ТЕОРЕТИЧЕСКИЕ ОСНОВЫ ТЕХНОЛОГИЙ ПЕРЕДАЧИ И ОБРАБОТКИ ИНФОРМАЦИИ И СИГНАЛОВ

УДК 004.9, 004.94, 004.56

МОДУЛЯРНАЯ ИНТЕРПРЕТАЦИЯ СООБЩЕНИЙ В СИСТЕМАХ ЗАЩИТЫ ИНФОРМАЦИИ

Коляда А.А.[1], Протасеня С.Ю.[1], Червяков Н.И.[2]
[1]Белорусский государственный университет, Минск, Республика Беларусь
[2]Северо-Кавказский федеральный университет», Ставрополь, РФ
E-mail: chervyakov@yandex.ru, whbear@yandex.ru

В статье излагаются принципиальные основы технологии модулярной интерпретации сообщений в системах защиты информации (СЗИ). Предлагаемая технология позволяет свести к предельно низким уровням сложность и время выполнения базовых процедур позиционно-модулярного интерфейса СЗИ рассматриваемого класса. Синтезированные кодирующий и декодирующий алгоритмы ориентированы на реализацию двухкаскадной композиционной модификации модулярной интерпретации сообщений в рамках так называемой таблично-сумматорной вычислительной технологии.

Ключевые слова: модулярная система счисления, минимально избыточный модулярный код, позиционный код, кодовое преобразование, деление на двоичную экспоненту.

Введение

В современном процессе развития высокопроизводительных средств защиты информации, компьютерно-арифметической базой которых служит арифметика модулярных систем счисления (МСС) – модулярная арифметика (МА), ключевая роль отводится проблематике оптимизации применяемых немодульных операций [1-11]. В случае криптосистем, базирующихся на умножении Монтгомери, оптимизации подлежат главным образом операции расширения модулярного кода (МК) и процедуры кодовых преобразований (процедуры позиционно-модулярного интерфейса). Что касается расширения кода МСС и преобразования его в позиционный код (ПК), то эти операции в значительной мере удается оптимизировать в рамках избыточного кодирования, и в частности в рамках так называемого минимально избыточного модулярного кодирования [2-5; 12-14]. Среди других активно развиваемых оптимизационных направлений в современных криптографических МА-приложениях следует отметить направление, которое охватывает разработки по применению наборов модулей специального вида [6; 15-19], обеспечивающих упрощение как модульных, так и немодульных операций.

Роль кодовых преобразований в системах защиты информации (СЗИ) модулярного типа состоит прежде всего в согласовании принятой формы представления входных сообщений и результатов дешифрования данных с базовой конфигурацией МА. Традиционно для синтеза требуемых процедур позиционно-модулярного интерфейса СЗИ рассматриваемого класса применяется двоичное представление входной и выходной информации, то есть ее позиционная интерпретация [1]. Получение МК числа, отождествляемого в СЗИ с входным сообщением, и выполнение обратного (декодирующего) преобразования с привлечением промежуточных форм целых чисел (ЦЧ) сопряжено с высокой трудоемкостью итоговых алгоритмов. Вместе с тем сложность и время реализации кодовых преобразований в СЗИ на основе МА удается свести практически к предельно низким уровням в рамках так называемой модулярной интерпретации сообщений.

Предлагаемый альтернативный подход базируется на том, что составные элементы компонент или сами компоненты исходной формы записи входного сообщения по тому или иному правилу группируются в слова, которые рассматриваются (интерпретируются) как цифры МК по требуемому набору модулей ЦЧ, отождествляемого с заданным сообщением. Как нетрудно видеть, конкретная модификация отображения, ставящего в соответствие каждому сообщению единственное ЦЧ из диапазона МСС, принципиального значения не имеет.

В статье дана математическая формализация принципа модулярной интерпретации сообщений в СЗИ, сформулированы кодирующий и декодирующий алгоритмы, реализующие применяемый

принцип, а также приведены оценки эффективности предлагаемого подхода.

Минимально избыточное модулярное кодирование

Введем следующие обозначения:

- $\lfloor a \rfloor$ и $\lceil a \rceil$ – наибольшее и наименьшее ЦЧ, соответственно не большее и не меньшее вещественной величины a;
- $\mathbf{Z}_m = \{0, 1, \ldots, m-1\}$, $\mathbf{Z}_m^- = \{-\lfloor m/2 \rfloor, -\lfloor m/2 \rfloor + 1, \ldots \lceil m/2 \rceil - 1\}$ – множества наименьших неотрицательных и абсолютно наименьших вычетов по натуральному модулю m;
- $|A|_{\mathrm{m}}$ – элемент кольца $\mathbf{Z}_m$, сравнимый с A (в общем случае рациональным числом) по модулю m;
- $\mathrm{sn}(a)$ – знаковая функция вида

$$sn(a) = \begin{cases} 0, \text{если } a \geq 0; \\ 1, \text{если } a < 0; \end{cases}$$

- «<<b» и «>>b» – операции сдвига двоичного кода ЦЧ на b бит влево и вправо соответственно;
- $\{m_1, m_2, \ldots, m_{\mathrm{s}}\}$ – базис МСС, состоящий из $s>1$ попарно простых модулей.

В МСС с базисом $\{m_1, m_2, \ldots, m_{\mathrm{s}}\}$ ЦЧ X представляется кодом $(\chi_1, \chi_2, \ldots, \chi_s)(\chi_i = |X|_{m_i}; i = \overline{1,s})$. Максимальная мощность множества $\mathbf{D}_{\mathrm{МСС}}$ чисел X, на котором отображение $X \to (\chi_1, \chi_2, \ldots, \chi_s)$ взаимно однозначно составляет $M_s = \prod_{i=1}^{s} m_i$ элементов. В этом случае $\mathbf{D}_{\mathrm{МСС}}$ выполняет роль диапазона МСС. Обычно в качестве диапазона используют $\mathbf{Z}_{M_s}$ или $\mathbf{Z}_{M_s}^-$.

Из Китайской теоремы об остатках следует, что ЦЧ $X \in \mathbf{D}_{\mathrm{МСС}}$ может быть получено по своему МК $(\chi_1, \chi_2, \ldots, \chi_s)$ с помощью равенства

$$X = \sum_{i=1}^{s-1} M_{i,s-1} \left| M_{i,s-1}^{-1} \chi_i \right|_{m_i} + M_{s-1} I_s(X), \quad (1)$$

где $M_{i,s-1} = M_{s-1} / m_i$; $M_{s-1} = \prod_{j=1}^{s-1} m_j$; $I_s(X)$ – интервальный индекс (ИИ) числа X [20]. Выражение (1) называется интервально-модулярной формой ЦЧ X.

При $|\mathbf{D}_{\mathrm{МСС}}| = \mathrm{M_s}$ МСС с базисом $\{m_1, m_2, \ldots, m_{\mathrm{s}}\}$ является неизбыточной. Между тем использование в системах счисления кодовой избыточности, как правило, позволяет существенно улучшить их арифметические и иные свойства. Так называемое минимально избыточное модулярное кодирование: $\mathrm{D}_{\mathrm{МИМСС}} \to Z_{m_1} \times Z_{m_2} \times \ldots \ldots \times \mathbf{Z}_{m_s}$ предусматривает применение диапазона $\mathbf{D}_{\mathrm{МИМСС}}$, мощность которого меньше мощности диапазона $\mathbf{D}_{\mathrm{МСС}}$ неизбыточной (классической) МСС с базисом $\{m_1, m_2, \ldots, m_{\mathrm{s}}\}$. Сущность реализуемого принципа раскрывает нижеследующее утверждение.

Теорема 1 «О минимально избыточном модулярном кодировании». Для того, чтобы в МСС с попарно простыми основаниями $m_1, m_2, \ldots, m_{\mathrm{s}}$ ИИ $I_s(X)$ каждого элемента $X = (\chi_1, \chi_2, \ldots, \chi_s)$ диапазона $\mathbf{Z}_{2M}^- = \{-M, -M+1, \ldots M-1\}$ ($M = m_0 M_{s-1}$; m_0 – вспомогательный модуль) полностью определялся компьютерным ИИ - вычетом $\hat{I}_s(X) = \left| I(X) \right|_{m_s}$, необходимо и достаточно, чтобы s-ое основание удовлетворяло условию: $m_s \geq 2m_0 + s - 2$ ($m_0 \geq s - 2$). При этом для $I_s(X)$ верны расчетные соотношения:

$$I_s(X) = \begin{cases} \hat{I}_s(X), & \text{если } \hat{I}_s(X) < m_0, \\ \hat{I}_s(X) - m_s, & \text{если } \hat{I}_s(X) \geq m_0; \end{cases} \quad (2)$$

$$\hat{I}_s(X) = \left| \sum_{i=1}^{s} R_{i,s}(\chi_i) \right|_{m_s}; \quad (3)$$

$$R_{i,s}(\chi_i) = \left| -m_i^{-1} \left| M_{i,s-1}^{-1} \chi_i \right|_{m_i} \right|_{m_s} \quad (i \neq s), \quad \to .$$

$$\to R_{s,s}(\chi_s) = \left| M_{s-1}^{-} \chi_s \right|_{m_s}. \quad (4)$$

Переход от МСС с базисом $\{m_1, m_2, \ldots, m_{\mathrm{s}}\}$ и $\mathbf{Z}_{M_s}^-$ к минимально избыточной МСС (МИМСС) с тем же базисом и диапазоном $\mathbf{Z}_{2M}^-$ предельно упрощает вычисление базовой интегральной характеристики МК – ИИ $I_s(X)$: см. (2)-(4). Это приводит к адекватной оптимизации и немодульных процедур, базирующихся на интервально-модулярной форме (1).

Тривиальность процедуры расчета в МИМСС интервально-индексной характеристике дает также дополнительные возможности для упрощения реализации принципа модулярной интерпретации сообщений в СЗИ. Это достигается за счет использования наряду с минимально избыточным МК (МИМК) $(\chi_1, \chi_2, \ldots, \chi_s)$ и вспомогательного так называемого интервально-модулярного кода (ИМК), который для ЦЧ X определяется как набор вычетов: $(\chi_1, \chi_2, \ldots, \chi_{s-1}, \hat{I}_s(X))$. Для перехода от ИМК к МИМК достаточно воспользоваться равенством

$$\chi_s = \left| \sum_{i=1}^{s-1} \left| M_{i,s-1} \left| M_{i,s-1}^{-1} \chi_i \right|_{m_i} \right|_{m_s} + \left| M_{s-1} \hat{I}_s(X) \right|_{m_s} \right|_{m_s}, \quad (5)$$

вытекающим из (1-(3). Формирование ИМК ЦЧ X по его МИМК фактически сводится к вычислению характеристики $\hat{I}_s(\mathrm{X})$: см. (3)-(4).

Принцип модулярной интерпретации сообщений в криптосистеме RSA

Применение принципа модулярной интерпретации данных в системах защиты информации становится возможным благодаря присущему им свойству замкнутости относительно входных сообщений. В настоящей статье предлагаемый подход демонстрируется на примере криптосистемы RSA, базирующейся на операциях умножения и возведения в степень по большому модулю p, которые реализуются с использованием модифицированной минимально избыточной модулярной схемы Монтгомери в рамках таблично-сумматорной вычислительной технологии [2-5].

Как известно [21], для системы RSA с модулем p базовые криптографические преобразования имеют вид

$$Y = E_{\langle p,e\rangle}(X) = \left|X^e\right|_p,\ D_{\langle d\rangle}(Y) = \left|Y^d\right|_p, \qquad (6)$$

где $\langle p,e\rangle$ и $\langle d\rangle$ – соответственно, открытый и секретный ключи; e – элемент множества $\{2,3,...,\varphi(p)-1\}$, взаимно простой с $\varphi(p)$ ($\varphi(p)$ – функция Эйлера от p); $d = \left|e^{-1}\right|_{\varphi(p)}$; X – ЦЧ из диапазона $\mathbf{Z}_p$, отождествляемое с входным сообщением $\mathbf{X}$.

Из (6) вытекает равенство

$$D_{\langle d\rangle}(E_{\langle p,e\rangle}(\mathrm{X})) = X,\ (X \in \mathbf{Z}_p), \qquad (7)$$

в котором и заключается свойство замкнутости криптосистемы относительно входного сообщения. Обозначим последовательность битов, в совокупности образующих запись сообщения $\mathbf{X}$, через

$$\mathrm{X} = \{x_0, x_1, ..., x_{N-1}\};\quad \left(x_j \in \mathrm{Z}_2\ \left(j = \overline{0, N-1}\right);\ \ N \geq 1\right). \qquad (8)$$

Получение конкретного значения числа X, отождествляемого с сообщением $\mathbf{X}$, осуществляется согласно некоторому взаимно однозначному отображению, ставящему в соответствие каждой последовательности вида (8) слово (X_0, X_1, ... X_{n-1}) ($n < N$) из кодового пространства применяемой рабочей системы счисления. Иначе говоря, выбор базового правила присвоения значений аргументу X реализуемой целевой функции (см. (6), (7)): X = (X_0, X_1, ... X_{n-1}) ($X \in \mathbf{Z}_p$) предполагает определенную кодовую интерпретацию набора булевых величин (8), которая описывается тем или иным взаимно однозначным отображением вида:

$$\{x_0, x_1, ..., x_{N-1}\} \rightarrow (X_0, X_1, \ldots X_{n-1}). \qquad (9)$$

При любом таком отображении, не выводящем X=(X_0, X_1, …, X_{n-1}) за пределы диапазона $\mathbf{Z}_p$, свойство (7) криптосистемы в случае ее функционирования в системе счисления, отвечающей принятой кодовой интерпретации входных сообщений $\mathbf{X}$, сохраняется. Если преобразования (6) реализуются в позиционной системе счисления (ПСС) с основанием r>1, то последовательность (8) отображается в ПК $\left(X_{n-1}\, X_{n-2} \ldots X_0\right)_r$ $\left(X_j \in \mathbf{Z}_r\ \left(j = \overline{0, n-1}\right)\right)$. При этом

$$X = \sum_{j=0}^{n-1} X_j \cdot r^j\ (r^n < p). \qquad (10)$$

Модулярная интерпретация сообщения $\mathbf{X}$ предполагает объединение элементов последовательностей (8) в группы, которым отвечают числовые значения, принимаемые в качестве цифр МК (χ_1, χ_2 … χ_s) числа X по модулям m_1, m_2, … m_s.

Отметим, что выполнение условия $X \in \mathbf{Z}_p$ в рамках рассматриваемой кодовой интерпретации сообщения $\mathbf{X}$ на практике более просто обеспечивается при использовании композиции отображений

$$\mathbf{X} \rightarrow \left(\chi_1,\ \chi_2 \ldots \chi_{s-1},\ \hat{I}_s(X)\right) \text{ и}$$

$$\left(\chi_1,\ \chi_2 \ldots \chi_{s-1},\ \hat{I}_s(X)\right) \rightarrow \left(\chi_1,\ \chi_2 \ldots \chi_{s-1},\ \chi_s\right),$$

второе из которых реализуется с помощью (5). В этом случае декодирующее преобразование также должно иметь композиционную структуру:

$$\left(\chi_1,\ \chi_2 \ldots \chi_{s-1},\ \chi_s\right) \rightarrow$$

$$\rightarrow \left(\chi_1,\ \chi_2 \ldots \chi_{s-1},\ \hat{I}_s(X)\right) \rightarrow \mathrm{X},$$

требующую вычисления согласно (3)-(4) характеристики $\hat{I}_s(X)$. Обозначенный подход, в сущности, позволяет говорить об интервально-модулярной интерпретации сообщений, выполняющей роль вспомогательной стадии итоговой модулярной интерпретации.

Предположим, что входное сообщение **X** задано в виде последовательности **X** = $\{X_0, X_1, ..., X_{n-1}\}$, состоящей из n байтовых величин, и пусть модули базовой МСС являются 16-битовыми простыми ЦЧ из промежутка $(2^{15};2^{16}]$. Тогда для получения цифр МК (χ_1, χ_2, …, χ_s) числа X, отождествляемого с сообщением **X** при его модулярной интерпретации, можно воспользоваться величинами

$$x_i = \left(X_{2i-2}\, X_{2i-1}\right)_{256} \left(i = \overline{1, \lceil n/2 \rceil}\right), \qquad (11)$$

которые имеют разрядность 16 бит. Поскольку величины (11) могут выходить за пределы $\mathbf{Z}_{m_i}$, то использовать x_i в качестве цифр МК по модулям m_i непосредственно нельзя. В предлагаемом способе формирования требуемого МК в качестве базового применяется правило $\chi_i = (2^{15} - 1) \wedge x_i$, согласно которому в двоичном коде величины x_i старший бит замещается значением 0. При этом прежнее значение данного бита сохраняется в дополнительном слове соответствующего блока цифр, конструируемого МК. Каждый полный блок состоит из 16 слов. Вводя $(s+1)$-элементный массив **MC_X** для МК ЦЧ X с учетом изложенного реализуемое предложенным способом кодирование входного сообщения **X**, основополагающее правило запишем в виде:

$$\begin{cases} \mathrm{MC\_X}[i + \lfloor i/16 \rfloor] = (2^{15} - 1) \wedge x_i \ (i = \overline{1, \lceil n/2 \rceil}); \\ \mathrm{MC\_X}[16i] = \bigcap_{j=1}^{15} ((2^{15} \vee x_{15i+j-15}) >> \\ \qquad >> (16 - j)) \ (i = \overline{1, \lceil n/30 \rceil}); \\ \mathrm{MC\_X}[16\lfloor n/30 \rfloor + \lfloor n/2 \rfloor_{15} + 1] = v = \\ \qquad = \bigcap_{j=1}^{\lfloor \lfloor n/2 \rfloor \rfloor_{15}} ((2^{15} \bigcup x_{15\lfloor n/30 \rfloor + j}) >> \\ \qquad >> (16 - j)); \text{при четном } n \text{ и } \lfloor \lfloor n/2 \rfloor \rfloor_{15} \neq 0; \\ \mathrm{MC\_X}[16\lfloor n/30 \rfloor + \lfloor n/2 \rfloor_{15} + 1] = (v << 8) + X_{n-1}, \\ \qquad \text{если } n \text{ нечетно и } \lfloor \lfloor n/2 \rfloor \rfloor_{15} < 8; \\ \mathrm{MC\_X}[16\lfloor n/30 \rfloor + \lfloor n/2 \rfloor_{15} + 1] = X_{n-1}, \\ \qquad \text{если } n \text{ нечетно и } \lfloor \lfloor n/2 \rfloor \rfloor_{15} > 7; \\ \mathrm{MC\_X}[16\lfloor n/30 \rfloor + \lfloor n/2 \rfloor_{15} + 2] = v \\ \qquad \text{в случае нечетного } n \text{ и } \lfloor \lfloor n/2 \rfloor \rfloor_{15} > 7. \end{cases} \qquad (12)$$

Количество цифр конструируемого МК, формируемых согласно (12), составляет

$$\tilde{s} = \lceil n/2 \rceil + \lfloor n/30 \rfloor + (1 - |n|_2) \cdot \mathrm{sn}(-\lfloor n/2 \rfloor_{15}) + \\ + |n|_2 \cdot \mathrm{sn}(7 - \lfloor \lfloor n/2 \rfloor \rfloor_{15}). \qquad (13)$$

Отметим, что в процессе кодирования входного сообщения **X** в массив **MC_X** в качестве нулевого элемента записывается длина сообщения (**MC_X**[0] = n), а остальные элементы, не охваченные правилом (12), обнуляются (**MC_X**[i] = 0 ($i = \overline{\tilde{s}+1, s}$)). Таким образом, получаемый в соответствии с (12) на вспомогательной стадии кодирования сообщения **X** ИМК имеет вид:

$$(\chi_1, \chi_2 \ldots, \chi_{\tilde{s}}, \chi_{\tilde{s}+1}, \ldots, \chi_{s-1}, \hat{I}_s(X)) = \\ = (\chi_1, \chi_2 \ldots \chi_{\tilde{s}}, 0, \ldots, 0, 0). \qquad (14)$$

Следовательно, искомый результат модулярной интерпретации X представляет собой МК

$$(\chi_1, \chi_2, \ldots, \chi_{\tilde{s}}, \chi_{\tilde{s}+1}, \ldots, \chi_{s-1}, \chi_s) = \\ = (\chi_1, \chi_2, \ldots, \chi_{\tilde{s}}, 0, \ldots, 0, \chi_s). \qquad (15)$$

С учетом (5) и (14) цифра χ_s кода (15) определяется по расчетному соотношению

$$\chi_s = \left| \sum_{i=1}^{\tilde{s}} \left| M_{i,s-1} \left| M_{i,s-1}^{-1} \chi_i \right|_{m_i} \right|_{m_s} \right|_{m_s}. \qquad (16)$$

Из (1) и (14) для ЦЧ X, отождествляемого с **X** при рассматриваемой модулярной интерпретации, вытекает равенство

$$X = \sum_{i=1}^{\tilde{s}} M_{i,s-1} \left| M_{i,s-1}^{-1} \chi_i \right|_{m_i} = \sum_{i=1}^{\tilde{s}} M_{i,s-1} \chi_{i,s-1} \\ \left(\chi_{i,s-1} = \left| M_{i,s-1}^{-1} \chi_i \right|_{m_i}\right). \qquad (17)$$

Найдем верхний ограничительный порог $X_{\text{ВП}}$ для числа вида (17). Из (17) имеем:

$$X \le \sum_{i=1}^{\tilde{s}} M_{i,s-1}(m_i - 1) = \sum_{i=1}^{\tilde{s}} M_{s-1} \frac{m_i - 1}{m_i} = \\ = M_{s-1}(\tilde{s} - \sum_{i=1}^{\tilde{s}} \frac{1}{m_i}) < M_{s-1}(\tilde{s} - \sum_{i=1}^{\tilde{s}} \frac{1}{m_{\tilde{s}}}) < \\ < M_{s-1}(\tilde{s} - \left\lfloor \frac{\tilde{s}}{m_{\tilde{s}}} \right\rfloor) = X_{ВП}. \qquad (18)$$

В применяемых базисах МСС основания упорядочиваются по возрастанию – поэтому из (18) следует, что $X_{ВП} = \tilde{s} \cdot M_{s-1}$.

Изложенное позволяет сформулировать следующее утверждение.

Теорема 2. Если модуль p, базис $\{m_1, m_2, \ldots, m_s\}$ применяемой МИМСС, параметры s, $\tilde{s}$, а также длина n (в байтах) сообщений (см. (9), (13), (18)) удовлетворяют условиям:

$$\begin{cases} X_{ВП} = \widetilde{s} \cdot M_{s-1} < p < m_0 \cdot M_{s-1} = M, \\ \widetilde{s} = \lceil n/2 \rceil + \lfloor n/30 \rfloor + (1 - |n|_2) \cdot \mathrm{sn}(-|n/2|_{15}) + \\ \quad + |n|_2 \cdot \mathrm{sn}(7 - \lfloor n/2 \rfloor_{15}) < s, \end{cases} \quad (19)$$

то двухкаскадная композиционная конфигурация модулярной интерпретации сообщений в криптосистеме RSA с модулем p, базирующаяся на схеме (12), корректна, то есть является реализуемой. Отметим, что первое условие в (19) можно ослабить, если в (12) цифры χ_i МК заменить на их нормированные аналоги $\chi_{i,\ s\text{-}1}$ (см. (17)). В этом случае (17) дает:

$$X = \sum_{i=1}^{\widetilde{s}} M_{i,s-1}\chi_{i,s-1} \le \sum_{i=1}^{\widetilde{s}} M_{i,s-1}(2^{15}-1) =$$
$$= (2^{15}-1)M_{s-1}\sum_{i=1}^{\widetilde{s}}\frac{1}{m_i} < (2^{15}-1)M_{s-1}\sum_{i=1}^{\widetilde{s}}\frac{1}{m_1} = \quad (20)$$
$$= (2^{15}-1)\widetilde{s}\,\frac{M_{s-1}}{m_1}.$$

В сравнении с (19) оценка (20) дает существенно большую свободу для выбора p. Вместе с тем указанная альтернативная модификация модулярной интерпретации сообщений требует дополнительных реализационных затрат на получение цифр МК (15) согласно формуле $\chi_i = \left|M_{i,s-1}\cdot\chi_{i,s-1}\right|_{m_i}$ $(i = \overline{1,\widetilde{s}})$. Что касается цифры χ_s МК (15), то ее вычисление в сравнении с (16) упрощается:

$$\chi_s = \left|\sum_{i=1}^{\widetilde{s}}\left|M_{i,s-1}\cdot\chi_{i,s-1}\right|_{m_s}\right|_{m_s}.$$

Алгоритмическое обеспечение модулярной интерпретации сообщений в СЗИ

На базе изложенных положений разработанной технологии модулярной интерпретации данных в криптосистемах RSA на основе МА синтезированы алгоритмы кодирования и декодирования сообщений. Для определенности предполагается, что сообщения задаются в виде байтовых последовательностей.

Алгоритм кодирования сообщений. Параметры алгоритма удовлетворяют условиям (19) теоремы 2, модуль p криптосистемы, основания $m_1, m_2, \ldots m_s$ применяемой МИМСС ($m_i \in (2^{15}; 2^{16}]$ $(i = \overline{1,s})$) и длина n сообщений (в байтах).

Входные данные: Сообщение $\mathbf{X} = \{X_0, X_1 \ldots X_{n-1}\}$ объемом n байтов, расположенное в массиве с идентификатором M_X ($\mathbf{M\_X}[j]=X_j$ $(j = \overline{0,n-1})$).

Выходные данные: МК $(\chi_1, \chi_2, \ldots, \chi_s) = (\chi_1, \chi_2, \ldots \chi_{\widetilde{s}}, 0, \ldots, 0, \chi_s)$ $(\widetilde{s} < s)$ отождествляемого с входным сообщением $\mathbf{X}$ числа X ($X \in \mathbf{Z}p$), который наряду с n помещается в $(s+1)$-элементный массив **MC_X** ($\mathbf{MC\_X}[0] = n$, $\mathbf{MC\_X}[i] = \chi_i$ $(i = \overline{1,s})$.

Тело алгоритма кодирования модулярно интерпретируемого сообщения

К_МИ.1. Инициализировать параметры и константы кодового преобразования; определить параметры и константы преобразования:

- число полных 16-битовых слов в сообщении – N_W $= \lfloor n/2 \rfloor = n >> 1$ (символом « >> b» обозначается операция сдвига целого число (ЦЧ) вправо на b бит);
- количество 16-элементных блоков из цифр формируемого МК, отвечающих 16-битовым словам сообщения, - N_B $= \lfloor N\_W/15 \rfloor$;
- количество оставшихся не вошедших в полные блоки 16-битовых слов – R_W$= |N_W|_{15}$;
- BExp_7 = 2^7, Mask_7 = BExp-1.

К_МИ.2. Активизировать $(s+1)$-элементный массив **MC X** для выходного МК, положив $\mathbf{MC\_X}[0] = n$, $\mathbf{MC\_X}[i] = 0$ $(i = \overline{1,s})$.

К_МИ.3. Переменным цикла j и i по компонентам входного сообщения и выходного кода, а также счетчику C_B блоков цифр МК присвоить начальные значения: $j = 0$, $i = 1$, C_B = 1.

К_МИ.4. Обнулить порядковый номер слова в блоке: $u = 0$ и положить $v = 0$, BExp = 1.

К_МИ.5. Получить очередное цифру МК текущего блока, реализуя операционную последовательность:

К_МИ.5.А. Из массива **M_X** извлечь j-ый элемент, полагая $w = \mathbf{M\_X}[j] = X_j$.

К_МИ.5.Б. Если BExp_7 $\wedge\, w \neq 0$, то положить $v = v \vee$ BExp, $w = w \wedge$ Mask_7.

К_МИ.5.В. Выполнить операции: $w = w << 8$, $\mathbf{MC\_X}[i] = w + \mathbf{M\_X}[j+1] = w + X_{j+1}$, $i = i + 1$, $j = j + 2$.

К_МИ.6. Если $u \neq 14$, то u инкрементировать $(u = u + 1)$, переменную BExp сдвинуть на один бит влево и перейти к К_МИ.5. По достижении равенства $u = 14$ в массив **MC_X** записать очередную цифру: $\mathbf{MC\_X}[i] = v$, после чего i инкрементировать ($i = i + 1$).

К_МИ.7. При C_B ≠ N_B счетчик блоков увеличить на 1 (C_B = C_B+1) и перейти к К_МИ.4.

Получить цифры МК заключительного (неполного) блока

К_МИ.8. Если R_W = 0 и n четно, то перейти к К_МИ.16. Если же R_W = 0, но n нечетно, то выполнить операцию присвоения **MC_X** [i] = **M_X**[n – 1] = X_{n-1} и перейти к К_МИ.16.

К_МИ.9. Положить: $u = 0$, $v = 0$, BExp = 1.

К_МИ.10. Получить очередную цифру МК заключительного блока, реализуя операционную последовательность:

К_МИ.10.А. Переменной w присвоить значение w = **M_X**[j] = X_j.

К_МИ.10.Б. При BExp_7 $\wedge\, w \neq 0$ положить $v = v \vee$ BExp, $w = w \wedge$ Mask_7.

К_МИ.10.В. Выполнить операции: $w = w <<$ 8, **MC_X** [i] = w + **M_X**[j + 1] = $w + X_{j+1}$, $i = i + 1, j = j + 2$.

К_МИ.11. Если $u \neq$ R_W, то u увеличить на 1 ($u = u + 1$), переменную BExp сдвинуть на один бит влево и перейти к К_МИ.10.

К_МИ.12. При четном n в массив **MC_X** записать последнюю цифру блока: **MC_X** [i] = v и перейти к К_МИ.16.

К_МИ.13. Выполнить операцию присвоения w = **M_X**[j] = X_j .

К_МИ.14. Если $u < 8$, то положить **MC_X** [i] = ($v <<$ 8) + w и перейти к К_МИ.16.

К_МИ.15. В случае, когда $u \geq 8$, в массив **MC_X** поместить две последние цифры МК заключительного блока: **MC_X** [i] = w, **MC_X** [i + 1] = v.

К_МИ.16. Используя (4) и (16), рассчитать s-ю цифру искомого МК согласно правилу

$$\mathrm{MC\_X[s]} = \left| -\,\mathrm{M_{s-1}}\big|_{m_s} \left| \sum_{i=1}^{s-1} R_{i,s}(\chi_i) \right|_{m_s} \right|_{m_s} \quad (\chi_i = \mathbf{MC\_X}[i])$$

и завершить работу алгоритма.

Алгоритм декодирования сообщений

Параметры алгоритма: удовлетворяющие условиям (19) теоремы 2 модуль p криптосистемы, основания $m_1, m_2 \ \ldots\ m_s$ применяемой МИМСС ($m_i \in (2^{15}; 2^{16}]$ ($i = \overline{1,s}$)) и длина n сообщений (в байтах).

Входные данные: подлежащий декодирующему преобразованию МК ($\chi_1, \chi_2 \ldots \chi_s$) некоторого ЦЧ $X \in \mathbf{Z}_p$, расположенный в (s + 1)-элементном массиве с идентификатором **MC_X** (**MC_X**[0] = n, **MC_X**[i] = χ_i ($i = \overline{1,s}$)).

Выходные данные: отождествляемое с числом X сообщение $\mathbf{X} = \{X_0, X_1 \ldots X_{n-1}\}$, элементы которого помещаются в массив с идентификатором **N_X**.

Тело алгоритма декодирования модулярно интерпретируемого сообщения

Д_МИ.1. Инициализировать параметры и константы декодирующего преобразования:

- длина (в байтах) формируемого сообщения – n = **MC_X**[0];
- число 16-битовых слов вида (11) в сообщении **X** – N_W = $\lfloor n/2 \rfloor = n >> 1$;
- количество полных (16-элементных) блоков из цифр МК, отвечающих 16-битовым словам вида (1), – N_B = $\lfloor N\_W/15 \rfloor = \lfloor n/30 \rfloor$;
- число цифр МК, отвечающих словам вида (11) в неполном блоке – R_W = $|N\_W|_{15}$;
- BExp_15 = 2^{15}, Mask_8 = $2^8 - 1$.

Д_МИ.2. Следуя (3)-(4), вычислить интервально-индексную характеристику

$$\hat{I}_s(X) = \left| \sum_{i=1}^{s} R_{i,s}(\chi_i) \right|_{m_s} \quad (\chi_i = \mathbf{MC\_X}[i]).$$

Д_МИ.3. В случае нарушения равенства **MC_X**[$\tilde{s}$ + 1] = **MC_X**[$\tilde{s}$ + 2] =…= **MC_X**[**s** – 1] = $\hat{I}_s(X) = 0$ (см. (19)) завершить работу алгоритма по причине фиксации ошибки в ИМК (χ_1, $\chi_2 \ldots \chi_{s-1}$, $\hat{I}_s(X)$).

Д_МИ.4. Активизировать n-байтовый массив **M_X** для формируемого сообщения.

Д_МИ.5. Переменным i и j цикла по элементам массивов **MC_X** и M_**X**, а также счетчику C_B_4 блоков цифр МК и параметров N_B_4 присвоить значения: $i = 1$, $j = 0$, C_B_4 = 16, N_B_4 = 16·N_B = N_B << 4.

Д_МИ.6. Положить v = **MC_X**[C_B_4].

Д_МИ.7. Получить очередную пару символов (байтов) сообщения, отвечающую паре одноименной цифре МК текущего блока, выполняя операционную последовательность:

Д_МИ.7А. Из массива **MC_X** извлечь очередную цифру МК: w = **MC_X**[i].

Д_МИ.7Б. При $1 \wedge v \neq 0$ осуществить коррекцию слова w согласно правилу $w = w \vee$BExp_15.

Д_МИ.7В. В массив **M_X** поместить пару компонент сообщения: **M_X**[j + 1] = Mask_8$\wedge w$, M_**X**[j] = w >>8.

Д_МИ.7Г. Положить $v = v >> 1$, $i = i + 1$, $j = j$+2.

Д_МИ.8. Если $i \neq$ C_B_4, то перейти к Д_МИ.7.

Д_МИ.9. Инкрементировать переменную i ($i = i + 1$), согласовав тем самым ее значение с переходом к очередному блоку цифр МК.

Д_МИ.10. При C_B_4≠N_B_4 увеличить C_B_4 на 16 (C_B_4 = C_B_4 + 16) и перейти к Д_МИ.6.

Получить компоненты сообщения, отвечающие заключительному (неполному) блоку цифр МК

Д_МИ.11. Если R_W = 0 и n четно, то завершить работу алгоритма. Если же R_W = 0, но n нечетно, то выполнить операцию $\mathbf{M\_X}[n-1] = \mathbf{MC\_X}[i]$ и завершить работу алгоритма.

Д_МИ.12. Положить: $u = i + \mathrm{R\_W}$.

Д_МИ.13. В случае четного n переменной v присвоить значение $v = \mathbf{MC\_X}[u]$.

Д_МИ.14. При нечетном n положить $\mathrm{M\_X}[n-1] = \mathrm{Mask\_8} \vee \mathbf{MC\_X}[u]$. Кроме того, если R_W < 8, то выполнить операцию $v = \mathbf{MC\_X}[u] >> 8$, если же R_W > 7, то – операцию $v = \mathbf{MC\_X}[u+1]$.

Д_МИ.15. Сформировать пару компонент сообщения, отвечающую текущей цифре МК заключительного блока, реализуя операционную последовательность:

Д_МИ.15А. Из массива **MC_X** извлечь очередную цифру МК: $w = \mathbf{MC\_X}[i]$.

Д_МИ.15Б. При $1 \wedge v \neq 0$ осуществить коррекцию слова w по правилу $w = w \vee \mathrm{BExp\_15}$.

Д_МИ.15В. В массив M_X поместить искомую пару компонент сообщения: $\mathrm{M\_X}[j+1] = \mathrm{Mask\_8} \wedge w$, $\mathrm{M\_X}[j] = w >> 8$.

Д_МИ.15Г. Положить $v = v >> 1$, $i = i + 1$, $j = j + 2$.

Д_МИ.16. Если $i \neq u$, то перейти к Д_МИ.15. По достижении равенства $i = u$ завершить работу алгоритма.

Приведенные алгоритмы кодирования и декодирования сообщений в СЗИ отличаются простотой и высоким быстродействием. Это обусловлено тем, что их реализация практически требует лишь логических операций и операций присвоения. Для традиционно применяемых кодирующих и декодирующих процедур, основанных на позиционной интерпретации сообщений [14; 22] согласно формуле вида (10), необходимые временные затраты составляют величину порядка $O(sn)$ модульных операций.

Заключение

Основные результаты представленной разработки по проблематике оптимизации средств позиционно-модулярного интерфейса СЗИ, компьютерно-арифметической базой которых служит МА, кратко можно охарактеризовать следующим образом.

1. Проведена математическая формализация принципа модулярной интерпретации сообщений для криптосистем RSA, функционирующих в МСС. В частности, описано базовое взаимно однозначное отображение множества сообщений на кодовое пространство используемой МСС и для построенного отображения получены достаточные условия корректности – реализуемости в рамках таблично-сумматорной вычислительной технологии.

2. Показано, что по критерию простоты выполнения требования принадлежности чисел, отождествляемых с соответствующими сообщениями, к рабочему диапазону криптосистемы оптимальной конфигурацией модулярной интерпретации данных является двухкаскадная композиционная конфигурация, которая порождается парой отображений – интервально-модулярным и модулярным. Это обеспечивается тривиальностью процедур перехода ИМК к МК и МК к ИМК.

3. Синтезированы эффективные кодирующий и декодирующий алгоритмы, реализующие композиционную модификацию принципа модулярной интерпретации сообщений в СЗИ. Предложенные алгоритмы включают лишь логические операции и операции присвоения, вследствие чего они отличаются простотой и высоким быстродействием. В рамках традиционной позиционной интерпретации сообщений в СЗИ модулярного типа прямое и обратное кодовые преобразования занимают время порядка O(sn) модульных операций каждое.

Литература

1. Kawamura S. Cox-Rower architecture for fast parallel Montgomery multiplication // Eurocrypt 2000, LNCS. Vol. 1807. Berlin, 2000. – P. 523-538.
2. Каленик А.Н. Умножение и возведение в степень по большим модулям с использованием минимально избыточной модулярной арифметики // Информационные технологии. 2012. № 4. – С. 37-44.
3. Каленик А.Н., Коляда А.А., Коляда Н.А., Протько Т.Г., Шабинская Е.В. Компьютерно-арифметическая и реализационная база быстрых процедур умножения по большим модулям на основе модифицированной модулярной схемы Монтгомери // Электроника инфо. №7, 29012. – С. 114-118.
4. Коляда А.А., Чернявский А.Ф., Шабинская Е.В. Генерирование и функционально-структурная оптимизация базового комплекта таблиц для

мультипликативной МИМА-схемы Монтгомери // Электроника инфо. № 4, 2013. – С. 35-41.
5. Коляда А.А., Коляда Н.А., Мазуренко П.А., Чернявский А.Ф., Шабинская Е.В. Табличносумматорная алгоритмизация минимально избыточной модулярной схемы Монтгомери для умножения по большим модулям // Наука и военная безопасность. №3, 2013. – С. 40-45.
6. Pettenghe H., Chaves R., Sousa L. Method to design general RNS reverse converters for extended moduli sets // IEEE Trans. Circuits and Syst. II: Express briefs, 2013. Vol. 60. Issue 12. – P. 877-881.
7. Лавриненко А.Н., Червяков Н.И. Округление чисел по модулю поля эллиптической кривой при выполнении криптографических преобразований в системе остаточных классов // ИКТ. Т.12, №2, 2014. – С. 4-7.
8. Wu Tao, Lee Shoguo, Leu Litian. Improved RNS Montgomery modular multiplication with residue recovery // Proc. Int. Conf. on soft computing techniques and engeneering aplication advances in intelligent systems and computing. 2014. Vol. 250, 2014. – P. 233-245.
9. Bigou K., Tisserand A. RNS modular multiplication through reduced base extentions // 25 Int. Conf. IEEE «Application specific systems, architectures and processors» (ASSAP 2014). Zurich, Switzerland, June, 2014. – P. 57-62.
10. Червяков Н.И., Дерябин М.А., Лавриненко И.Н. Реализация алгоритма Монтгомери в системе остаточных классов на базе эффективного алгоритма расширения системы оснований // Нейрокомпьютеры: разработка, применение. №9, 2014. – С. 37-45.
11. Saeedeh J., Molahosseini A.S. Towardes fast Implementation of fully homomorphic Encryption an RNS Approach // Материалы I МНК «Параллельная компьютерная алгебра и ее приложения в новых инфокоммуникационных системах». Ставрополь, октябрь, 2014. – С. 197 - 205.
12. Чернявский А.Ф., Коляда А.А., Коляда Н.А. и др. Интервально-индексная технология расширения модулярного кода // Электроника инфо. №6, 2010. – С. С. 66-71.
13. Коляда А.А., Кучинский П.В., Чернявский А.Ф. Интервально-индексная технология синтеза параллельных алгоритмов модулярно-позиционного кодового преобразования с табличносумматорной конфигурацией // Нейрокомпьютеры: разработка, применение. №9, 2014. – С. 46-51.
14. Коляда А.А., Кучинский П.В., Червяков Н.И., Чернявский А.Ф., Шабинская Е.В. Метод деления на двоичную экспоненту для преобразования минимально избыточного модулярного кода в позиционный код // ИКТ. Т.12, №3, 2014. – С. 4-10.
15. Esmaeildoust M., Navi K., Taheri M., Molahosseini A.S., Khodabashi S. Efficient RNS to binary converters for the new 4-module set $\left\{2^{2n}-1,\ 2^{2n+1}-1,\ 2^{2n}-1,\ 2^{n-1}-1\right\}$ // IEICE Electronics Express. Vol. 9, Issue 1, 2012. – P. 1-7.
16. Zarandi A.A.E., Molahosseini A.S., Mehdi H. Modern Resedue Number System Moduli Sets: Effecienty VS. Complexety // Нейрокомпьютеры: разработка, применение. №9, 2014. – С. 9-12.
17. Jaberipur G., Ahmadifar H. Are ROM–less revers RNS Converter for Moduli set $\left\{2^{q},\ 2^{q}\right\}$ // Computer and Didgital Techniques. IET, Vol. 8, Issue 1, 2014. – P. 11-22.
18. Ciewobr H., Gbolagade K.A. Modulo Operation Free Reverse Convertion in the $\left\{2^{2n+1}-1,\ 2^{2n},\ 2^{2n}-1\right\}$ Moduli Set // Int. J. of Computer Applications. Vol. 85, Issue 1, 2014. – P. 11-14.
19. Noorimehr M.R., Hosseinzadeh M., Farshidi R. High Speed Recidue to Binary Converter for the new Four-moduli set $\left\{2^{2n},\ 2^{2n}+1,\ 2^{n/2}+1,\ 2^{n/2}-1\right\}$ // Arabian J. for Science and Eng. Vol. 39, Issue 4, 2014. – P. 2887-2893.
20. Коляда А.А., Пак И.Т. Модулярные структуры конвейерной обработки цифровой информации. Минск: Университетское, 1992. – 256 с.
21. Харин Ю.С., Берник В.И., Матвеев Г.В. и др. Математические и компьютерные основы криптологии. Минск: Новое знание, 2003. – 382 с.
22. Городецкий Д.А., Коляда А.А., Коляда Н.А., Шабинская Е.В. Применение таблично-сумматорной вычислительной технологии для позиционно-модулярного кодового преобразования по схеме Горнера // Материалы I МНК «Параллельная компьютерная алгебра и ее приложения в новых инфокоммуникационных системах». Ставрополь, октябрь, 2014. – С. 247-252.

Получено 02.06.2015

Коляда Андрей Алексеевич, д.ф.-м.н., доцент, гл.н.с. НИИ Прикладных физических проблем (ПФП) им. А.Н. Севченко Белорусского государственного университета (БГУ). Тел. 8-10-375-17-212-47-45; 8-10-375-17-271-96-09. E-mail: razan@tut.by

Протасеня Стелла Юрьевна, м.н.с. НИИ ПФП им. А.Н. Севченко БГУ. Тел. 8-10-375-17-212-47-45. E-mail: estellita@mail.ru

Червяков Николай Иванович, д.т.н., профессор, заслуженный деятель науки и техники РФ, заведующий Кафедрой прикладной математики и математического моделирования Северо-Кавказского федерального университета. Тел. (8-865) 275-35-64. E-mail: chervyakov@yandex.ru, whbear@yandex.ru

MESSAGE MODULAR INTERPRETATION FOR INFORMATION PROTECTION SYSTEMS

Kolyada A.A.[1], Protasenia S.U.[1], Chervyakov N.I.[2]
[1]Belarusian State University, Minsk, Belarus
[2]North-Caucasus Federal University, Stavropol, Russian Federation
E-mail: whbear@yandex.ru

Fundamental principles of modular technology interpretation posts in information protection systems (IPS) are presented in the article. The computer arithmetic base of these technologies is the modular arithmetic (MA). In particular, given the mathematical formalization of the principle of the modular massages' interpretation, as well as the necessary and sufficient conditions for its feasibility by a two-stage scheme of composition within the table-summatory computing MA-structure. The proposed technology allows to minimize difficulty and the execution time of the basic procedures of a position-modular IPS interface of this class. The coding and decoding algorithms that contain only logic and assignment operation are synthesized. In the traditional positional interpretation of data in IPS of modular type the forward and reverse code conversion takes time O (ns) modular operations each (n – length of position code of messages, and s- length of modular code of messages).

Keywords: *modular number system, minimal redundant modular code, position code, code conversion, binary exponent division*

DOI: 10.18469/ikt.2015.13.3.01

Kolyada Andrey Alekseevich, Doctor of Physico-Mathematical Science, chief researcher of the Research Institute of Applied Physical Problems n.a. AN Sevchenko, Belarusian State University, Minsk, Belarus. Tel.: +375292553584. E-mail: razan@tut.by

Protasenia Stella Jurjevna, junior researcher of the Research Institute of Applied Physical Problems n.a. AN Sevchenko, Belarusian State University, Minsk, Belarus. Tel.: +375172124745. E-mail: estellita@mail.ru.

Chervyakov Nikolay Ivanovich, Doctor of Technical Science, Professor, the Head of Department of Applied Mathematics and Mathematical Modeling, North-Caucasus Federal University, Stavropol, Russian Federation. Tel.: +78652354861. E-mail: k-fmf-primath@stavsu.ru.

References

1. Kawamura S. Cox-Rower architecture for fast parallel Montgomery multiplication. Eurocrypt 2000, LNCS, vol. 1807, pp. 523-538. doi: 10.1007/3-540-45539-6_37
2. Kalenik A.N. Umnozhenie i vozvedenie v stepen' po bol'shim moduljam s ispol'zovaniem minimal'no izbytochnoj moduljarnoj arifmetiki [Multiplication and exponentiation on a large modules with application the minimally redundant modular arithmetic]. *Informacionnye tehnologii*, 2012, no 4, pp. 37-44.
3. Kalenik A.N., Kolyada A.A., Kolyada N.A., Protko T.G., Shabinskaya E.V. Komp'juterno-arifmeticheskaja i realizacionnaja baza bystryh procedur umnozhenija po bol'shim moduljam na osnove modificirovannoj moduljarnoj shemy Montgomeri [Computer-arithmetical and realizable base of fast procedures of multiplying large modules on the basis of a modified modular scheme of Montgomery]. *Jelektronika info*, 2012, no 7, pp. 114-118.
4. Kolyada A.A., Chernyavsky A.F., Shabinskaya E.V. Generirovanie i funkcional'no-strukturnaja optimizacija bazovogo komplekta tablic dlja mul'tiplikativnoj MIMA–shemy Montgomeri [Generation and functional

- structural optimization of a basic set of tables for the multiplicative MIMA-scheme of Montgomery]. *Jelektronika info*, 2013, no 4, pp. 35-41.
5. Kolyada A.A., Kolyada N.A., Mazurenko P.A., Chernyavsky A.F., Shabinskaya E.V. Tablichno-summatornaja algoritmizacija minimal'no izbytochnoj moduljarnoj shemy Montgomeri dlja umnozhenija po bol'shim moduljam [Table-summation algorithmization minimally redundant modular circuit for Montgomery multiplication of large modules]. *Nauka i voennaja bezopasnost'*, 2013, no. 3, pp. 40-45.
6. Pettenghe H., Chaves R., Sousa L. Method to design general RNS reverse converters for extended moduli sets. *IEEE trans. circuits and syst. II: Express briefs*, 2013, vol. 60, no. 12, pp. 877-881. doi: 10.1109/TCSII.2013.2286433
7. Lavrienko A.N., Chervyakov N.I. Okruglenie chisel po modulju polja jellipticheskoj krivoj pri vypolnenii kriptograficheskih preobrazovanij v sisteme ostatochnyh klassov [Rounding of modular representations in the elliptic curve field for cryptography applications in residue number system]. *Infokommunikacionnye tehnologii*, 2014, vol. 12, no. 2, pp. 4-7.
8. Wu Tao, Lee Shoguo, Leu Litian. Improved RNS Montgomery modular multiplication with residue recovery. *Proc. Int. Conf. on soft computing techniques and engeneering aplication advances in intelligent systems and computing*, 2014, vol. 250, pp. 233-245. doi: 10.1007/978-81-322-1695-7_27
9. Bigou K., Tisserand A. RNS modular multiplication through reduced base extentions. *25 Int. Conf. «Application specific systems, architectures and processors (ASSAP 2014)»*, Zurich, Switzerland, 18 – 20 june, 2014, IEEE, pp. 57 – 62. doi: 10.1109/ASAP.2014.6868631
10. Chervyakov N.I., Deriabin M.A., Lavrienko I.N. Realizacija algoritma Montgomeri v sisteme ostatochnyh klassov na baze jeffektivnogo algoritma rasshirenija sistemy osnovanij [Montgomery algorithm realization based on efficient algorithm of modular base extension in residue number system]. *Nejrokomp'jutery: razrab., primenenie*, 2014, no. 9, pp. 37-45.
11. Saeedeh J., Molahosseini A.S. Towardes fast Implementation of fully homomorphic Encryption an RNS Approach. *Proc. of the 1st International Conference «Parallel algebra and its applications in novel information systems»*. Stavropol, Russia, October 20-24, 2014, pp. 197 - 205.
12. Chernyavsky A.F., Kolyada A.A., Kolyada N.A. and etc. Interval'no-indeksnaja tehnologija rasshirenija moduljarnogo koda [Interval and index technology of expansion of a modular code]. *Jelektronika info*, 2010, no. 6, pp. 66-71.
13. Kolyada A.A., Kuchynski P.V., Chernyavsky A.F. Interval'no-indeksnaja tehnologija sinteza parallel'nyh algoritmov moduljarno- pozicionnogo kodovogo preobrazovanija s tablichno-summatornoj konfiguraciej [The interval-index technology of the synthesis of parallel modular-positional conversion algorithms using table-summatory configuration]. *Nejrokomp'jutery: razrab., primenenie*, 2014, no. 9, pp. 46-51.
14. Kolyada A.A., Kuchynski P.V., Chervyakov N.I., Chernyavsky A.F., Shabinskaya E.V. Metod delenija na dvoichnuju jeksponentu dlja preobrazovanija minimal'no izbytochnogo moduljarnogo koda v pozicionnyj kod [Binary exponent division method for conversion of the minimally redundant modular code to the positional code]. *Infokommunikacionnye tehnologii*, 2014, vol. 12, no. 3, pp. 4-10.
15. Esmaeildoust M., Navi K., Taheri M., Molahosseini A.S., Khodabashi S. Efficient RNS to binary converters for the new 4-module set $\left\{2^{2n}-1,\ 2^{2n+1}-1,\ 2^{2n}-1,\ 2^{n-1}-1\right\}$. *IEICE Elec-tronics Express*, 2012, vol. 9, Issue 1, pp. 1 – 7.
16. Zarandi A.A.E., Molahosseini A.S., Mehdi H. Modern Resedue Number System Moduli Sets: Effecienty VS. Complexety. *Nejrokomp'jutery: razrab., primenenie*, 2014, pp. 9-12.
17. Jaberipur G., Ahmadifar H. Are ROM–less revers RNS Converter for Moduli set $\left\{2^{q},\ 2^{q}\right\}$. Computer *and Digital Techniques, IET*, 2014, vol. 8, no. 1, pp. 11-22. doi: 10.1049/iet-cdt.2012.0148
18. Ciewobr H., Gbolagade K.A. Modulo Operation Free Reverse Convertion in the $\left\{2^{2n+1}-1,\ 2^{2n},\ 2^{2n}-1\right\}$ Moduli Set. *Int. J. of Computer Applications*, 2014, vol. 85, no. 1, pp. 11-14.
19. Noorimehr M.R., Hosseinzadeh M., Farshidi R. High Speed Recidue to Binary Converter for the new Four-moduli set $\left\{2^{2n},\ 2^{2n}+1,\ 2^{n/2}+1,\ 2^{n/2}-1\right\}$. *Arabian J. for Science and Eng.*, 2014, vol. 39, no. 4, pp. 2887-2893.

20. Kolyada A.A., Pack I.T. *Moduljarnye struktury konvejernoj obrabotki cifrovoj informacii* [Modular structures of conveyor processing of digital information]. Minsk, University publ., 1992, 256 p.
21. Harin Iu.S., Bernik V.I., Matveev G. V. and etc. *Matematicheskie i komp'juternye osnovy kriptologii* [Mathematical and computational base of cryptology]. Minsk: Novoe znannie, 2003, 382 p.
22. Gorodecky D.A., Kolyada A.A., Kolyada N.A., Shabinskaya E.V. Primenenie tablichno-summatornoj vychislitel'noj tehnologii dlja pozicionno-moduljarnogo kodovogo preobrazovanija po sheme Gornera [Application of the table-summatory computing technology for positional-modular conversion based on the Horner scheme]. *Trudy pervoj mezhdunarodnoj konferencii «Parallel'naja komp'juternaja algebra i ee prilozhenija v novyh infokommunikacionnyh sistemah»* [Proceedings of the 1st International Conference «Parallel algebra and its applications in novel information systems»]. Stavropol, Russia, October 20-24, 2014, pp. 247-252.

Received 02.06.2015

УДК 621.396.674.3

МЕТОД РАСЧЕТА МИКРОПОЛОСКОВОГО ВИБРАТОРА, РАСПОЛОЖЕННОГО НА КИРАЛЬНОЙ ПОДЛОЖКЕ

Клюев Д.С., Нещерет А.М., Осипов О.В.
Поволжский государственный университет телекоммуникаций и информатики, Самара, РФ
E-mail: klyuevd@yandex.ru

В статье приведено описание самосогласованного метода решения внутренней электродинамической задачи о распределении тока на поверхности микрополоскового вибратора, расположенного на киральной подложке. Сформулированы требования, которым должна удовлетворять физическая модель излучателя микрополосковой антенны. Показан вывод элементов матрицы входных адмитансов для кирального слоя, в котором в качестве проводящих включений использованы правовинтовые спирали, а также вывод элементов матрицы поверхностных импедансов. Получено сингулярное интегральное уравнение с особенностью Коши для расчета плотности тока на поверхности микрополоскового вибратора, численное решение которого является корректной математической задачей.

Ключевые слова: киральная среда, микрополосковая антенна, метод сингулярных интегральных уравнений, самосогласованный метод, матрица поверхностных импедансов, плотность тока, корректная математическая задача.

Введение

В современной электродинамике значительный интерес представляет, особенно в диапазонах СВЧ и КВЧ, исследование композитных искусственных сред, обладающих пространственной дисперсией. В диапазонах СВЧ и КВЧ, в отличие от оптически-активных сред, такая среда является искусственной и представляет собой диэлектрическую среду с макроскопическими проводящими включениями различных параметров (геометрическая форма элемента, линейные размеры и т.д.) [1]. Такие среды часто называют метаматериалами. Примером такой среды является киральная среда, представляющая собой совокупность равномерно распределенных и хаотически ориентированных в изотропной диэлектрической среде проводящих элементов зеркально-асимметричной формы [2].

В качестве проводящих включений (киральных элементов) обычно используются лево- и правовинтовые спирали, разомкнутые кольца с выступающими концами, плоские *S*-образные полоски и т.д. В связи с этим существуют объемные модели киральной среды, состоящие из совокупности трехмерных киральных элементов (лево- и правовинтовые спирали и т.д.), и, соответственно, планарные, состоящие из плоских киральных элементов (плоские *S*-образные полоски) [2-4]. Причем последние обладают меньшим значением параметра киральности χ, чем модели, состоящие из совокупности трехмерных киральных элементов [5].

Для того чтобы киральная среда обладала пространственной дисперсией, необходимо, чтобы линейные размеры киральных элементов l были меньше длины волны λ, а расстояние между ними было соизмеримо с ней. В оптически-активных средах, состоящих из молекул зеркально-асимметричной формы, размер этих молекул соизмерим с длиной волны.