УДК 681.3

А.Н. Каленик, д.ф.-м.н. А.А. Коляда, Н.А. Коляда,
академик НАН Беларуси А.Ф. Чернявский, к.т.н. Е.В. Шабинская

Умножение и возведение в степень по большим модулям с использованием минимально избыточной модулярной арифметики

Предлагаются новые быстрые алгоритмы умножения и возведения в степень по большому модулю, основанные на минимально избыточной модулярной схеме Монтгомери. Главной отличительной особенностью разработанной схемы является использование интервально-индексных характеристик и интервально-модулярной формы чисел в базовых процедурах расширения кода. Достигаемая за счет этого оптимизация синтезированных мультипликативных алгоритмов обеспечивает (3,5−3,6)-кратное повышение производительности (в сравнении с наиболее близким модулярным аналогом) при выполнении на однопроцессорной ЭВМ. В случае мультипроцессорной реализации получаемый выигрыш в быстродействии является (7−8)-кратным. Созданные алгоритмы предназначены для применения в криптосистемах с открытым ключом.

Криптосистема, умножение и возведение в степень по большому модулю, мультипликативная схема Монтгомери, модулярная система счисления, минимально избыточная модулярная арифметика, интервальный индекс, интервально-модулярная форма, расширение модулярного кода.

Введение

Как известно [1−11] мультипликативные операции, определенные на кольцах вычетов по большим модулям составляют эффективную основу для построения систем криптографической защиты информации. В частности они широко применяются в системах электронной цифровой подписи , а также в криптосистемах 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, 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 модулярная вычислительная технология (МВТ).

В настоящее время арифметика модулярных систем счисления (МСС) – модулярная арифметика (МА) широко применяется в системах параллельной обработки для решения задач, требующих быстрых точных вычислений. Внутренний (кодовый) параллелизм модулярных вычислительных структур (МВС) обеспечивает ей ряд существенных преимуществ над позиционными структурами при проведении расчетов в ДБЧ. К таким преимуществам относятся: независимость длительности модульных операций при их параллельной реализации от числа оснований, а значит от длины кода МСС; идеальная приспособленность алгоритмов МА к конвейеризации и табличным вычислениям; простота организации на базе инструментальных платформ позиционного типа многомашинного и мультипроцессорного режимов обработки данных; гибкость табличного механизма реконфигурации МВС и др.

С повышением уровня модульности выполняемых вычислительных процессов продуктивность МСС значительно возрастает, причем на ДБЧ влияние данного фактора особенно ощутимо. Весьма показательным в этом отношении примером служат мультипликативные МА-процедуры, основанные на схеме Монтгомери [4−15]. В рамках метода Монтгомери используется операция деления нацело, а не операция общего деления. Поэтому модулярные конфигурации алгоритма Монтгомери для умножения по большим модулям отличаются высокой производительностью.

Наиболее трудоемкую часть МА-процедур Монтгомери составляют операции расширения модулярного кода (МК). Оптимизация данных операций является ключевым направлением развития МВТ на ДБЧ для крип-

тографических приложений. Эффективной основой для решения обозначенной оптимизационной проблемы могут служить минимально избыточные МСС (МИМСС) [16−19].

Представляемая разработка нацелена на реализацию фундаментальных преимуществ табличной конфигурации компьютерной арифметики МИМСС – минимально избыточной МА (МИМА) на ДБЧ в части оптимизации алгоритмов умножения и возведения в степень по большому модулю, базирующихся на схеме Монтгомери.

1. Компьютерно-арифметическая база модулярных мультипликативных процедур на основе схемы Монтгомери.

Введем обозначения:

- $\mathbf{Z}$ – множество целых чисел (ЦЧ);
- $\lfloor x \rfloor$ и $\lceil x \rceil$ − наибольшее и наименьшее ЦЧ соответственно не большее и не меньшее вещественной величины x;
- $\mathbf{Z}_m = \{0, 1, \ldots, m-1\}$ и $\mathbf{Z}_m^- = \{-\lfloor m/2 \rfloor, -\lfloor m/2 \rfloor+1, \ldots, \lceil m/2 \rceil-1\}$ – множества наименьших неотрицательных и абсолютно наименьших вычетов по натуральному модулю $m>1$ соответственно;
- $|a|_m$ – элемент множества $\mathbf{Z}_m$, сравнимый с a (в общем случае рациональной величиной) по модулю m;
- $\mathrm{sgn}(x)$ – знаковая функция вида $\mathrm{sgn}(x) = \begin{cases} 0, & \text{если } x \geq 0, \\ 1, & \text{если } x < 0; \end{cases}$
- $M_n = \prod_{j=1}^{n} m_j$, $M_{i,n} = M_n / m_i$ $(i = \overline{1,n})$, где $m_1, m_2, \ldots, m_n$ – натуральные модули ($n \geq 1$);
- p – рабочий модуль (большое ЦЧ) для мультипликативных операций.

На множестве $\mathbf{Z}$ МСС определяется посредством набора попарно простых модулей (оснований) – $m_1, m_2, \ldots, m_k$ ($k>1$). Число $X \in \mathbf{Z}$ в данной МСС представляется в виде $X=(\chi_1, \chi_2, ..., \chi_k)$ ($\chi_i = |X|_{m_i}$ $(i = \overline{1,k})$). В неизбы-

точной МСС с основаниями $m_1, m_2, \ldots, m_k$ можно закодировать не более M_k ЦЧ. При этом в качестве диапазона используют множества $\mathbf{Z}_{M_k}$ или $\mathbf{Z}^{-}_{M_k}$.

Декодирующее отображение для МСС с диапазоном $\mathbf{Z}_{M_k}$, ставящее в соответствие коду $(\chi_1, \chi_2, ..., \chi_k)$ единственный элемент X из $\mathbf{Z}^{-}_{M_k}$, может быть реализовано [16] с помощью соотношения

$$X = \sum_{i=1}^{k-1} M_{i,k-1} \left| M^{-1}_{i,k-1} \chi_i \right|_{m_i} + M_{k-1} I_k(X), \qquad (1)$$

где; $I_k(X)$ – интервальный индекс (ИИ) числа X относительно модулей $m_1, m_2, \ldots, m_k$. Выражение (1) называется интервально-модулярной формой (ИМФ) ЦЧ X.

Справедливо [16] следующее утверждение.

Теорема 1. Для ИИ $I_l(X)$ ЦЧ $X \in \mathbf{Z}_{M_l}$ в МСС с попарно простыми основаниями $m_1, m_2, \ldots, m_{l-1}$, $m_l \geq l-2$ $(l \geq 2)$ имеет место формула

$$I_l(X) = \hat{I}_l(X) - m_l \Theta_l(X), \qquad (2)$$

где

$$\hat{I}_l(X) = \left| I_l(X) \right|_{m_l} = \left| \sum_{i=1}^{l} R_{i,l}(\chi_i) \right|_{m_l}; \qquad (3)$$

$$R_{i,l}(\chi_i) = \left| -m_i^{-1} \left| M^{-1}_{i,l-1} \chi_i \right|_{m_i} \right|_{m_l} \quad (i = \overline{1, l-1}), \quad R_{l,l}(\chi_l) = \left| M^{-}_{l-1} \chi_l \right|_{m_l}; \qquad (4)$$

$\Theta_l(X) \in \{0,1\}$.

Величина $\Theta_l(X)$ называется минимальной интегральной характеристикой МК (ИХМК), отвечающая ЦЧ X в МСС с основаниями $m_1, m_2, \ldots, m_l$.

Из-за наличия в (2) $\Theta_l(X)$ в классической (неизбыточной) МСС вычисление интервально-индексной характеристики $I_l(X)$ требует применения общего алгоритма формирования ИХМК [16, 20], который является довольно трудоемким.

Арифметические свойства МСС удается значительно улучшить за счет избыточного кодирования элементов рабочего диапазона. Предложенное в [16] так называемое минимально-избыточное модулярное кодирование $\Phi_{\text{МИМСС}}$: $(\mathbf{Z}_{m_1} \times \mathbf{Z}_{m_2} \times ... \times \mathbf{Z}_{m_k}) \to \mathbf{D}$ предусматривает использование диапазона $\mathbf{D}$ с мощностью $|\mathbf{D}| < M_k$. Сущность реализуемого принципа раскрывает нижеследующее утверждение.

Теорема 2. Для того, чтобы в МСС с попарно простыми основаниями $m_1, m_2, \ldots, m_k$ ИИ $I(X) = I_k(X)$ каждого элемента X диапазона $\mathbf{D} = \mathbf{Z}_{2M}^{-} = \{-M, -M+1, ..., M-1\}$ ($M=m_0M_{k-1}$; m_0 – вспомогательный модуль) однозначно определялся компьютерным ИИ – вычетом $\hat{I}_k(X) = |I(X)|_{m_k}$, необходимо и достаточно, чтобы k-е основание МСС удовлетворяло условию $m_k \geq 2m_0+k-2$ ($m_0 \geq k-2$). При этом для $I(X)$ верна формула

$$I(X) = \begin{cases} \hat{I}_k(X), & \text{если } \hat{I}_k(X) < m_0, \\ \hat{I}_k(X) - m_k, & \text{если } \hat{I}_k(X) \geq m_k - m_0 - k + 2. \end{cases} \qquad (5)$$

Компьютерный ИИ $\hat{I}_k(X)$ вычисляется согласно (3), (4) при $l=k$.

Из теоремы 2 видно, что при минимально избыточном модулярном кодировании ИИ и, отвечающая ему ИМФ, позволяют достичь принципиально нового, в сравнении с традиционными конфигурациями МА, уровня оптимизации немодульных процедур по таким, в частности, характеристикам как быстродействие и объем реализационных затрат. Весьма показательными в этом отношении являются операции расширения МК, выполняемые в рамках МА-алгоритмов Монтгомери для умножения по большим модулям p [17−19].

Пусть, например, некоторый МК $(\chi_{l+1}, \chi_{l+2}, ..., \chi_k)$ по набору оснований $\{m_{l+1}, m_{l+2}, ..., m_k\}$ ($1<l<k$) необходимо расширить на модули m_j $j = \overline{1,l}$). Если на m_k наложить условие

$$m_k \geq 2m_0+k-l-2 \ (m_0 \geq k-l-2), \qquad (6)$$

то согласно теореме (2) МСС с основания $m_{l+1}, m_{l+2}, ..., m_k$ и диапазоном $\mathbf{D}' = \mathbf{Z}^{-}_{2M'} = \{-M', -M'+1, ..., M'-1\}$ $(M' = M / M_l)$ будет минимально избыточной. Предположим, что коду $(\chi_{l+1}, \chi_{l+2}, ..., \chi_k)$ отвечает ЦЧ $X \in \mathbf{D}'$. Тогда требуемая операция расширения сводится к расчету ИИ $I'_k(X)$ числа $X=(\chi_{l+1}, \chi_{l+2}, ..., \chi_k)$ относительно $m_{l+1}, m_{l+2}, ..., m_k$ по формулам типа ((3)−(5)):

$$I'_k(X) = \begin{cases} \hat{I}'_k(X), & \text{если } \hat{I}'_k(X) < m_0, \\ \hat{I}'_k(X) - m_k, & \text{если } \hat{I}'_k(X) \geq m_k - m_0 - k + l + 2; \end{cases} \tag{7}$$

$$\hat{I}'_k(X) = |I'_k(X)|_{m_k} = \left| \sum_{i=l+1}^{k} R'_{i,k}(\chi_i) \right|_{m_k}; \tag{8}$$

$$R'_{i,k}(\chi_i) = \left| -m_i^{-1} \left| \frac{M_l m_i}{M_{k-1}} \chi_i \right|_{m_i} \right|_{m_k} \quad (i = \overline{l+1, k-1}), \; R'_{k,k}(\chi_k) = \left| \frac{M_l}{M_{k-1}} \chi_k \right|_{m_k}; \tag{9}$$

и применению к ИМФ

$$X = \sum_{i=l+1}^{k-1} \frac{M_{k-1}}{M_l m_i} \left| \frac{M_l m_i}{M_{k-1}} \chi_i \right|_{m_i} + \frac{M_{k-1}}{M_l} I'_k(X) \tag{10}$$

(см. (1)) операции приведения к остатку по модулю m_j. Результирующее расчетное соотношение имеет вид

$$\chi_j = |X|_{m_j} = \left| \sum_{i=l+1}^{k-1} \left| \frac{M_{k-1}}{M_l m_i} \right| \frac{M_l m_i}{M_{k-1}} \chi_i \Big|_{m_i} \Big|_{m_j} + \left| \frac{M_{k-1}}{M_l} I'_k(X) \right|_{m_j} \right|_{m_j} \quad (j = \overline{1, l}). \tag{11}$$

Для операции расширения МК ЦЧ X по набору $\mathbf{M}_1$ оснований на основания набора $\mathbf{M}_2$, где $\mathbf{M}_1, \mathbf{M}_2 \subset \mathbf{M}$ $\{m_1, m_2, ..., m_k\}$ будем употреблять условное обозначение ЕС(X; $\mathbf{M}_1$, $\mathbf{M}_2$).

Что касается модульных операций над произвольными ЦЧ A и B, заданными своими МК:

$$A=(\alpha_1,\alpha_2,...,\alpha_k),\ \ B=(\beta_1,\beta_2,...,\beta_k)\,(\alpha_i=|A|_{m_i},\beta_i=|B|_{m_i}\,(i=\overline{1,k}))\,,$$

то в МСС с основаниями $m_1,m_2,...,m_k$ они выполняются независимо по каждому из оснований, т.е. по правилу

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

$$(|\,\alpha_1\circ\beta_1\,|_{m_1},|\,\alpha_2\circ\beta_2\,|_{m_2},...,|\,\alpha_k\circ\beta_k\,|_{m_k})\ \ (\circ\in\{+,-,\cdot\})\,. \qquad (12)$$

В свойстве (12) заключается главное фундаментальное преимущество МА над арифметикой позиционных систем счисления (ПСС).

2. Метод Монтгомери для умножения по большому модулю

Пусть A, B – операнды подлежащей выполнению операции умножения по некоторому большому модулю p. Сущность основополагающей идеи, выдвинутой Монтгомери [21] для построения требуемой мультипликативной схемы, состоит в аддитивной вариации произведения $C=AB$, которая обеспечивает деление без остатка значения результирующего выражения на специально выбираемый вспомогательный модуль S. Для достижения указанной цели предложено варьирующее соотношение вида

$$\widetilde{C}=C+|\,-Cp^{-1}\,|_S\ p\,. \qquad (13)$$

При S взаимно простом с p из (13) следует, что

$$|\,\widetilde{C}\,|_S=|\,C+|\,-Cp^{-1}\,|_S\ p\,|_S=|\,C-Cp^{-1}p\,|_S=0\,. \qquad (14)$$

Таким образом, число

$$\widetilde{C}/S=(C+p\,|\,-Cp^{-1}\,|_S\,/S) \qquad (15)$$

является целым. Переход в (15) к остаткам по модулю p дает

$$|\,\widetilde{C}/S\,|_p=|\,C/S\,|_p=|\,AB/S\,|_p\,. \qquad (16)$$

В соответствии с (16) по методу Монтгомери в качестве искомого произведения операндов A и B принимается ЦЧ

$$\widetilde{\gamma}=|\,AB/S\,|_p=(\widetilde{C}/S)-Qp\,, \qquad (17)$$

где Q – однозначно определяемый (для заданных A и B) целочисленный коэффициент.

Изложенное позволяет заключить, что базовая вычислительная схема для метода Монтгомери сводится к операционной последовательности:

$$< C=AB;\ D=|CF|_S\ (F=|-p^{-1}|_S);\quad \widetilde{C}=C+Dp;\ \widetilde{\gamma}=(\widetilde{C}/S)-Qp >. \quad (18)$$

Как видно из (18) трудоемкость ПСС-версий метода Монтгомери определяется, главным образом, сложностью операций умножения больших чисел: AB, $|CF|_S$ и Dp. Сказанное относится и к операции мультипликативной инверсии: $F=|-p^{-1}|_S$. Однако, являясь параметром долговременного использования, величина F может быть получена на этапе предварительных вычислений. Поэтому сложность операции определения F принципиального значения не имеет. В МСС все указанные операции относятся к разряду модульных (см. (12)) и реализуются значительно проще, чем в ПСС. Именно этим обстоятельством, обусловленным кодовым параллелизмом МВС, в первую очередь, и продиктована целесообразность применения МА в криптосистемах.

3. Минимально избыточная модулярная схема Монтгомери для умножения по большим модулям

Пусть операнды A, B и модуль p заданы в МСС с основаниями m_1, m_2, ..., m_k: $A=(\alpha_1, \alpha_2, \ldots, \alpha_k)$, $B=(\beta_1, \beta_2, \ldots, \beta_k)$, $p=(\pi_1, \pi_2, \ldots, \pi_k)$ $(\alpha_i=|A|_{m_i}, \beta_i=|B|_{m_i}, \pi_i=|p|_{m_i}\ (i=\overline{1,k}))$ и пусть $S=M_l$ $(1<l<k)$. Так как мультипликативная инверсия $F\in \mathbf{Z}_{M_l}$, то она однозначно определяется своим МК $(\varphi_1, \varphi_2, \ldots, \varphi_l)$, цифры которого находятся согласно равенствам $\pi_i=|-1/\varphi_i|_{m_i}\ (i=\overline{1,l})$. Реализация данных равенств производится на стандартных компьютерных диапазонах, причем в ходе предварительных вычислений. Число D также определяется кодом МСС с основаниями m_1, m_2, ..., m_l:

$$D=|CF|_{M_l}=(\delta_1, \delta_2, \ldots, \delta_l)=(|\gamma_1\varphi_1|_{m_1}, |\gamma_2\varphi_2|_{m_2}, ..., |\gamma_l\varphi_l|_{m_l})$$

$$(\delta_i=|D|_{m_i}, \gamma_i=|C|_{m_i}=|\alpha_i\beta_i|_{m_i}\ (i=\overline{1,l}). \quad (19)$$

Поскольку ЦЧ D, полученное согласно (19) участвует в дальнейших вычислениях при получении $\widetilde{C}$ по полной системе модулей – m_1, m_2, ..., m_k, то МК (δ_1, δ_2, …, δ_l) должен быть расширен на остальные модули: m_{l+1}, m_{l+2}, …, m_k. В рамках неизбыточного модулярного кодирования, а именно таковым является кодовое пространство МСС с основаниями m_1, m_2, ..., m_l и диапазоном $\mathbf{Z}_{M_l}$, данная операция требует использования сложно вычисляемых ИХМК, например, ранга [8]. В целях устранения отмеченного негативного фактора D заменим на число

$$\hat{D} = \sum_{i=1}^{l-1} M_{i,l-1} \mid M_{i,l-1}^{-1} \delta_i \mid_{m_i} + M_{l-1} \hat{I}_l(D), \tag{20}$$

где $\hat{I}_l(D) = |I_l(D)|_{m_l}$ − компьютерный ИИ ЦЧ D и $\hat{D}$ относительно модулей m_1, m_2, ..., m_l, который вычисляется по формулам (3), (4) при $X = D$, $(\chi_1, \chi_2, ..., \chi_l) = (\delta_1, \delta_2, \ldots, \delta_l)$.

Применяя (1) и (2) запишем $\hat{D}$ в виде

$$\hat{D} = \sum_{i=1}^{l-1} M_{i,l-1} \mid M_{i,l-1}^{-1} \delta_i \mid_{m_i} + M_{l-1}(\hat{I}_l(D) - m_l \Theta_l(D) + m_l \Theta_l(D)) =$$

$$= \sum_{i=1}^{l-1} M_{i,l-1} \mid M_{i,l-1}^{-1} \delta_i \mid_{m_i} + M_{l-1} I_l(D) + M_l \Theta_l(D) = D + M_l \Theta_l(D), \tag{21}$$

где $\Theta_l(D)$ – двузначная минимальная ИХМК (см. теорему 1). Из (21) вытекает равенство

$$\mid \hat{D} \mid_{M_l} = D. \tag{22}$$

В соответствии с изложенным искомая модификация базового соотношения для вариации произведения C имеет вид

$$\hat{C} = C + \hat{D}p = C + (\sum_{i=1}^{l-1} M_{i,l-1} \mid M_{i,l-1}^{-1} \delta_i \mid_{m_i} + M_{l-1} \hat{I}_l(D)) p. \tag{23}$$

С учетом (20), (22) и (14) из (23) следует, что

$$\mid C \mid_{M_l} = \mid C + \mid \hat{D}p \mid_{M_l} \mid_{M_l} = \mid C + \mid Dp \mid_{M_l} \mid_{M_l} = 0.$$

Таким образом, ЦЧ (23) без остатка делится на M_l, то есть число

$$\hat{\gamma} = \hat{C} / M_l = (C + (\sum_{i=1}^{l-1} M_{i,l-1} \mid M_{i,l-1}^{-1} \delta_i \mid_{m_i} + M_{l-1} \hat{I}_l(D)) p) / M_l \qquad (24)$$

является целым.

Процесс реализации (24) в МСС с основаниями модулей m_1, m_2, ..., m_k, то есть получения кода $(\hat{\gamma}_1, \hat{\gamma}_2, ..., \hat{\gamma}_k)$ ЦЧ $\hat{\gamma}$ $(\hat{\gamma}_i = |\hat{\gamma}|_{m_i} (i = \overline{1, k}))$ состоит из двух шагов. На первом шаге $\hat{\gamma}$ вычисляется по набору модулей $\{m_{l+1}, m_{l+2}, ..., m_k\}$, а на втором шаге сформированный усеченный МК $(\hat{\gamma}_{l+1}, \hat{\gamma}_{l+2}, ..., \hat{\gamma}_k)$ расширяется на модули m_1, m_2, ..., m_l. При этом данная операция: ЕС($\hat{\gamma}$; $\{m_{l+1}, m_{l+2}, ..., m_k\}$, $\{m_1, m_2, ..., m_l\}$), естественно должна выполняться по упрощенной минимально избыточной процедуре расширения – согласно формулам (7)–(9), (11) при $X = \hat{\gamma}$, $(\chi_{l+1}, \chi_{l+2}, ..., \chi_k) = (\hat{\gamma}_{l+1}, \hat{\gamma}_{l+2}, ..., \hat{\gamma}_k)$.

Необходимым и достаточным условием корректности двухшагового процесса вычисления величины $\hat{\gamma}$ служит принадлежность ЦЧ $\hat{C}$ и $\hat{\gamma}$ соответственно неотрицательным компонентам $\{0, 1, ..., \lceil M_k/2 \rceil - 1\}$ диапазона $\mathbf{Z}_{M_k}^{-}$ МСС с основаниями m_1, m_2, ..., m_k и $\mathbf{Z}_{M'}$ диапазона $\mathbf{D}' = \mathbf{Z}_{2M'}^{-}$ МИМСС с основания m_{l+1}, m_{l+2}, ..., m_{k-1}, m_k. $\geq 2m_0 + k - l - 2$ (см. (6)). Поскольку из $0 \leq \hat{\gamma} = \hat{C} / M_l < M' = m_0 M_{k-1} / M_l$ вытекает неравенство $0 \leq \hat{C} < m_0 M_{k-1} \leq \leq M_{k-1}((m_k - k + l + 2)/2) < M_k/2$, то условие $\hat{\gamma} \in \mathbf{Z}_{M'}$ гарантирует выполнение и условия $\hat{\mathbf{C}} \in \mathbf{Z}_{M_k}^{-}$ при этом МСС с основаниями m_1, m_2, ..., m_k необязательно должна быть минимально избыточной.

Найдем ограничения на модули m_1, m_2, ..., m_k и p, гарантирующие выполнение условия $\hat{\gamma} \in \mathbf{D}'$. Получим сначала верхнюю оценку для $\hat{D}$.

Пусть $m\_\max = \max\{m_1, m_2, ..., m_k\}$. Из (20) имеем

$$\hat{D} = M_{l-1} \left(\sum_{i=1}^{l-1} m_i^{-1} \mid M_{i,l-1}^{-1} \delta_i \mid_{m_i} + \hat{I}_l(\hat{D}) \right) \leq M_{l-1} \left(\sum_{i=1}^{l-1} m_i^{-1} (m_i - 1) + m_l - 1 \right) =$$

$$= M_{l-1}\left(l-1-\sum_{i=1}^{l-1}\frac{1}{m_i}\right)+M_l-M_{l-1}<M_l+M_{l-1}\left(l-2-\sum_{i=1}^{l-1}\frac{1}{m\_\max}\right)<$$

$$<M_l+M_{l-1}\left(l-2-\left\lfloor\frac{l-1}{m\_\max}\right\rfloor\right)=M_l+M_{l-1}(l-2). \qquad (25)$$

Пусть $A, B\in\mathbf{Z}_p$. Тогда с учетом (25) из (24) получим

$$\hat{\gamma}<(p^2+(M_l+M_{l-1}(l-2))p)/M_l=p(1+(p+M_{l-1}(l-2))/M_l). \qquad (26)$$

Из (26) видно, что при $p+M_{l-1}(l-2)<M_l$ ЦЧ $\hat{\gamma}\in\mathbf{Z}_{2p}$. Такого же результата, то есть принадлежности $\hat{\gamma}$ множеству $\mathbf{Z}_{2p}$ можно достичь и в случае, когда $A, B\in\mathbf{Z}_{2p}$. Соответствующее ограничение на основания МСС и модуль p вытекает из неравенства $\hat{\gamma}<(4p^2+(M_l+M_{l-1}(l-2))p)/M_l<2p$ и имеет вид

$$4p+M_{l-1}(l-2)<M_l. \qquad (27)$$

В рамках данного условия, обеспечивающего $\hat{\gamma}\in\mathbf{Z}_{2p}$ при $A, B\in\mathbf{Z}_{2p}$, допускается режим многократного обращения к процедуре умножения по модулю p с использованием в качестве операндов результатов уже выполненных операций умножения. Это, в частности, необходимо для реализации в криптосистемах операций возведения в степень по модулю p.

Так на первом шаге применяемой мультипликативной схемы $\hat{\gamma}$ вычисляется в МИМСС с основаниями $m_{l+1}, m_{l+2}, \ldots, m_k$, то ее диапазон $\mathbf{D}'$ ввиду $\hat{\gamma}\in\mathbf{Z}_{2p}$ должен удовлетворять требованию

$$2p<M'=m_0M_{k-1}/M_l=M/M_l. \qquad (28)$$

Таким образом приведенные оценочные выкладки позволяют заключить, что при $A, B, \hat{\gamma}\in\mathbf{Z}_{2p}$, корректность предлагаемой вычислительной МИМА-схемы метода Монтгомери (см. (23), (24)) обеспечивается в рамках условий (27) и (28).

Переход в (24) к остаткам по модулю p дает $\tilde{\gamma}=|\hat{\gamma}|_p=|\hat{C}M_l^{-1}|_p=$ $=|ABM_l^{-1}|_p$. Поскольку $\hat{\gamma}<2p$, то искомое произведение ЦЧ A и B по модулю p можно получить по $\hat{\gamma}$ с использованием равенства $\tilde{\gamma}=|ABM_l^{-1}|_p=$

$= \hat{\gamma} - Qp$ $(Q \in \{0, 1\})$. При этом для величины Q справедлива формула $Q = 1 - \mathrm{sgn}(\hat{\gamma} - p)$.

С учетом вышеизложенного результирующую мультипликативную схему, основанную на МИМА, можно записать в виде операционной последовательности:

$$\langle C = AB = (\gamma_1, \gamma_2, ... \gamma_k,); D = |CF|_{M_l} = (\delta_1, \delta_2, ..., \delta_l) \ (F = |-p^{-1}|_{M_l} =$$
$$= (\varphi_1, \varphi_2, ..., \varphi_l)); (\hat{\delta}_{l+1}, \hat{\delta}_{l+2}, ..., \hat{\delta}_k) = \mathrm{EC}(\hat{\mathbf{D}}; \{m_1, m_2, ..., m_l\}, \{m_{l+1}, m_{l+2}, ..., m_k\});$$
$$\hat{\gamma} = \hat{C} / M_l = (\hat{\gamma}_{l+1}, \hat{\gamma}_{l+2}, ..., \hat{\gamma}_k)(\hat{\gamma}_j = |(\gamma_j + |\hat{\delta}_j \pi_j|_{m_j}) M_l^{-1}|_{m_j} \ (j = \overline{l+1, k})); \quad (29)$$
$$(\hat{\gamma}_1, \hat{\gamma}_2, ..., \hat{\gamma}_l) = \mathrm{EC}(\hat{\gamma}; \{m_{l+1}, m_{l+2}, ..., m_k\} \{m_1, m_2, ..., m_l\});$$
$$\tilde{\gamma} = \hat{\gamma} - (1 - \mathrm{sgn}(\hat{\gamma} - p))p \rangle.$$

Отметим, что расчет цифр МК $(\hat{\delta}_{l+1}, \hat{\delta}_{l+2}, ..., \hat{\delta}_k)$ числа $\hat{D}$ по набору модулей $\{m_{l+1}, m_{l+2}, ..., m_k\}$ осуществляется с помощью указанной в (29) операции расширения, которая в соответствии с (20) выполняется по правилу

$$\hat{\delta}_j = |\sum_{i=1}^{l-1} |M_{i,l-1}|M_{i,l-1}^{-1} \delta_i|_{m_i}|_{m_j} + |M_{l-1} \hat{I}_l(D)|_{m_j}|_{m_j} \ (j = \overline{l+1, k}) \quad (30)$$

с применением (3), (4). Поскольку $|\hat{C}|_{M_l} = 0$, то согласно (23) для МК числа $\hat{C}$ по набору оснований $\{m_1, m_2, ..., m_k\}$ верна формула

$$\hat{C} = (0,0,...,0, |\gamma_{l+1} + |\hat{\delta}_{l+1} \pi_{l+1}|_{m_{l+1}}|_{m_{l+1}}, ..., |\gamma_k + |\hat{\delta}_k \pi_k|_{m_k}|_{m_k}), \quad (31)$$

а для ЦЧ (24), вычисляемого в МИМСС с модулями m_{l+1}, m_{l+2}, ..., m_k, – формула

$$\hat{\gamma} = \hat{C} / M_l = (\hat{\gamma}_{l+1}, \hat{\gamma}_{l+2}, ..., \hat{\gamma}_k)(\hat{\gamma}_j = |M_l^{-1}(\gamma_j + |\hat{\delta}_j \pi_j|_{m_j})|_{m_j} \ (j = \overline{l+1, k})). \quad (32)$$

Из изложенного вытекает нижеследующее утверждение.

Теорема 3. Пусть наборы оснований (простых чисел): $\{m_1, m_2, ..., m_l\}$ и $\{m_{l+1}, m_{l+2}, ..., m_k\}$ неизбыточной и минимально избыточной МСС соответственно с диапазонами $\mathbf{Z}_{M_l}$ и $\mathbf{D}' = \mathbf{Z}_{2M'}^{-}$ $(M' = M / M_l, M = m_0 M_{k-1},$

$m_0 \geq k-l-2,\ m_k \geq 2m_0+k-l-2,\ 1<l<k)$ совместно с модулем p, взаимно простым с M_l, удовлетворяют условию

$$\begin{cases} 4p + M_{l-1}(l-2) < M_l, \\ 2p < M / M_l \end{cases} \tag{33}$$

и пусть операнды A и B мультипликативной операции $\tilde{\gamma} = |ABM_l^{-1}|_p$ принадлежат множеству $\mathbf{Z}_{2p} = \{0, 1, ..., 2p-1\}$. Тогда величина $\hat{\gamma}$, вычисляемая в рамках схемы (29), также является элементом множества $\mathbf{Z}_{2p}$ при этом $\hat{\gamma} \equiv \tilde{\gamma} (\mathrm{mod}\ p)$ и для $\tilde{\gamma}$ верна формула

$$\tilde{\gamma} = \hat{\gamma} - (1 - \mathrm{sgn}(\hat{\gamma} - p))p. \tag{34}$$

4. Алгоритмы умножения и возведения в степень по большому модулю на основе МИМА-схемы Монтгомери

На базе вычислительной МИМА-схемы (29) типа Монтгомери синтезированы алгоритмы модульного умножения и возведения в степень для криптосистем. Ключевой отличительной особенностью данных алгоритмов является широкое применение таблиц. При этом необходимый комплект рабочих таблиц генерируется на этапе предварительных вычислений с обеспечением минимизации трудоемкости процесса, реализуемого в реальном времени.

Алгоритм умножения по большому модулю *p*.

Параметры алгоритма: определяющие основания МСС – m_0, m_1, ..., m_k и модуль $p=(\pi_1, \pi_2, \ldots, \pi_k)$), которые удовлетворяют условиям теоремы 3.

Входные данные: операнды A и B ($A, B \in \mathbf{Z}_{2p}$), представленные в МСС – $A=(\alpha_1, \alpha_2, \ldots, \alpha_k)$, $B=(\beta_1, \beta_2, \ldots, \beta_k)$.

Выходные данные: МК $(\hat{\gamma}_1, \hat{\gamma}_2, ..., \hat{\gamma}_k)$ аналога $\hat{\gamma} \in \mathbf{Z}_{2p}$ произведения Монтгомери $\tilde{\gamma} = |ABM_l^{-1}|_p$ ($\hat{\gamma} \equiv \tilde{\gamma} (\mathrm{mod}\ p)$).

Предварительно вычисляемые данные:

- код ($\varphi_1, \varphi_2, \ldots, \varphi_l$) противоположного значения $F=|-p^{-1}|_{M_l}$ мультипликативной инверсии $|p^{-1}|_{M_l}$ модуля p в МСС с основаниями $m_1, m_2, ..., m_l$, получаемый с помощью равенств $\varphi_i=|-1/\pi_i|_{m_i}$ $(i=\overline{1, l})$;
- таблицы ИИ – *TIIi* и *TII_i*, которые формируются согласно (4) и (9):

  $TIIi\ [\chi]=R_{i,l}(\chi)$ $(\chi\in\mathbf{Z}_{m_i};\ i=\overline{1, l})$; $TII\_i\ [\chi]=R'_{i,k}(\chi)$ $(\chi\in\mathbf{Z}_{m_i};\ i=\overline{l+1, k})$;
- таблицы расширения МК – *TEi_j* и *TE_i_j*, генерируемые в соответствии с (11) и (30) по формулам

$$TEi\_j[\chi]=\begin{cases}|M_{i,l-1}|M_{i,l-1}^{-1}\chi|_{m_i}|_{m_j}\ (\chi\in\mathbf{Z}_{m_i}) \text{ при } i=\overline{1, l-1},\\ |M_{l-1}\chi|_{m_j}\ (\chi\in\mathbf{Z}_{m_l}) \text{ при } i=l\end{cases} \qquad (j=\overline{l+1, k});$$

$$TE\_i\_j[\chi]=\begin{cases}|\dfrac{M_{k-1}}{M_l m_i}|\dfrac{M_l m_i}{M_{k-1}}\chi|_{m_i}|_{m_j}\ (\chi\in\mathbf{Z}_{m_i}) \text{ при } i=\overline{l+1, k-1},\\ |\dfrac{M_{k-1}}{M_l}\chi|_{m_j}\ (\chi\in\mathbf{Z}_{m_k}) \text{ при } i=k \text{ и } \chi<m_0,\\ |\dfrac{M_{k-1}}{M_l}(\chi-m_k)|_{m_j}\ (\chi\in\mathbf{Z}_{m_k}) \text{ при } i=k \text{ и } \chi\ge m_0\end{cases} \qquad (j=\overline{1, l});$$

- таблицы *TMPli* умножения на константу M_l^{-1}, которые согласно (32) рассчитываются по формуле: $TMPli\,[\chi]=|M_l^{-1}\chi|_{m_i}$ $(\chi\in\mathbf{Z}_{2m_i-1};\ i=\overline{l+1, k})$.

Тело алгоритма.

УМ.М1 Найти произведение $C=AB=(\gamma_1, \gamma_2, ..., \gamma_k) = (|\alpha_1\beta_1|_{m_1}, |\alpha_2\beta_2|_{m_2}, \ldots, |\alpha_k\beta_k|_{m_k})$.

УМ.М2 В МСС с основаниями $m_1, m_2, ..., m_l$ сформировать код числа $D=|CF|_{M_l}$: $(\delta_1, \delta_2, ..., \delta_l) = (|\gamma_1\varphi_1|_{m_1}, |\gamma_2\varphi_2|_{m_2}, ..., |\gamma_l\varphi_l|_{m_l})$.

УМ.М3 Вычислить интервально-индексную характеристику $\hat{I}_l(\hat{D})=\hat{I}_l(D)$ числа $\hat{D}=\sum_{i=1}^{l-1}M_{i,\,l-1}|M_{i,\,l-1}^{-1}\delta_i|_{m_i}+M_{l-1}\hat{I}_l(D)$ по расчетному соотношению $\hat{I}_l(\hat{D})=\eta_l=|\sum_{i=1}^{l}TIIi[\delta_i]|_{m_l}$.

УМ.М4 Определить цифры МК $(\hat{\delta}_{l+1}, \hat{\delta}_{l+2}, ..., \hat{\delta}_k)$ ЦЧ $\hat{D}$ в МСС с основаниями m_{l+1}, m_{l+2}, ..., m_k. по правилу

$$\hat{\delta}_j = |\sum_{i=1}^{l-1} TEi\_j[\delta_i] + TEl\_j[\eta_l]|_{m_j} \ (j = \overline{l+1, k}).$$

УМ.М5 Получить код числа $\hat{C} = C + \hat{D}p$ в МИМСС с модулями m_{l+1}, m_{l+2}, ..., m_k.:

$$(\gamma'_{l+1}, \gamma'_{l+2}, ..., \gamma'_k) = (\gamma_{l+1} + |\hat{\delta}_{l+1}\pi_{l+1}|_{m_{l+1}}, \gamma_{l+2} + |\hat{\delta}_{l+2}\pi_{l+2}|_{m_{l+2}}, ..., \gamma_k + |\hat{\delta}_k\pi_k|_{m_k}.$$

УМ.М6 В МИМСС с основаниями m_{l+1}, m_{l+2}, ..., m_k сформировать код $(\hat{\gamma}_{l+1}, \hat{\gamma}_{l+2}, ..., \hat{\gamma}_k)$ ЦЧ $\hat{\gamma} = \hat{C}M_l^{-1}$ по правилу $\hat{\gamma}_i = TMPli[\gamma'_i]$ $(i = \overline{l+1, k})$.

УМ.М7 Рассчитать интервально-индексную характеристику $\hat{I}'_k(\hat{\gamma})$ ЦЧ $\hat{\gamma}$: $\hat{I}'_k(\hat{\gamma}) = \eta'_k = |\sum_{i=l+1}^{k} TII\_i[\hat{\gamma}_i]|_{m_k}$.

УМ.М8 Расширить МИМК $(\hat{\gamma}_{l+1}, \hat{\gamma}_{l+2}, ..., \hat{\gamma}_k)$ на модули m_1, m_2, ..., m_l :с применением соотношения $\hat{\gamma}_j = |\sum_{i=l+1}^{k-1} TE\_i\_j[\hat{\gamma}_i] + TE\_k\_j[\eta'_k]|_{m_j}$ $(j = \overline{1, l})$.

УМ.М9 Число $\hat{\gamma} = \hat{C}M_l^{-1} = (\hat{\gamma}_1, \hat{\gamma}_2, ..., \hat{\gamma}_k)$ зафиксировать в качестве искомого аналога нормированного произведения $\tilde{\gamma} = |ABM_l^{-1}|_p$ операндов A и B по модулю p и завершить работу алгоритма.

Мультипликативная МИМА-процедура Монтгомери УМ.М1 − УМ.М9 предназначена в первую очередь для вычисления степеней натуральных чисел по большим модулям p – целочисленных величин вида $Y = |X^E|_p$, где X и E – заданы соответственно модулярным и двоичным кодами: X=(χ_1, χ_2, …, χ_k) и $E = (e_{s-1}\ e_{s-2}\ \ldots\ e_0)_2$ ($e_{s-1} = 1$; s – разрядность ЦЧ E). Примем в качестве основы для расчета степеней традиционно применяемый метод умножения с возведением в квадрат (square multiply method) [1, 2, 8], который использует мультипликативную декомпозицию функции Y:

$$Y = \left| X^{\sum_{j=0}^{s-1} e_j 2^j} \right|_p = \left| X^{e_0} (X^{e_1} (X^{e_2} (...(X^{e_{s-2}} (X^{e_{s-1}})^2)^2...)^2)^2)^2 \right|_p . \qquad (35)$$

Введем для операции умножения по модулю p, выполняемой согласно процедуре УМ.М1 − УМ.М9, обозначение ММ(A, B) (A и B − операнды, представленные в МСС с основаниями m_1, m_2, ..., m_k). Тогда на базе (35) можно сформулировать нижеследующий алгоритм возведения в степень.

Входные данные: $X=(\chi_1, \chi_2, \ldots, \chi_k)$ $(\chi_i=|X|_{m_i})$ $(i=\overline{1,k})$, $X\in\mathbf{Z}_{2p}$; $E=(e_{s-1}\, e_{s-2} \ldots e_0)_2$ $(e_{s-1}=1;\ s\geq 1)$.

Выходные данные: $Y=(\xi_1, \xi_2, \ldots, \xi_k)$ $(\xi_i=|Y|_{m_i}$ $(i=\overline{1,k})$, $Y\equiv X^E (\mathrm{mod}\, p)$, $Y\in\mathbf{Z}_{2p}$.

Предварительно вычисляемые данные:

$N=|M_l^2|_p=(\nu_1,\nu_2,...,\nu_k)$ $(\nu_i=|N|_{m_i}$ $(i=\overline{1,k}))$, $M_l=\prod_{i=1}^{l} m_i$ $(1<l<k)$.

Тело алгоритма:

ВС1. Получить МК $(\chi'_1,\chi'_2,...,\chi'_k)$ ЧЧ X' = ММ(X, N).

ВС2. Присвоить переменной $Y=(\xi_1, \xi_2, \ldots, \xi_k)$ начальное значение $Y=X'$.

ВС3. Для всех $j=s-2, s-3, \ldots, 0$ выполнить:

а) Y = ММ(Y, Y);

б) если $e_j=1$, то найти Y = ММ(Y, X').

ВС4. Определить МК $(\chi_1, \chi_2, \ldots, \chi_k)$ искомого значения степени: $Y=MM(Y, 1)$ и завершить работу алгоритма.

Используемая в алгоритме ВС1−ВС4 константа N обеспечивает отсутствие в конечном результате Y коэффициента M_l^{-1} произведений Монтгомери. Требуемый МК этой константы можно получить с помощью синтезированного в [22] МИМА-алгоритма деления по схеме Ферма.

В таблице приведены времена выполнения алгоритма УМ.М1−УМ.М9 на ПЭВМ и мультипроцессорном кластером (МПК). Представленные данные получены в предположении, что основания МСС являются 16-битовыми. По сравнению с наиболее близким модулярным аналогом − разработкой фирмы Toshiba [8], однопроцессорная программная версия предложенного алгоритма обеспечивает повышение производительности в 3,5-3,6 раз при p разрядностью 1024−2462 бита. В случае мультипроцессорной реализации достигаемый выигрыш в быстродействии как минимум 8-кратный. Временные затраты на выполнение операции модульного возведения в степень прямо пропорциональны соответствующим характеристикам применяемых процедур умножения с коэффициентом, примерно составляющим 1,5 s (s – разрядность показателя степени).

Заключение

Представленная разработка по оптимизации модулярной схемы Монтгомери для умножения по большим модулям показывает, что для решения данной проблемы табличная МИМА обеспечивает принципиально новые возможности. Наиболее важные результаты выполненных исследований состоят в нижеследующем.

1. В мультипликативной МА-схеме Монтгомери применен новый способ аддитивной вариации произведения операндов, обеспечивающий сокращение реализационных затрат при расчете базовой ИХМК на первом каскаде схеме в $l/2$ раз.

2. Для мощностей диапазонов используемых усеченных МСС получены устанавливаемые в соответствии с разрядностью рабочего модуля p условия, которые гарантируют корректность режима многократного обращения к МИМА-процедуре умножения без выхода результатов за пределы кольца $\mathbf{Z}_{2p}$, в том числе и в рамках созданного алгоритма модульного возведения в степень. При этом также достигается уменьшение затрат при формировании ИХМК на втором каскаде схемы в $(k-l)/2$ раз.

3. На базе МИМА-схемы Монтгомери синтезирован алгоритм умножения по модулю p, имеющий сумматорно-табличную конфигурацию. Для его выполнения требуются лишь операции извлечения вычетов из таблиц и суммирование ЦЧ на позиционных сумматорах стандартной разрядности.

4. Для предложенного МИМА-алгоритма умножения по большим модулям приведены оценки минимальных временных затрат на его реализацию как в мультипроцессорном кластере, так и в ПЭВМ. Однопроцессорная программная версия алгоритма при (1024−2462)-битовых p превосходит адекватный вариант наиболее близкого модулярного аналога [8] по производительности в 3,5−3,6 раз. Это относится и к синтезированной процедуре модульного возведения в степень.

Список литературы

1. Харин, Ю.С. Компьютерный практикум по математическим методам защиты информации / Ю.С. Харин, С.В. Агиевич. –Мн.: БГУ, 2001. – 190 с.

2. Харин, Ю.С. Математические и компьютерные основы криптологии / Ю.С. Харин и др. – Мн.: Новое знание, 2003. – 382 с.

3. Инютин С.А. Основы модулярной арифметики / С.А. Инютин. – Ханты-Мансийск: Полиграфист, 2008. – 208 с.

4. Posch, K.S. Modulo reduction in residue number system / K.S. Posch, R. Posch // IEEE Trans. on parallel and distributed syst. – 1995. – Vol. 6, № 5. – P. 449–454.

5. Schwemmlein, J. RNS-modulo reduction upon a restricted base value set and its applicability to RSA cryptography // J. Schwemmlein, K.S. Posch, R. Posch // Comput. and security. – 1998. – Vol. 17, № 7. – P. 637–650.

6. Bajart, J.-C. An RNS montgomery modular multiplication algorithm / J.-C. Bajart, L.-S. Didier, P. Kornerup // IEEE Trans. Comput. – 1998. – Vol. 47, № 7. – P. 766–776.

7. Hiasat, A.A. New efficient structure for a modular multiplier for RNS / A.A. Hiasat // IEEE Trans. Comput.– 2000.– Vol. 49, № 2. – P. 170–174.

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

9. Nozaki, H. Implementation of RSA Algorithm Based on RNS Montgomery Multiplication / H. Nozaki, M. Motoyama, A. Shimbo, S. Kawamura // Proc. Cryptographic Hardware and Embedded Systems (CHES 2001). – Sept., 2001. – P. 364–376.

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

11. Амербаев, В.М. Модулярная арифметика, как криптографический примитив / В.М. Амербаев, В.Н. Дьячков // Юбил. международная научно-техн. конференция «50 лет модулярной арифметики" (В рамках 5-ой международной научно-технической конференции «Электроника и информатика – 2005"). – Зеленоград, РФ 23-25 нояб., 2005. – Сб. начн. трудов. – М.; Зеленоград: НИЭТ; М.; Зеленоград: АНГСТРЕМ, 2006. – С. 187–193.

12. Lim, Z. An RNS-Enhanced microprocessor implementation of public key cryptography / Z. Lim, B.J. Phillips // Signals, Systems and Computers.-2007.-ACSSC 2007. Conf. Rec. of the forte-first Asilomar Conf. – 4–7 nov., 2007. – P. 1430–1434.

13. Shien, M.-D. An new modular exponentiation architecture for efficient design of RSA cryptosystem / M.-D. Shien, J.-H. Chen, H.-S. Wu, W.-C. Lin // IEEE Trans. Very Large Scale Integr. (VLSI) Syst. – 2008. – Vol. 16, № 9. – P. 1151–1161.

14. Lee, K.-J. Systolic multiplier for Montgomery's algorithm / K.-J. Lee, K.-J. Yoo // Integration. – 2002. – Vol. 32, № 1–2. – P. 99–109.

15. RSA speedup with residue number system immune against hardware fault cryptanalysis / S.-M. Yen [et al.] // Lect. Notes Comput. Sci. – 2002. – Vol. 2288. – P. 297–413.

16. Коляда, А.А. Модулярные структуры конвейерной обработки цифровой информации / А.А. Коляда, И.Т. Пак. – Минск: Университетское. –1992. – 256 с.

17. Чернявский, А.Ф. Интервально-индексная технология расширения модулярного кода / А.Ф. Чернявский, А.А. Коляда, Н.А. Коляда, Е.В. Шабинская // Электроника инфо. – 2010. – № 6. – С. 66–71.

18. Коляда, А.А. Умножение по большим модулям с использованием минимально избыточной модулярной схемы Монтгомери / А.А. Коляда, А.Ф. Чернявский // Информатика. – 2010. – № 3. – С. 31−48.

19. Умножение по большим модулям методом Монтгомери с применением минимально избыточной модулярной арифметики / А.Ф. Чернявский, А.А. Коляда, Н.А. Коляда, Е.В. Шабинская : материалы Всерос. науч. конф. с элементами научной школы для молодежи «Параллельная компьютерная алгебра», Ставрополь, 11−15 окт. 2010 г. / Ставрополь. гос. у-т // Нейрокомпьютеры: разработка, применение. – 2010. − № 9. − С. 3–8.

20. Коляда, А.А. Общая технология вычисления интегральных характеристик модулярного кода / А.А. Коляда, А.Ф. Чернявский // Доклады НАН Беларуси. – 2008. – Т. 52, № 4. – С. 38–44.

21. Montgomery, P.L. Modular multiplication without trial division / P.L. Montgomery // Mathematics of Computation.– 1985. – Vol. 170, № 44. – P. 519–521.

22. Умножение по большому модулю в минимально избыточной модулярной системе счисления с применением операций масштабирования / А.А. Коляда, Н.А. Коляда, В.В. Ревинский, А.Ф. Чернявский, Е.В. Шабинская // Информатика. – 2009. – № 4. – С. 49–65.

Таблица – Времена выполнения МИМА-алгоритма умножения по модулю на основе метода Монтгомери с использованием процессоров Intel Pentium 4 (3ГГц)

Параметры алгоритма и базовой МИМСС				Временные затраты на реализацию алгоритма (в нс)	
$\lceil \log_2 p \rceil$	l	k	M	в ПЭВМ	в МПК
64	5	10	$1{,}000183 \cdot 2^{132}$	295,46	62,8
128	9	18	$1{,}000427 \cdot 2^{260}$	668,98	78,8
256	17	34	$1{,}000916 \cdot 2^{516}$	1800,02	110,8
512	33	67	$1{,}001893 \cdot 2^{1028}$	5750,36	176,8
1024	66	133	$1{,}003910 \cdot 2^{2052}$	20183,9	308,8
2462	157	315	$1{,}009480 \cdot 2^{4928}$	105121,48	672,8