Базисы модулярной системы счисления для табличной реализации мультипликативной схемы Монтгомери

Мазуренко П.А., Каленик А.Н., Коляда А.А., Шабинская Е.В.
Кафедра интеллектуальных систем
Белорусский государственный университет
Минск, Республика Беларусь
e-mail: {mazurenkopa@gmail.com, andrei.kalenik@gmail.com, razan@tut.by, shabinskaya@rambler.ru }

***Аннотация*—Излагаются основополагающие принципы процедуры формирования базисов модулярных систем счисления (МСС), предназначенных для табличной реализации мультипликативных операций по большим модулям методом Монтгомери. Применены оптимизационные критерии, которые обеспечивают широкие возможности для проведения табличных вычислений, сокращение расчетов, осуществляемых криптосистемами в реальном времени, минимизацию числа оснований МСС и объема оперативной памяти для таблиц.**

Ключевые слова: модулярные системы счисления, базисы систем счисления, схема Монтгомери

I. *Введение*

Как известно [1−5] мультипликативные операции, определенные на кольцах вычетов по большим модулям составляют эффективную основу для создания средств защиты информации. В частности они широко применяются в системах с открытым ключом, базирующихся на схемах RSA, Рабина и т.д. В свете сказанного особую важность имеют разработки по внедрению в практику новых вычислительных технологий (ВТ), которые обеспечивают высокую производительность при оперировании в диапазонах больших чисел (ДБЧ) и, прежде всего, при выполнении операций умножения и возведения в степень по большим модулям. В этом отношении значительный интерес представляет ВТ на основе модулярной арифметики (МА) – арифметики модулярных систем счисления (МСС).

С повышением уровня модульности целевых функций решаемых задач продуктивность МА существенно возрастает, причем на ДБЧ влияние данного фактора проявляется в наибольшей мере. Отмеченным свойством обладают, в частности, мультипликативные МА-процедуры, основанные на схеме Монтгомери [1, 3−5].

II. *Базовая мультипликативная схема Монтгомери*

Пусть A и B – операнды подлежащей выполнению операции умножения по некоторому большому модулю p и пусть A, B и p заданы кодами МСС с базисом $\{m_1, m_2, \ldots, m_k\}$ – т.е. с попарно простыми основаниями $m_1, m_2, \ldots, m_k$:

$A=(\alpha_1,\alpha_2,...,\alpha_k)$, $B=(\beta_1,\beta_2,...,\beta_k)$,

$p=(\pi_1,\pi_2,...,\pi_k)$, где $\alpha_i=|A|_{m_i}$, $\beta_i=|B|_{m_i}$, $\pi_i=|p|_{m_i}$ $(i=\overline{1,k};\ k>1)$; через $|x|_m$ обозначается элемент множества $\mathbf{Z}_m=\{0, 1, \ldots, m-1\}$, сравнимый с x (в общем случае рациональным числом) по натуральному модулю $m>1$.

Согласно методу Монтгомери в качестве искомого произведения A и B принимается целое число (ЦЧ) $\tilde{\gamma}=|ABM_l^{-1}|_p$ $\left(M_l=\prod_{i=1}^{l} m_i;\ 1<l<k\right)$.

В [4, 5] на базе минимально избыточной МА разработана мультипликативная схема Монтгомери, описываемая операционной последовательностью

$$\langle\ C=AB=(\gamma_1,\gamma_2,...,\gamma_k);$$

$$D=|CF|_{M_l}=(\delta_1,\delta_2,...,\delta_l)\ \ (F=|-p^{-1}|_{M_l}=$$

$$=(\varphi_1,\varphi_2,...,\varphi_l));(\hat{\delta}_{l+1},\hat{\delta}_{l+2},...,\hat{\delta}_k)=$$

$$=\mathrm{EC}(\hat{D};\{m_1,m_2,...,m_l\},\{m_{l+1},m_{l+2},...,m_k\});$$

$$\hat{\gamma}=\hat{C}/M_l=(\hat{\gamma}_{l+1},\hat{\gamma}_{l+2},...,\hat{\gamma}_k)(\hat{\gamma}_j=$$

$$=|(\gamma_j+|\hat{\delta}_j\pi_j|_{m_j})M_l^{-1}|_{m_j}\ \ (j=\overline{l+1,k}));$$

$$(\hat{\gamma}_1,\hat{\gamma}_2,...,\hat{\gamma}_l)=$$

$$=\mathrm{EC}(\hat{\gamma};\{m_{l+1},m_{l+2},...,m_k\},\{m_1,m_2,...,m_l\});$$

$$\tilde{\gamma}=\hat{\gamma}-(1-\mathrm{sn}(\hat{\gamma}-p))p\ \rangle;$$

где через EC и sn обозначаются соответственно операция расширения модулярного кода [7] и знаковая функция вида

$$\mathrm{sn}(x)=\begin{cases}0, & \text{если } x\geq 0,\\ 1, & \text{если } x<0.\end{cases}$$

Предложенная схема реализуется с помощью двух МСС: неизбыточной и минимально избыточной. Первая МСС определяется базисом $\{m_1, m_2, ..., m_l\}$ на диапазоне $\mathbf{Z}_{M_l}$, а вторая – базисом $\{m_{l+1}, m_{l+2}, ..., m_k\}$ на диапазоне $\mathbf{Z}_{2M'}^{-}=\{\_M',-M'+1, ..., M'-1\}$, где $\left(M'=m_0\left(\prod_{i=1}^{k-1} m_i\right)/M_l=M/M_l;\ m_0-\right.$ вспомогатель-

ный модуль ($m_0 \geq \_l-2$, $\_l=k-1$); $m_k \geq 2m_0+k-l-2$; M_l и p взаимно просты. При этом основания МСС и модуль p удовлетворяют условию

$$\begin{cases} 4p + M_{l-1}(l-2) < M_l, \\ 2p < M / M_l \end{cases} \quad (1)$$

III. *Принципы синтеза процедуры формирования базисов МСС*

Реализационная база предложенной схемы Монтгомери в решающей мере зависит от величины модулей МСС. Известные МА-умножители по большим p, конструируемые как правило на БИС- и СБИС-архитектурах обычно используют 32-битовые основания [1, 3]. Это ограничивает возможности повышения производительности за счет внедрения табличных технологий. В рамках табличного подхода к построению средств умножения для криптосистем вычислительный процесс, осуществляемый в реальном времени удается в максимальной степени разгрузить от трудоемких расчетов, которые могут быть выполнены предварительно. В первую очередь к таким расчетам относятся процедуры формирования базового комплекта таблиц (КТ) для мультипликативных МА-алгоритмов на ДБЧ. Реализация сформулированного принципа позволяет синтезировать алгоритмы умножения с предельно простой таблично-сумматорной конфигурацией, включающие лишь операции извлечения вычетов из предварительно генерируемых таблиц и накопления сумм ЦЧ с помощью позиционных сумматоров стандартной разрядности. При этом время мультипликативных операций на ДБЧ значительно уменьшается.

Следуя критерию максимального заполнения (упаковки) таблиц в условиях байтовой организации их слов, основания m_1, m_2, ..., m_k будем выбирать из множества простых чисел (ПЧ) интервала $(2^{15}; 2^{16})$. Применяемая методика выбора базисов МСС предусматривает построение по методу “решета” Эратосфена [6] таблицы (массива) TPrine ПЧ, не превышающих установленного порога m_max и распределение k последних (наибольших) элементов этой таблицы по двум искомым наборам оснований, помещаемым в (l+1)- и ($\_l$+1)-элементные массивы ABas1 и ABas2 соответственно. Содержимое данных массивов формируются по правилам: ABas1[i] = m_i = TPrine[N–2l+ 2i]($i = \overline{1, l}$); ABas2[j] = m_{l+j} = TPrine[N–2$_l$ + 2j–1]($j = \overline{1, \_l}$), где N – количество ПЧ в таблице TPrine. Получаемые базисы фиксируются как искомые при выполнении системы условий:

$$\begin{cases} r + 2 < \sum_{i=1}^{l-1} \log_2 m_i + \log_2 (m_l - l + 2), \\ r + 1 < \log_2 m_0 + \sum_{j=l+1}^{k-1} \log_2 m_j, \end{cases} \quad (2)$$

где $r = \lceil \log_2 p \rceil$ – разрядность модуля p;

$$m_0 = \lfloor (m_k - (k-l) + 2)/2 \rfloor = \lfloor (m_k - \_l + 2)/2 \rfloor;$$

через $\lfloor x \rfloor$ и $\lceil x \rceil$ обозначаются наибольшее и наименьшее ЦЧ соответственно не большее и не меньшее вещественной величины x.

Условия (2) представляют собой усиленный вариант условий (1), получаемый в результате замены p на 2^r.

Компьютерные расчеты по алгоритму, синтезированному на основе изложенных принципов формирования базисов МСС [7] показывают, что для модулей p, разрядностью 1024÷2462 бита наборы модулей $\{m_1, m_2, ..., m_l\}$ и $\{m_{l+1}, m_{l+2}, ..., m_k\}$ содержат от 65 до 155 оснований

[1] Shinichi Kawamura, Masanobu Koike, Fumihiko Sano, Atsushi Shimbo. Cox-Rower architecture for fast parallel Montgomery multiplication. - Eurocrypt 2000, LNCS. – Vol. 1807. – Berlin, 2000. – P. 523–538.

[2] Ю.С. Харин, В.И. Берник, Г.В. Матвеев и др. Математические и компьютерные основы криптологии. – Мн.: Новое знание, 2003. – 382с.

[3] J.-C. Bajard, L. Imbert. A Full RNS Implementation of RSA. - IEEE Trans. Comp. – 2004. – Vol. 53, № 6. – P. 769–774.

[4] А.Ф. Чернявский, А.А. Коляда, Н.А. Коляда, Е.В. Шабинская. Умножение по большим модулям методом Монтгомери с применением минимально избыточной модулярной арифметики. – Нейрокомпьютеры: разраб., применение. – 2010. – № 9. Москва, 2010. – С. 3–8.

[5] А.Н. Каленик, А.А. Коляда, Н.А. Коляда, А.Ф. Чернявский, Е.В. Шабинская. Умножение и возведение в степень по большим модулям с использованием минимально избыточной модулярной арифметики. – Информационные технологии. – 2012. – № 4. – С. 37–44.

[6] И.М. Виноградов. Основы теории чисел. – М.: Наука, – 1972. – 168 с.

[7] А.Н. Каленик, А.А. Коляда, Н.А. Коляда, Т.Г. Протько, Е.В. Шабинская. Компьютерно-арифметическая и реализационная база быстрых процедур умножения по большим модулям на основе модифицированной модулярной схемы Монтгомери. – Электроника инфо. – 2012. – № 2. – С. 105–108.