УДК 004.056.55

В.Б.УФИМЦЕВА
Харьковская государственная академия городского хозяйства

МЕТОД И АЛГОРИТМЫ ХЕШИРОВАНИЯ ИНФОРМАЦИИ НА ОСНОВЕ ОБОБЩЕННЫХ МАТРИЦ ФИБОНАЧЧИ

Рассматриваются быстродействующий метод и алгоритмы преобразования информации, использующиеся при хешировании в системах обеспечения целостности и аутентификации, на основе обобщенных матриц Фибоначчи.

Современные системы управления городским хозяйством характеризуются все более широким применением информационных технологий. Особый нематериальный характер электронной информации делает легким ее копирование, изменение и подделку. Это приводит к необходимости создания методов обеспечения целостности и аутентификации информации в процессе ее обмена.

Разработка эффективных методов обеспечения целостности и аутентификации информации современных систем управления городским хозяйством требует использования комбинированных методов ее преобразования. Так, электронная цифровая подпись документа формируется с помощью асимметричного преобразования. Однако в связи с низкой скоростью такого документа производится подпись не самого документа, а его сжатого эквивалента. Одной из наиболее используемых функций сжатия является хеширование информации на основе симметричного блочного преобразования.

Существует много эффективных методов хеширования информации, разработанных такими известными специалистами, как Р.Л.Ривест, Р.Меркли и др. [1]. Однако объемы информации, циркулирующие в автоматизированных системах управления, в том числе в системах управления городским хозяйством, непрерывно возрастают, что приводит к необходимости минимизации вычислительной сложности методов хеширования, являющихся основой многих систем обеспечения целостности и аутентификации информации.

Наиболее существенный вклад в вычислительную сложность функции хеширования вносит метод симметричного преобразования информации. Одним из способов увеличения быстродействия этого метода является сокращение количества итераций симметричного преобразования без потери качества преобразования путем усиления диффузионных процессов. Такого результата можно добиться эффективным сочетанием схемы смешивания нелинейных F-функций и схемы обмена подблоков (СО).

Минимизация вычислительной сложности хеш-функции путем разработки нового быстродействующего метода и алгоритмов симметричного преобразования информации при обеспечении необходимых показателей качества является нашей главной задачей.

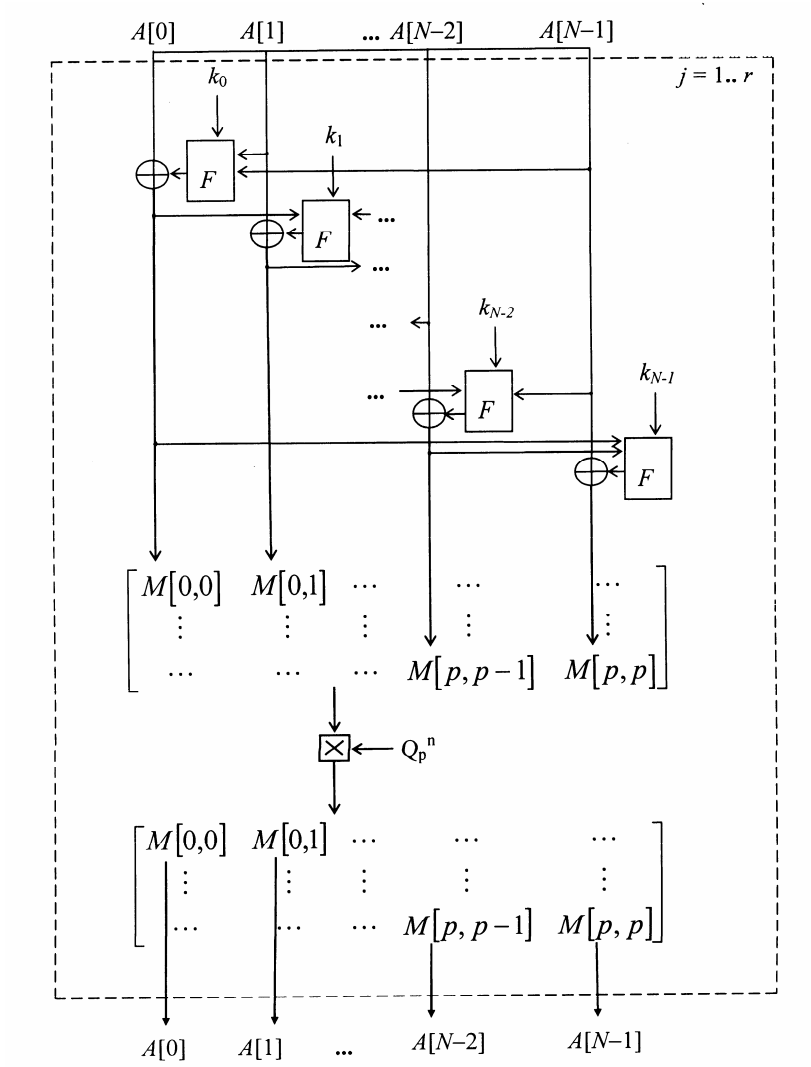
Разработанный метод MDEM является модифицированной сетью Фейстеля. Основная особенность метода – использование в СО умножения на обобщенную матрицу Фибоначчи. MDEM является параметрическим алгоритмом и более точно обозначается как MDEM-$w/r/b/p$, где w – размер слова (8, 16 или 32 бита); r – число итераций; b – длина ключа K в байтах; p – значение порядка матрицы Фибоначчи. Параметризация метода позволяет пользователю выбрать алгоритм, соотношение стойкости требуемого объема памяти, скорости, размера блока и, соответственно, хеш-значения (от 32 бит при $w=8$, 64 бит при $w=16$, 128 бит при $w=32$) которого являются оптимальными для конкретного применения и делают алгоритм приспособленным к эволюционным изменениям технических средств в будущем.

Метод MDEM (см. рисунок) использует циклическую схему смешивания F -функций и в СО умножение $(p+1)\times(p+1)$-матрицы, состоящей из подблоков, на Q_p^n-матрицу Фибоначчи, что сводится к операциям сложения и сдвига подблоков [2].

Порядок матрицы Фибоначчи p определяет количество входных подблоков $N=(p+1)\times(p+1)$ и, соответственно СО, а степень n зависит от секретного ключа шифрования и определяет СО, что обеспечивает неопределенность конкретного алгоритма шифрования при выполнении условия открытости метода.

СО метода MDEM имеет $(p+1)$ кластеров, так как при умножении на матрицу Фибоначчи операции производятся со столбцами. Каждый кластер содержит $(p+1)$ подблоков. Обычно период СО кластера равен количеству подблоков в этом кластере, однако в СО на основе матриц Фибоначчи количество итераций, в которых подблоки меняются местами, может быть больше 1 и зависит от степени матрицы, следовательно, период в каждом кластере и, соответственно, СО всего шифра равен

$$P=\frac{p+1}{|n|}. \qquad (1)$$



Функциональная схема метода MDEM

Исследование диффузионных процессов, происходящих в методе MDEM, показало, что при порядке матрицы Фибоначчи $p = 1$ (четыре подблока) и степени матрицы $n = 2; -1; -2$ достигает полной диффузии в 1,5 раза быстрее, чем финалист AES шифр RC6 [3] и в 2 раза бы-

стрее СФ с аналогичной схемой смешивания F -функций. При порядке матрицы Фибоначчи $p > 1$ полная диффузия достигается за два раунда, однако даже за один раунд в каждом кластере значительно увеличивается относительная диффузия, так как охватывает не только текущий кластер, но и все предшествующие.

На основе метода MDEM был разработан алгоритм преобразования информации, построенный с использованием нелинейной функции алгоритма RC6.

MDEM состоит из трех компонентов: алгоритма расширения ключа, алгоритма прямого преобразования и алгоритма обратного преобразования. Эти алгоритмы используют шесть базовых операций:

$a + b$ – целочисленное сложение;

$a - b$ – целочисленное вычитание;

$a \oplus b$ – битовая операция “исключающее ИЛИ” над w-битовыми словами;

$a \times b$ – целочисленное умножение;

$a <<< b$ – циклический сдвиг w-битового слова a влево на величину, равную значению младших $\lg w$ (логарифм w по основанию два) бит слова b;

$a >>> b$ – циклический сдвиг w-битового слова a влево на величину, равную значению младших $\lg w$ бит слова b.

Все операции производятся в кольце целых чисел по модулю 2^w, что предотвращает возникновение избыточности информации.

Алгоритм расширения ключа практически аналогичен алгоритму расширения ключа алгоритма RC6™, который обеспечивает влияние каждого бита секретного ключа пользователя на каждый бит подключей шифрования. Различие состоит лишь в количестве подключей, необходимых для преобразования.

Алгоритм прямого/обратного преобразования MDEM работает с N w-битовыми подблоками $A[i]$ $(i = 0,...,N-1)$, получаемыми из входного текста и таблицей расширения ключа пользователя $S[0,...,N\cdot(r+1)-1]$. Алгоритм преобразования MDEM включает начальное отбеливание, итеративные операции над подблоками данных “исключающее ИЛИ” со значением квадратичной функции $2x^2+x$ от следующего подблока и циклического сдвига по значению квадратичной функции от предыдущего подблока данных, суммирование с подключом по модулю 2^w и умножение на матрицу Фибоначчи $Q_p{}^n$.

Алгоритм MDEM был реализован на языке С на компьютере с процессором AMD Duron 1100 МГц под управлением ОС Linux (Red

Hat 8.0). Статистические исследования строгого лавинного критерия по тестам NIST [4] подтвердили повышение быстродействия метода по сравнению с аналогом – шифром RC6 благодаря использованию в сети Фейстеля схемы обмена на основе умножения на матрицу Фибоначчи. MDEM при порядке матрицы Фибоначчи $p=1$ и всех степенях матрицы удовлетворяет СЛК после 2 раундов, что аналогично четырем раундам RC6, а последний – только после пяти раундов. Результаты статистического анализа критериев сбалансированности, корреляции между входом и выходом алгоритма и корреляционного иммунитета подтвердили сохранение статистических характеристик алгоритма. Выходная последовательность MDEM имеет свойства случайной после 1 раунда (2 раунда RC6), что на 2 раунда быстрее, чем у симметричного алгоритма RC6.

Таким образом, использование параметрического метода преобразования информации MDEM на основе модифицированной схемы Фейстеля с цепочечной схемой смешивания функций и СО с умножением на обобщенную матрицу Фибоначчи, что способствует усилению процесса диффузии, позволяет создавать алгоритмы с усиленным быстродействием за счет уменьшения количества итераций без потери качества преобразования. Применение этих алгоритмов в функциях сжатия позволяет получать различные размеры хеш-значения и сократить время хеширования.

1.Schneier B. Applied Cryptography. New York: John Wiley & Sons, 1996.

2.Самойленко Н.И., Уфимцева В.Б. Свойства *p*-чисел и Q_p^n-матриц Стахова в кольце целых чисел $Z/(q)$ // Радиоэлектроника и информатика. – Харьков: ХНУРЭ. – 2003. – № 1. – С.111 – 115.

3.The RC6 Block Cipher / R.L.Rivest, M.J.B.Robshaw, R.Sidney, Y.L.Yin, AES algorithm submission, June 1998.

4.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.

Получено 13.10.2003