальных системах счисления в остаточных классах, в которых основаниями служат не простые числа, а неприводимые многочлены над полем $GF(2)$ [3,4]. Криптографические алгоритмы и методы, разработанные на базе НПСС, называют нетрадиционными, модулярными или непозиционными.

Нетрадиционные методы и алгоритмы криптографии, построенные на базе непозиционных полиномиальных систем счисления, позволяют повысить надежность алгоритма шифрования и уменьшить длину ключа. Криптостойкость в этом случае определяется полным ключом, зависящим не только от длины ключа (ключевой последовательности), но и от выбранной системы полиномиальных оснований, а также от количества перестановок оснований в системе. Чем больше длина полного ключа шифрования в НПСС, тем больше вариантов выбора систем рабочих оснований. Поэтому криптостойкость предложенного алгоритма шифрования с использованием НПСС существенно возрастает с увеличением длины электронного сообщения [3].

Этапы алгоритма шифрования на базе НПСС

При шифровании электронного сообщения длиной N бит сначала из множества всех неприводимых многочленов степени не выше значения N выбираются рабочие основания

$$p_1(x), p_2(x), \ldots, p_S(x) \quad (1)$$

Согласно китайской теореме об остатках, все выбираемые основания должны отличаться друг от друга, даже если они являются неприводимыми полиномами одной степени. Рабочий диапазон данной системы определяется многочленом $P(x)=p_1(x),p_2(x),\ldots,p_S(x)$ степени m:

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

где S – число выбранных рабочих оснований. В этой системе любой многочлен степени меньше m имеет единственное представление в виде последовательности остатков (вычетов) от его деления на основания (1). Следовательно, сообщение длиной N бит может быть представлено в видепоследовательности 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 $F(x)\equiv\alpha_i(x)\left(mod\,p_i(x)\right),i=\overline{1,S}$.

Таким же образом, ключ длины N бит интерпретируется 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 $G(x)\equiv\beta_i(x)\left(mod\,p_i(x)\right),i=\overline{1,S}$.

Тогда в качестве криптограммы $\omega_1(x),\omega_2(x),...,\omega_S(x)$ может рассматриваться некоторая функция $H(F(x),G(x))$:

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

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

В соответствии с операциями непозиционной системы счисления операции в функциях $F(x),G(x)$, $H(x)$ выполняются параллельно по модулям полиномов $p_1(x),p_2(x),...,p_S(x)$, выбранных в качестве оснований НПСС.

При программной реализации этого нетрадиционного алгоритма шифрования, используется метод шифрования [4]. Шифртекст получается в результате умножения многочленов (2) и (3) в соответствии со свойствами сравнений по двойному модулю:

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

то есть представлена в виде остатков от деления произведений $\alpha_i(x)\beta_i(x)$ на соответствующие основания $p_i(x)$:

$$H(x)=(\omega_1(x),\omega_2(x),\ldots,\omega_S(x)). \tag{5}$$

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

$$\beta_i(x)\beta_i^{-1}(x) \equiv 1\left(mod\ p_i(x)\right), i = 1,2,\ldots,S. \tag{6}$$

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

$$F(x) \equiv G^{-1}(x)H(x)\left(mod\ P(x)\right). \tag{7}$$

Модификация криптографического алгоритма с применением сети Фейстеля

При разработке симметричных блочных шифров широкую популярность приобрела криптосистема, названная схемой Фейстеля. Впервые она была использована Хорстом Фейстелем в 1973 г. при разработке шифра Lucifer [5], и затем применялась во многих разработках блочных шифров, в том числе и в финалистах AES [6]. Схема Фейстеля является методом смешивания подблоков входного текста в шифре посредством повторяющегося применения зависящих от ключей нелинейных функций, называемых *F*-функциями и выполнения перестановок подблоков. Раунд блокового шифра является преобразованием, которое соединяет подблоки входного блока посредством *F*-функций и перестановок подблоков. В стандартной сети Фейстеля открытый текст разбивается на два подблока одинаковой длительности. 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 раунде.

Разработанный алгоритм шифрования на базе НПСС является основой для решения задач его практического использования. Для получения модели нетрадиционного алгоритма шифрования предполагается использование модифицированной сети Фейстеля. Целью этих работ является улучшение статистических характеристик непозиционных криптограмм. В связи с этим планируется рассмотреть несколько моделей схемы Фейстеля.

В отличие от традиционной сети Фейстеля, где входными данными является открытый текст сообщения, в разрабатываемой модели на вход подаётся битовая последовательность шифотекста, получаемая в (4).

Необходимым условием стойкости шифра является достижение полной диффузии. Диффузионный процесс шифра характеризуется результатом распространения влияние одного входного бита на много выходных. Шифр называется полным, если каждый выходной бит зависит от всех входных [7]. В рассматриваемых моделях все F -функции подразумеваются полными.

В большинстве шифров с архитектурой сети Файстеля используемая функция F в течение каждого раунда зависит только от одного из подключей, вырабатываемых из основного ключа шифра. Сеть с такого рода зависимостью функции гаммирования называют гетерогенной и гомогенной в противном случае. Применение гетерогенных сетей может значительно улучшить характеристики шифра, поскольку неравномерное изменение внутренних свойств сети в пределах допустимых границ делает изучение свойств шифра достаточно затруднительным занятием.

Для примера рассмотрим модель, в которой блок входных данный F длиной 128 бит разделяется на два подблока равной длины R_i и L_i.

При использовании гомогенной сети на каждом этапе шифрования используется отдельная ключевая последовательность *K(i)*:

$$\begin{aligned} L_i &:= R_{i-1}, \\ R_i &:= L_{i-1} \oplus F(R_{i-1}, K_i) \end{aligned} \tag{8}$$

При использовании гетерогенной сети на каждом этапе функция шифрования F подблока зависит не только от раундового ключа *K(i)*, но и от выбранной системы оснований (1):

$$L_i := R_{i-1},$$
$$R_i := L_{i-1} \oplus F(R_{i-1}, K_i, P(x)) \quad (9)$$

При компьютерном моделировании разработанных модифицированных алгоритмов будет проведен анализ статистических характеристик получаемых шифртекстов. Проверка на удовлетворение модели строгому лавинному критерию будет проведена путем проверки полученной битовой последовательности по статистическому тесту равномерности (частот) – Frequency (Monobit) Test Американского института стандартов NIST для криптографических функций [8]. «NISTStatisticalTestSuite» – статистический пакет, состоящий из 16 тестов, разработанных для проверки случайности двоичных последовательностей, производимых как техническими средствами, так и программным обеспечением.

Заключение. Предлагаемая система шифрования основывается на теории непозиционных полиномиальных систем счисления. Криптостойкость разработанного алгоритма характеризуется полным секретным ключом шифрования, который определяется не только длиной ключевой последовательности, но и выбранной системой полиномиальных оснований.

Разрабатываемая модель модификации криптографического алгоритма на основе сети Фейстеля позволит существенно повысить статистические характеристики получаемых шифротекстов.

Список использованной литературы:

1 Акушский И.Я., Юдицкий Д.И. Машинная арифметика в остаточных классах. – М.: Советское радио, 1968.- 439 с.

2 Бияшев Р.Г. Разработка и исследование методов сквозного повышения достоверности в системах обмена данными распределенных АСУ: дисс. докт. тех. наук: 05.13.06: защищена 09.10. 1985: утв. 28.03.1986. - М., 1985. - 328 с.

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

4 Нысанбаев Р.К. Криптографический метод на основе полиномиальных оснований // Вестник Мин-ва науки и высшего образования и Нац. акад. наук Республики Казахстан – Алматы: Гылым. – 1999. – № 5. – С. 63-65.

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

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

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

8 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.