УДК 681.325.3:621.391.7

Л.К. Бабенко, О.Б. Макаревич,
Р.В. Набережный, А.Н. Рыбалко

г. Таганрог, ТРТУ, http://www.tsure.ru

РЕАЛИЗАЦИЯ СКОРОСТНЫХ БЛОЧНЫХ ШИФРОВ НА МИКРОПРОЦЕССОРЕ NM 6403

Широкое применение компьютерных технологий в автоматизированных системах обработки информации и управления привело к обострению проблемы защиты информации, циркулирующей в компьютерных системах, от несанкционированного доступа. Защита информации в компьютерных системах обладает рядом специфических особенностей, связанных с тем, что информация не является жёстко связанной с носителем, может легко и быстро копироваться и передаваться по каналам связи. Известно очень большое число угроз информации, которые могут быть реализованы как со стороны внешних, так и со стороны внутренних нарушителей.

Радикальное решение проблем защиты электронной информации может быть получено только на базе использования криптографических методов, которые позволяют решать важнейшие проблемы защищённой автоматизированной обработки и передачи данных. Криптографические преобразования данных являются наиболее эффективным средством обеспечения конфиденциальности данных, их целостности и подлинности. Только их использование в совокупности с необходимыми техническими и организационными мероприятиями могут обеспечить защиту от широкого спектра потенциальных угроз.

Одним из сдерживающих факторов массового применения методов шифрования является потребление значительных временных ресурсов процессора при программной реализации большинства хорошо известных шифров (DES, ГОСТ 28147-89, FEAL, REDOC, IDEA). Решением данной проблемы может быть совместное использование современных скоростных методов криптографического преобразования и высокоскоростных процессорных устройств.

Для исследований в качестве скоростного блочного шифра был выбран 512-байтовый блочный шифр на основе механизма усиления рассеивания, разработанный Н.А. Молдовяном и А.А Молдовяном [1,2].

В данном шифре используется псевдослучайная ключевая последовательность, представляющая собой множество 8-битовых слов $\{q_j\}$, где $j=0,1,2,\ldots,2050$. При

выполнении элементарных шагов шифрования используются 32-битовые подключи $Q(x)=q_{x+3}q|_{x+2}|q_{x+1}|q_x$, где x=0,1,2,…,2047.

Алгоритм шифрования состоит в следующем:

ВХОД: 512-байтовый блок данных, представленный в виде пронумерованной последовательности 32-битовых слов $\{T_h\}$, h=0,1,2,…,127.

1.Установить начальные значения переменных G, Y, U, n и m в зависимости от ключа.

2.Вычислить текущие значения переменных:

$m:=\{[m+(G \text{ div } 2^{21})] \bmod 2^{11}\} \oplus (U \bmod 2^{11})$, $Y:=[Y+Q(m)] \bmod 2^{32}$,

$n:=\{[n+(G \text{ div } 2^{11})] \bmod 2^{11}\} \oplus (Y \bmod 2^{11})$, $U:=[(U+G) \bmod 2^{32}] \oplus Q(n)$,

$l:=[(n-G) \bmod 2^{11}] \oplus (U \bmod 2^{11})$, $V:=V \oplus Q(l)$,

где m, n, l определяют индексы подключей, используемых для определения переменных Y, U, V, которые используются для преобразования текста.

3.Если выполняется дешифрование то перейти к шагу 5.

4.Выполнить текущий шаг шифрования текущего раунда:

$G:=[(L_h-Y) \bmod 2^{32}] \oplus V$, $C_h=(G+U) \bmod 2^{32}$

и перейти к шагу 6.

5.Выполнить текущий шаг дешифрования текущего раунда:

$G:=(L_h-U) \bmod 2^{32}$, $C_h=[(G \oplus V) \bmod 2^{32}$.

6.Если не последний 32-битный подблок, то перейти к шагу 2.

7.Выполнять последовательность действий со 2-го по 6-ой шаг в зависимости от количества раундов.

ВЫХОД: 512-байтовый блок $\{C_h\}$, h=0,1,2,…,127.

В этом алгоритме переменные Y, U и V принимают значения в зависимости от “псевдослучайно” выбираемых комбинаций из i подключей, где i – номер текущего элементарного шага преобразования (i=1,2,…,128) в данном раунде шифрования. Число различных возможных значений переменных зависит от i. На шагах с номерами i=4,5,…,128 возможны примерно 2^{96} различных наборов {Y,U,V}. Реализация конкретного набора зависит от входного блока и ключа шифрования. Рассматриваемый алгоритм составлен в соответствии со следующим

критерием: процедуры преобразования должны быть составлены так, чтобы изменение любого бита входного сообщения приводило к изменению выборки подключей. Этот критерий гарантирует, что для всех различных входных сообщений будут генерироваться уникальные последовательности наборов $\{Y_i,U_i,V_i\}$, где индексом i отмечены значения переменных на шагах преобразования с соответствующими номерами.

Рассмотрена реализация данного шифра на симуляторе процессора NM6403[3].

Нейропроцессор NM6403 представляет собой высокопроизводительный микропроцессор с LIW (long instruction word, длинное командное слово) архитектурой, в состав функциональных устройств которого входят: 2 устройства адресных вычислений, устройство обработки скаляров и устройство выполнения матричных операций с перестраиваемой структурой для эффективного выполнения операций над векторами. Адресные устройства совместно с устройством для обработки скалярных операндов далее именуются как скалярный процессор.

Устройство для выполнения матричных операций именуется далее как векторный процессор. Адресные устройства используются совместно скалярным и векторным процессорами. Векторный и скалярный узлы могут работать параллельно, что увеличивает производительность процессора.

Основные характеристики процессора таковы:

1. объем адресного пространства процессора состовляет 16 Гбайт;
2. за одно обращение к внешней памяти по локальной или глобальной шине пересылается 64-разрядное слово;
3. одновременно может выполняться либо два обращения к памяти на считывание, либо одно обращение на считывание, а другое - на запись. Таким образом, при использовании одно-тактовых памятей пропускная способность интерфейса с памятью такова:

   максимальная - 640 Мбайт/сек;

   минимальная - 320 Мбайт/сек;

4. формат инструкций нейропроцессора 32-х и 64-х разрядный.
5. все скалярные команды исполняются за 1 такт; векторные - в течение нескольких тактов;
6. производительность нейропроцессора при работе с 8 разрядными данными оценивается в 720 млн. операций умножения-сложения в секунду.

Векторный процессор является основным вычислительным узлом нейропроцессора и ориентирован на обработку данных произвольной разрядности от 2 до 64 разрядов, упакованных в 64-разрядные слова.

Векторный процессор включает 3 блока внутренней памяти, каждый из которых содержит 32 64-х разрядных слова, набор специальных регистров управления, а также функциональное устройство с настраиваемой на разрядность операндов структурой для выполнения матричных операций.

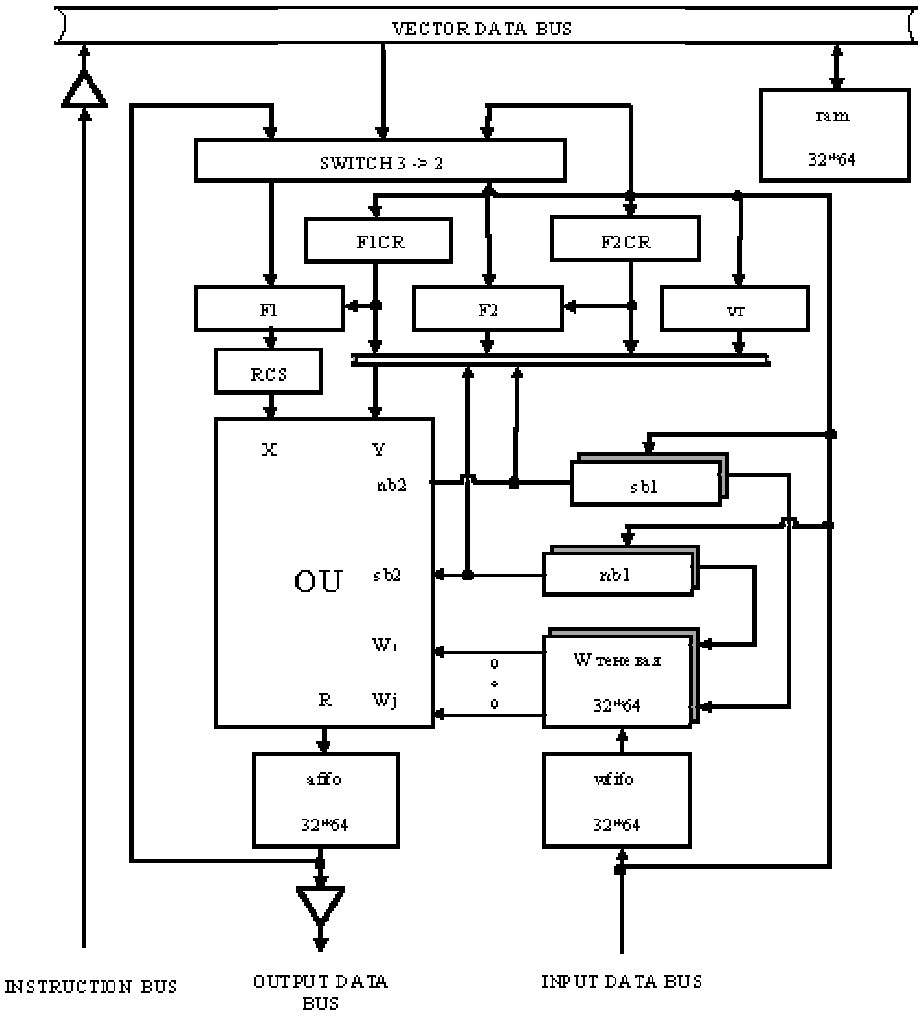

Рис 1.

В данном процессоре:

OU - операционное устройство;

ram – векторный регистр размерностью 32 64-разрядных слова;

afifo – регистр результатов векторных операций размерностью 32 64-разрядных слова;

wfifo, w-теневая - матрицы весов, используемые для взвешенного суммирования;

sb1, nb1 – 64-разрядные регистры, задающие разбиение входных 64-разрядных слов.

F1CR, F2CR, F1, F2, vr, RCS – узлы, использующиеся для эффективного выполнения нейровычислений.

Организация процесса шифрования схематично показано на рис. 2.

В алгоритме шифрования идет обработка 32-разрядных слов, поэтому в одно 64-разрядное слово, обрабатываемое векторным процессором, помещялось два текущих 32-разрядных операнда. Для того, чтобы 64-разрядное слово интерпритировалось как два 32-разрядных, в регистр nb1 заносилась константа, содержащая 1 в 32-ом разряде.

Шифр текст

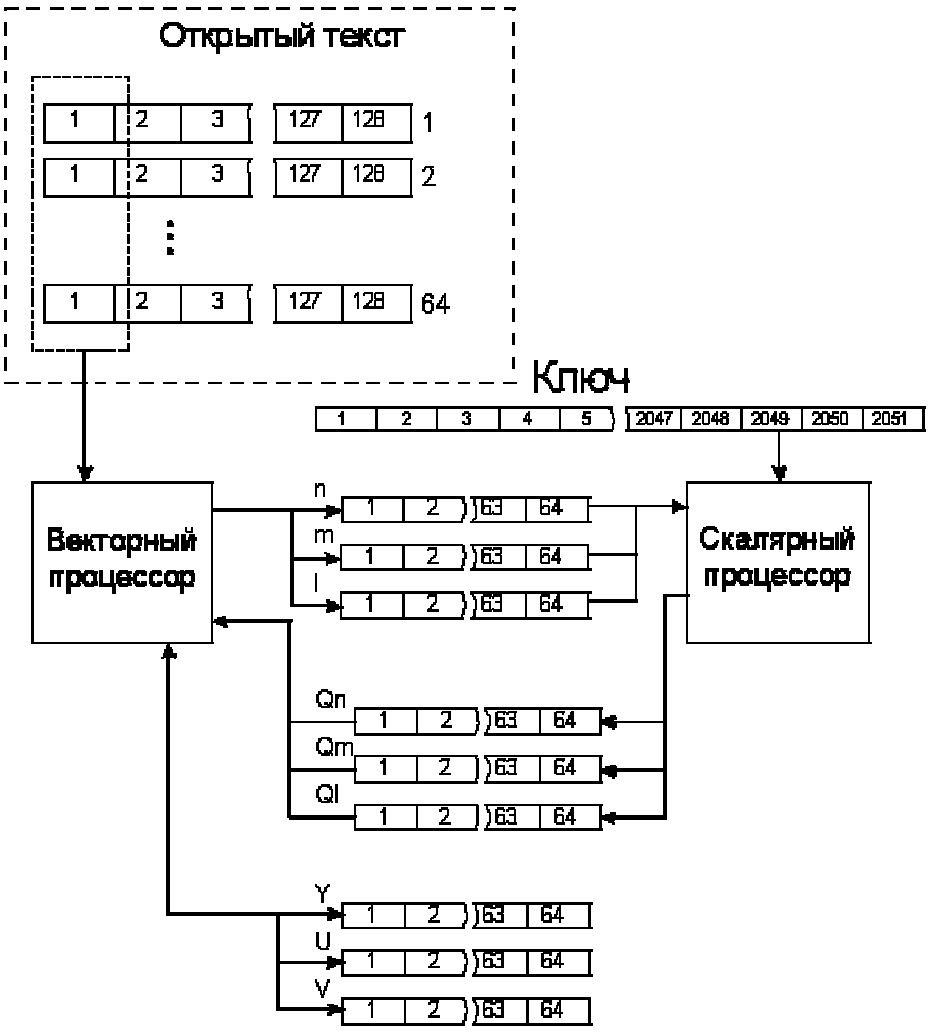

Рис. 2.

Для эффективного использования вычислительных ресурсов нейропроцессора на шифрование запускалось параллельно 64 512-байтовых блока данных. При этом

основные процедуры шифрования выполнялись на векторном процессоре, а вспомогательные операции на скалярном процессоре.

Описание реализации.

Из каждого 512-байтового блока берем очередной 32-разрядный подблок. Формируем 64-элементные массивы индексов подключей (n,m,l) с использованием векторного процессора. Далее определяем массивы подключей Qn, Qm, Ql на скалярном процессоре, участвующих в формировании массивов Y, U, V, которые непосредственно используются для шифрования или дешифрования 64 выбранных 32-разрядных подблоков данных. Результат шифрования формируется на выходе операционного устройства (OU) векторного процессора и заносится в память на место обработанного открытого текста.

Предварительная оценка скорости шифрования на процессоре NM6403 составила 11 Мбит/с.

Учитывая тот факт, что процессор NM6403 достаточно просто объединяется в многопроцессорные системы, на его основе может быть построено устройство линейного шифрования на магистральной и абонентских каналах со скоростями до сотен Мбит/с.

Литература

1. Молдовян Н.А. Скоростные блочные шифры. – СПб, Издательство СПбГУ, 1998.-230с.
2. Молдовян А.А., Молдовян Н.А.,Советов Б.Я. Скоростные программные шифры и средства защиты информации в компьютерных системах. СПб, ВАС, 1997.-136с.
3. Микросхема интегральная нейропроцессор NM6403. Базовое программное обеспечение. Описание языка ассемблера. ЮФКВ.30002-01 35 01 (ЮФКВ.30002-01 35 01 001ФЛ). Листов 1.