УДК 621.3.037.3 *МРНТИ 28.21.19*

МЕТОДЫ УСКОРЕНИЯ МОДУЛЬНОЙ АРИФМЕТИКИ МНОГОРАЗРЯДНЫХ ЧИСЕЛ

К. А. Абдикаликов, д.т.н.

Акгюбинский государственный университет
им. К. Жубанова

Шифрлау/шифрды ашу амалыньщ жылдамдыгын арттыратын, шифрлаудыц непзп алгоритмдержде пайдаланылатын математикальщ есептеулердщ тш'мд! aflicrepi усынылган.
Тутнд) сездер: кепразрядты сандар, модульды арифметика.

The efficient methods of mathematical computations used in main algorithms of coding increasing the speed of coding/decoding are proposed.
Key words: many-digit numbers, modular arithmetic.

Одной из основных проблем, возникающих при использовании асимметричных алгоритмов, является низкая скорость проведения операций зашифрования-расшифрования. Этот факт особенно характерен для алгоритмов на устройствах с небольшими вычислительными возможностями. Один из выходов - уменьшение размерности параметров системы, который приводит к уменьшению стойкости алгоритма.

Другим решением этой проблемы является применение эффективных процедур проведения основных видов математических вычислений, используемых в алгоритмах шифрования. Суть большинства методов ускорения вычислений заключается в оптимизации операций модульного умножения и возведения в степень.

Один из методов оптимизации операции умножения двух целых чисел заключается в том, что множитель и множимое разбиваются на несколько чисел меньшей размерности. В результате одна операция умножения двух больших чисел заменяется несколькими операциями умножения чисел меньшей, по сравнению с исходными числами, размерности. Подобная идея использована в алгоритме Карацубы - Офмана [1] и алгоритме Шёнхаге - Штрассена [2], основанном на быстром преобразовании Фурье [3].

Алгоритм Шёнхаге - Штрассена [2] требует O(MogMoglogA) битовых операций, что намного меньше, нежели в алгоритме Карацубы - Офмана [1]. Этот алгоритм специально был разработан для перемножения чисел большой размерности.

Данный алгоритм быстрого умножения целых чисел работает над произвольным полем, в котором существует *кг*[1] и *к*-й корень из единицы. Быстрое преобразование Фурье первоначально было разработано для полей комплексных чисел. Однако существуют определённые вычислительные трудности при использовании комплексных чисел. В связи с вышеизложенным аппаратная реализация этого алгоритма является весьма трудной задачей.

Рассмотрим несколько методов ускорения сложения двух целых чисел.

Алгоритм параллельного суммирования с параллельным переносом основывается на предварительном вычислении битов переноса, с последующим суммированием:

$$S_i = A_i \oplus B_i \oplus C_i.$$

Для вычисления битов переноса введем вспомогательные функции G_j и P_i, назовем их функциями генерации и распространения сигнала переноса:

$$G_i = A_i B_i, \; P_i = A_i + B_i.$$

С учетом этого выражения для сигнала переноса можно записать следующим образом

$$C_i = G_{i-1} + P_{i-1} C_{i-1}.$$

Записав это выражение в виде системы уравнений для всех *к* битов и последовательно подставляя выражение для С, в выражение для C_2, затем выражение для C_2 в выражение для C_3 и т. д., можно получить соотношения, описывающие процесс параллельного формирования сигналов переноса в параллельном сумматоре:

Cг w 2 + pfAco>

c^r - - * W , -

Время вычисления результата при реализации алгоритма параллельного суммирования с параллельным переносом не зависит от разрядности суммируемых чисел и является величиной постоянной. Однако увеличение разрядности суммируемых чисел приводит

к большому увеличению количества оборудования при аппаратной реализации алгоритма. Кроме того, реальные конъюнкторы и дизъюнкторы могут иметь не более 16 входов и могут нагружаться не более чем на 20 последующих логических элементов. Эти обстоятельства вынуждают переходить к реализации сумматора с двухступенчатым переносом в ущерб быстродействию вычисления суммы. Следует отметить, что при больших значениях к > 128 даже двухступенчатая организация переносов может потребовать слишком большого расхода оборудования. В этом случае прибегают к организации трехступенчатого переноса.

Алгоритм суммирования целых чисел с задержкой переносов является двухуровневым алгоритмом суммирования целых чисел с запоминанием переносов. Основная задача этого алгоритма - уменьшить объём вычислений при умножении двух целых чисел. Алгоритм суммирования целых чисел с задержкой переносов выдаёт в качестве результата пару целых чисел (Д 7), используя следующие выражения:

$$S_i = A_i \oplus B_i \oplus C_i; \qquad C'_{i+1} = A_i B_i + A_i C_i + B_i C_i;$$

$$T_i = S_i \oplus C_i; \quad D_{i+1} = S_i C_i,$$

где $D_0 = 0$.

Важной особенностью алгоритма суммирования целых чисел с задержкой переносов является следующее свойство:

$$D_{i+1} T = 0 \quad \text{для} \quad i = 0,1,2,\ldots,4\text{-}1.$$

Эта особенность важна при реализации эффективных алгоритмов модульного умножения.

С точки зрения аппаратной реализации алгоритмы суммирования целых чисел с запоминанием переносов и суммирования целых чисел с задержкой переносов используют простые операции булевой алгебры и не требуют большого расхода оборудования для своей реализации.

При умножении двух 4-разрядных чисел произведение имеет разрядность 24, Значит, что для реализации операции умножения двух целых k-разрядных чисел, а именно для суммирования частичных произведений при аппаратной реализации, необходимо использовать сумматор двух 24-разрядных чисел. С целью уменьшения требуемого оборудования при аппаратной реализации вышеупомянутой операции предлагается алгоритм суммирования частичных произведений с выталкиванием младшего бита. Идея данного алгорит-

ма основана на том, что при суммировании частичных произведений младший бит первого слагаемого не участвует в вычислении функций генерации и распространения сигнала переноса и, таким образом, не влияет на конечный результат операции суммирования. Следовательно, вполне допустимо при аппаратной реализации операции умножения двух k-разрядных чисел использование сумматора 4-разрядных чисел.

Алгоритм работает следующим образом. После получения двух частичных произведений первое частичное произведение сдвигается вправо на один разряд с выталкиванием младшего разряда в результирующий 24-разрядный регистр, после чего производится операция арифметического сложения двух 4-разрядных чисел. Алгоритм выполняется до тех пор, пока не просуммируются все частичные произведения. Результат постепенно накапливается в результирующем 24-разрядном регистре.

Предложенный алгоритм может быть применен в любом из вышеописанных алгоритмов умножения двух целых чисел, при аппаратной реализации которых он может существенно уменьшить требования к количеству затрачиваемого оборудования.

Литература

1. *Карацуба А. А., Офман Ю. П.* Умножение многоразрядных чисел на автоматах//ДАН СССР. - 1962. - Т. 145. - С. 293-294.

2. *Шенхаге А., Штрассен В.* Быстрое умножение больших чисел // Кибернет. сб. - 1973. - Вып. 10. - С. 87-98.

3. *Абдикаликов К. А., Задирака В. К.* Элементы современной криптологии и методы защиты банковской информации. - Алматы: Гылым, 1999. -336 с.