ТЕОРЕТИЧЕСКИЕ ОСНОВЫ ТЕХНОЛОГИЙ ПЕРЕДАЧИ И ОБРАБОТКИ ИНФОРМАЦИИ И СИГНАЛОВ

УДК 004.9, 004.94, 004.56

ПРИМЕНЕНИЕ МИНИМАЛЬНО ИЗБЫТОЧНОЙ МОДУЛЯРНОЙ АРИФМЕТИКИ ДЛЯ ВЫПОЛНЕНИЯ КРИПТОГРАФИЧЕСКИХ ПРЕОБРАЗОВАНИЙ В СИСТЕМЕ RSA

Коляда А.А.[1], Кучинский П.В.[1], Червяков Н.И.[2]
[1]Институт прикладных физических проблем имени А.Н. Севченко Белорусского государственного университета, Минск, Беларусь
[2]Северо-Кавказский федеральный университет, Ставрополь, РФ
E-mail: razan@tut.by

Статья посвящена проблемам создания и параметризации математического обеспечения криптографических RSA-преобразований с применение минимально избыточной модулярной арифметики (МИМА). Представляемая разработка включает МИМА-алгоритмизацию метода умножения с квадрированием для возведения в степень по модулю криптосистемы, а также синтез алгоритма расчета коэффициента денормировки вычислительной схемы данной операции. Описанный алгоритм возведения в степень базируется на оптимизированной мультипликативной МИМА-процедуре типа Монтгомери. Реализация с его помощью криптографического преобразования по модулям разрядностью 1024 … 2048 бит на ПЭВМ с процессором Intel Core i5 (тактовая частота 2,27 ГГц) в среднем занимает время порядка 0,56 … 5,67 с. Для расчета денормирующего коэффициента создан новый мультипликативно-субстрактивный метод и на его основе синтезирован простой и эффективный алгоритм, время работы которого на персональной ЭВМ не превышает 13,3 мин.

Ключевые слова: криптосистема RSA, криптографическое RSA-преобразование, модулярная система счисления, интервально-индексные характеристики, минимально избыточная модулярная арифметика, умножение Монтгомери.

Введение

В современных фундаментальных исследованиях и конкретных разработках в области защиты информации особое место занимают криптографические приложения на основе модулярной арифметики (МА) – арифметики модулярных систем счисления (МСС) [1-10]. Это обусловлено тем, что кодовый параллелизм модулярных вычислительных структур (МВС) обеспечивает им ряд существенных преимуществ над позиционными структурами при оперировании в диапазонах больших чисел.

Весьма показательную в этом отношении сферу применения МСС составляют алгоритмы умножения и возведения в степень по большим модулям, основанные на мультипликативной МА-схеме Монтгомери, которые активно используются для высокоскоростной реализации базовых криптографических преобразований в системах RSA [1-2; 5-8; 11-14].

Наиболее трудоемкую часть МА-алгоритмов умножения Монтгомери составляют операции расширения модулярного кода (МК). По уровню простоты процедур немодульных операций, включая расширение кода, среди известных версий МА на текущий момент выделяется так называемая минимально избыточная МА (МИМА) [15]. Синтезированная на базе МИМА оптимизированная модификация мультипликативной схемы Монтгомери для умножения по большим модулям позволяет сократить временные затраты на вычисление интегральных характеристик МК в операциях расширения до теоретического минимума.

Другим важным свойством указанной схемы является обеспечение замкнутости динамического числового диапазона для криптографических преобразований относительно умножения Монтгомери, благодаря чему отпадает необходимость в коррекции произведений при выполнении операций возведения в степень по системному модулю. Наряду с отмеченным при использовании минимально избыточной МСС (МИМСС) достигается также значительное упрощение решения сложных задач параметризации криптосистемы RSA. В частности, это относится к проблемам

генерирования ключей шифрования и дешифрования, вычисления денормирующего коэффициента (ДНК) для процедуры возведения в степень по системному модулю и др.

В статье представлена минимально избыточная модулярная конфигурация алгоритма возведения в степень по большим модулям, который служит основой для реализации базовых преобразований в МИМА-криптосистеме RSA. При этом для синтезированного алгоритма предложены методологические и алгоритмические средства расчета ДНК. Для разработанных средств получены оценки эффективности.

Компьютерно-арифметическая база для криптографических преобразований по схеме RSA модулярного типа

Введем обозначения:

- $\lfloor a \rfloor$ и $\lceil a \rceil$ − наибольшее и наименьшее целые числа (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.$|A|_m$ и $|A|_m^-$ – элементы множеств $\mathbf{Z}_m$ и $\mathbf{Z}_m^-$, сравнимые с А (в общем случае рациональным числом) по модулю m;
- $\mathrm{sn}(a)$ – знаковая функция вида

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

- p − рабочий модуль криптосистемы (большое число).

В МСС с базисом $\mathbf{M}_1$ $\{m_1, m_2, \ldots, m_l\}$, состоящим из $l > 1$ попарно простых модулей (оснований), ЦЧ X представляется кодом $(\chi_1, \chi_2, \ldots, \chi_l)(\chi_i = |X|_{m_i}; i = \overline{1,l})$. Максимальная мощность множества $\mathbf{D}\{\mathbf{M_1}\}$ чисел X, на котором отображение $X \to (\chi_1, \chi_2, \ldots, \chi_l)$ взаимно однозначно, составляет $M_l = \prod_{i=1}^{l} m_i$ элементов. В этом случае $\mathbf{D}\{\mathbf{M_1}\}$ выполняет роль диапазона МСС. Обычно в качестве диапазона используют $\mathbf{Z}_{M_l}$ или $\mathbf{Z}_{M_l}^-$.

Из Китайской теоремы об остатках следует, что ЦЧ X может быть получено по своему МК $(\chi_1, \chi_2, \ldots, \chi_l)$ с помощью равенства

$$X = \sum_{i=1}^{l-1} M_{i,l-1} \cdot \chi_{i,l-1} + M_{l-1} I_l(X) \quad (\chi_{i,l-1} = \left| M_{i,l-1}^{-1} \chi_i \right|_{m_i}), \tag{1}$$

где $M_{i,l-1} = M_{l-1} / m_i$; $M_{l-1} = \prod_{j=1}^{l-1} m_j$; $I_l(X)$ – интервальный индекс (ИИ) числа X [15].

При $|\mathbf{D}\{\mathbf{M_1}\}| < \mathrm{M}_l$ МСС с базисом $\mathbf{M_1}$ является неизбыточной. Использование кодовой избыточности позволяет существенно улучшить арифметические и иные свойства МСС. Сущность применяемого минимально избыточного модулярного кодирования раскрывает нижеследующее утверждение.

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

$$I_l(X) = \begin{cases} \hat{I}_l(X), & \text{если } \hat{I}_l(X) < m_0, \\ \hat{I}_l(X) - m_l, & \text{если } \hat{I}_l(X) \geq m_0; \end{cases} \tag{2}$$

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

$$R_{i,l}(\chi_i) = \left| -m_i^{-1} \right| M_{i,l-1}^{-1} \chi_i \Big|_{m_i} \Big|_{m_l} \quad (i \neq l),$$
$$R_{l,l}(\chi_l) = \left| M_{l-1}^{-} \chi_l \right|_{m_l}. \tag{4}$$

Определение 1. Выражение (1) называется интервально-модулярной формой (ИМФ), а набор величин $(\chi_1, \chi_2, \ldots, \chi_{l-1}, I_l(X))$ или $(\chi_{1,l-1}, \chi_{2,l-1}, \ldots, \chi_{l-1,l-1}, I_l(X))$ - интервально-модулярным кодом (ИМК) числа X по базису $\mathbf{M}_1$. В указанных формах ИМК допускается также использование вместо $I_l(X)$ характеристики $\hat{I}_l(X)$.

Как следует из теоремы 1, переход от неизбыточной МСС с базисом $\mathbf{M_1}$ и диапазоном $Z_{M_l}^-$ к МИМСС тем же базисом и диапазоном Z_{2M}^- предельно упрощает вычисление базовой интегральной характеристики кода – ИИ $I_l(X)$ (см. (2)-(4)). Это приводит к адекватной оптимизации и немодульных процедур, базирующихся на ИМФ (1). В частности, для расширения минимально избыточного МК (МИМК) – $(\chi_1, \chi_2, \ldots, \chi_l)$ на модули

некоторого базиса $\mathbf{M_2} = \{m_{l+1}, m_{l+2}, ..., m_k\} (l < k)$ достаточно согласно (2)-(4) вычислить $I_l(X)$ и затем воспользоваться расчетным соотношением:

$$\chi_j = \left| \sum_{i=1}^{l-1} M_{i,l-1} \cdot \chi_{i,l-1} + M_{l-1} I_l(X) \right|_{m_j}; \quad (j = \overline{l+1,k}). \tag{5}$$

Для операции расширения, реализуемой по формуле (5), далее употребляется условное обозначение: $(\chi_{l+1}, \chi_{l+2}, ..., \chi_k) = EC(X; \mathrm{M}_1, \mathrm{M}_2)$ или его сокращенная форма: $EC(X; \mathrm{M}_1, \mathrm{M}_2)$.

Аппарат ИМФ успешно может применяться и для синтеза других немодульных процедур, например процедуры детектирования знака числа. Наряду с компьютерным ИИ $\hat{I}_l(X) = |I_l(X)|_{m_l}$ введем другую евклидову составляющую $J_l(X) = \lfloor I_l(X) / m_l \rfloor$ ИИ $I_l(X)$, определяемую равенством

$$I_l(X) = \hat{I}_l(X) + m_l \cdot J_l(X) \tag{6}$$

и называемую главным ИИ числа X в МСС с базисом $\mathbf{M_1}$. Справедливо [16-17] нижеследующее утверждение.

Теорема 2. Пусть в МСС с основаниями $\mathbf{M_1}$, $\mathbf{M_2}$, ..., $\mathbf{M}_l \geq l - 2$ $(l \geq 2)$ целому числу X отвечает код $(\chi_1, \chi_2, ..., \chi_l)$ и пусть J_1 (X) – главный ИИ данного ЦЧ. Знаки чисел X и J_1 (X) совпадают при $l = 2$, а также при $l > 2$, если J_1 (X) $\neq -1$.

Применение теоремы 2 для определения знаков чисел в классе решаемых задач криптографических МА-приложений обеспечивает высокую эффективность.

Алгоритм возведения в степень по большому модулю для криптографических преобразований

Процедуры умножения Монтгомери предназначены в первую очередь для вычисления степеней натуральных чисел по рабочему модулю p криптосистемы RSA – целочисленных величин вида

$$Y = |X^e|_p, (X,\ e > 1). \tag{7}$$

Исходя из сказанного эффективность разработанных мультипликативных алгоритмов, синтезированных на основе МИМА-схемы Монтгомери [14], так же, как и других алгоритмов умножения рассматриваемого класса, следует оценивать в контексте проблемы вычисления функции (7), которая описывает криптографические преобразования, выполняемые в системе RSA.

В данном случае основание степени (7) представляет собой число, отождествляемое в системе с шифруемым или дешифруемым сообщением, а показатель является ключом шифрования или дешифрования.

Примем в качестве основы для расчета степеней (7) традиционно применяемый метод умножения с квадрированием (square multiply method) [18], который предполагает двоичное кодирование показателя: $e = (e_{b-1}\ e_{b-2}\ \ldots\ e_0)_2$ $(e_{b-1} = 1;\ b$ – разрядность ЦЧ $e)$ и использует мультипликативную декомпозицию функции Y вида:

$$Y = \left| X^{\sum_{j=0}^{b-1} e_j 2^j} \right|_p = \left| X^{e_0} (X^{e_1} (X^{e_2} (...(X^{e_{b-2}} (X^{e_{b-1}})^2)^2 ...)^2)^2)^2 \right|_p. \tag{8}$$

Применяемый для реализации (8) алгоритм умножения Монтгомери по модулю p работает в модулярном базисе $\mathbf{M} = \{m_1, m_2, \ldots, m_l, m_{l+1}, m_{l+2}, \ldots, m_k\}$ $(1 < l < k)$, который объединяет два базиса: $\mathbf{M_1} = \{m_1, m_2, \ldots, m_l\}$ и $\mathbf{M_2} = \{m_{l+1}, m_{l+2}, \ldots, m_k\}$. При этом мультипликативная схема, положенная в основу базового способа умножения операндов $A = (\alpha_1, \alpha_2, \ldots, \alpha_k)$ и $B = (\beta_1, \beta_2, \ldots, \beta_k)$ по модулю $p = (\pi_1, \pi_2, \ldots, \pi_k)$ $((\alpha_i = |A|_{m_i}, \beta_i = |B|_{m_i}, \pi_i = |p|_{m_i}\ (i = \overline{1,k}))$, описывается в виде операционной последовательности:

$$\begin{aligned}
&\langle\ C = A \cdot B = (\gamma_1, \gamma_2, ..., \gamma_k) = \\
&= (|\alpha_1 \beta_1|_{m_1}, |\alpha_2 \beta_2|_{m_2}, ..., |\alpha_k \beta_k|_{m_k}); \\
&D = (\delta_1, \delta_2, .., \delta_l) = (|\gamma_1 \varphi_1|_{m_1}, |\gamma_2 \varphi_2|_{m_2}, ..., |\gamma_l \varphi_l|_{m_l}) \\
&(\varphi_i = |-\pi_i^{-1}|_{m_i}\ (i = \overline{1,l})); \ \hat{D} = (\delta_1, \delta_2, .., \delta_{l-1}, \hat{I}_l(D)); \\
&\hat{D} = (\hat{\delta}_{l+1}, .\hat{\delta}_{l+2}, ..., \hat{\delta}_k) = EC(\hat{D}; \mathrm{M}_1, \mathrm{M}_2); \\
&\hat{\gamma} = (\hat{\gamma}_{l+1}, \hat{\gamma}_{l+2}, ..., \hat{\gamma}_k) = (\hat{\gamma}_j \left| \gamma_j + \hat{\delta}_j \cdot \pi_j \right|_{m_j} M_l^{-1} \Big|_{m_j} \\
&(j = \overline{l+1,k}));\ \hat{\gamma} = (\hat{\gamma}_1, \hat{\gamma}_2, ..., \hat{\gamma}_l) = EC(\hat{\gamma}; \mathrm{M}_2, \mathrm{M}_1).
\end{aligned} \tag{9}$$

Корректность мультипликативной МИМА-схемы Монтгомери (9) обеспечивается в условиях нижеследующего утверждения.

Теорема 3. Пусть базисы $\mathbf{M_1}$ и $\mathbf{M_2}$ неизбыточной и минимально избыточной МСС, соответственно, с диапазонами

Z_{M_l} и $Z^-_{2m_0 M_{k-1}/M_l}$ $(m_0 \geq \max\{l-2, k-l-2\}$, $m_k \geq 2m_0 + k - l - 2, M_{k-1} = \prod_{i=1}^{k-1} m_i)$,

совместно с модулем p, взаимно простым с M_l, удовлетворяют условию: $2p < \min\{m_0 \cdot M_{l\text{-}1}, m_0 \cdot M_{k\text{-}1}/M_l\}$ и пусть операнды A, B мультипликативной операции $\tilde{\gamma} = \left|ABM_l^{-1}\right|_p$ принадлежат множеству Z_{2p}. Тогда величина $\hat{\gamma}$, вычисляемая в рамках схемы (9), также является элементом множества Z_{2p}. При этом $\hat{\gamma} \equiv \tilde{\gamma} (\mathrm{mod}\, p)$ и для $\tilde{\gamma}$ верна формула $\tilde{\gamma} = \hat{\gamma} - (1 - \mathrm{sn}(\hat{\gamma} - p))p$.

Введем для операции умножения по модулю p, выполняемой согласно схеме (9), условное обозначение ММ(A, B) (A и B – операнды, представленные в базовой МИМСС с основаниями $m_1, m_2, ..., m_k$). Тогда на базе (8) с учетом теоремы 3 можно сформулировать нижеследующий алгоритм возведения в степень.

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

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 возведения в степень по модулю p:

ВС.1. Получить МИМК $(\chi_1', \chi_2', ..., \chi_k')$ ЧЧ $X' = MM(X, N)$.

ВС.2. Присвоить переменной $Y = (\xi_1, \xi_2, \ldots, \xi_k)$ начальное значение $Y = X'$.

ВС.3. Для всех $j = b-2, b-3, \ldots, 0$ выполнить:

ВС.3А. $Y = MM(Y, Y)$.

ВС.3В. Если $e_j = 1$, то найти $Y = MM(Y, X')$.

ВС.4. Определить МИМК $(\chi_1, \chi_2, \ldots, \chi_k)$ искомого значения степени: $Y = MM(Y, 1)$ и завершить работу алгоритма.

Временные затраты на реализацию алгоритма ВС.1…ВС.4 составляют $t_{\text{ВС}} = (b + N_{1,e})t_{\text{ММ}}$, где $N_{1,e} = \sum_{j=0}^{b-1} e_j$ - количество единиц в двоичном коде ЧЧ e; $t_{\text{ММ}}$ – время операции умножения по модулю p.

Пусть b = r_p/2(r_p – разрядность (в битах) модуля p) и пусть количество единичных цифр в двоичном коде показателя степени (7) подчиняется равномерному закону распределения. Тогда $N_{1,e} = b/2$ и $t_{\text{ВС}}$=0,75r_p$\cdot t_{\text{ММ}}$. Для (1024…2048)-битовых p криптографическое RSA- преобразование с применением алгоритма ВС.1…ВС.4 на основе мультипликативной процедуры, реализующей схему Монтгомери (9), на ПЭВМ с процессором Intel Core i5 (тактовая частота 2,27 ГГц) в среднем занимает время порядка 0,56 … 5, 67 с.

Математическая формализация мультипликативно-субстрактивного метода вычисления денормирующего коэффициента для криптографических RSA-преобразований

Используемая в алгоритме ВС.1…ВС.4 константа $N = \left|M_l^2\right|_p$ обеспечивает отсутствие в конечном результате Y коэффициента $\left|M_l^{-1}\right|_p$ нормировки произведений Монтгомери по модулю p. Поскольку p является большим числом, то вычисление ДНК N относится к разряду сложных задач. Благодаря мультипликативной структуре ЧЧ M_l^2 для расчета N удалось разработать метод, который весьма прост в реализации. Демонстрируемый далее подход к решению рассматриваемой задачи базируется на мультипликативно-субстрактивном способе приведения числа M_l^2 к остатку по модулю p с помощью теоремы 2 и вычислительной схемы, конструируемой согласно сравнению вида

$$\Big(\big(...\big(\big(...\big(\big(m_1 - u_1 p\big)m_2 - u_2 p\big)...\big)m_l - u_l p\big) \times m_1 - v_1 p\big)...\big)m_l - v_l p\big) \equiv \left(\prod_{i=1}^{l} m_i \cdot \prod_{j=1}^{l} m_j\right) \equiv N (\mathrm{mod}\, p), \quad (10)$$

где $u_1, u_2, \ldots u_l, v_1, v_2, \ldots, v_l$ – адаптивно выбираемые подходящие целочисленные множители.

Запишем (10) в более наглядной и приемлемой для компьютерной реализации форме:

$$\begin{aligned} &\left\langle N_0^{(1)} = 1,\ N_i^{(1)} = N_{i-1}^{(1)} \cdot m_i - u_i \cdot p \quad (i = \overline{1,l}),\right. \\ &\left. N_0^{(2)} = N_l^{(1)},\ N_i^{(2)} = N_{i-1}^{(2)} \cdot m_i - v_i \cdot p \quad (i = \overline{1,l}) \right\rangle. \end{aligned} \quad (11)$$

Процесс приведения ЧЧ M_l^2 к остатку по модулю p, осуществляемый по схеме (11), является рекурсивным. На каждой итерации этого процесса выполняется одна и та же типовая операция, которая состоит в выделении из множества

$$N(m) = \left\{\forall n' = nm - fp \,|\, f \in Z_m\right\} (n \in Z_p;$$
$$m \in M_1 = \left\{m_1, m_2, ..., m_l\right\})$$

элемента, принадлежащего также и к $\mathbf{Z}_p$. Поиск искомого значения параметра f требует детектирования знаков ЦЧ вида

$$n' = nm - fp \ \ (f \in \mathrm{Z}_m). \tag{12}$$

При использовании сравнительно небольших модулей МСС, например $m \in (2^{15}; 2^{16})$, для выполнения указанных операций может быть применен упрощенный алгоритмический инструментарий, основанный на ИМФ чисел и теореме 2.

Пусть ЦЧ n и p заданы своими ИМФ в базисе $\mathbf{M}_1$:

$$n = \sum_{i=1}^{l-1} M_{i,l-1} \cdot \upsilon_{i,l-1} + M_{l-1} \cdot I_l(n)$$
$$(\upsilon_{i,l-1} = \left| M_{i,l-1}^{-1} \cdot \upsilon_i \right|_{m_i},\ \upsilon_i = \left| n \right|_{m_i}), \tag{13}$$

$$p = \sum_{i=1}^{l-1} M_{i,l-1} \cdot \pi_{i,l-1} + M_{l-1} \cdot I_l(p)$$
$$(\pi_{i,l-1} = \left| M_{i,l-1}^{-1} \cdot \pi_i \right|_{m_i},\ \pi_i = \left| p \right|_{m_i}), \tag{14}$$

где $I_l(n)$ и $I_l(p)$ – интервальные индексы чисел n и p, соответственно. Обозначим через $(\upsilon'_1, \upsilon'_2, ..., \upsilon'_l)$ код числа n' в МСС с модулями $m_1, m_2, ..., m_l$ и его ИИ через $I_l(n')$. Для получения ИМФ ЦЧ вида

$$n' = \sum_{i=1}^{l-1} M_{i,l-1} \cdot \upsilon'_{i,l-1} + M_{l-1} \cdot I_l(n')$$
$$(\upsilon'_{i,l-1} = \left| M_{i,l-1}^{-1} \cdot \upsilon'_i \right|_{m_i}) \tag{15}$$

достаточно в (12) подставить (13)-(14) и затем, применяя лемму Евклида, выполнить преобразование

$$\begin{aligned} n' &= m\left(\sum_{i=1}^{l-1} M_{i,l-1} \cdot \upsilon_{i,l-1} + M_{l-1} \cdot I_l(n) \right) - \\ &- f\left(\sum_{i=1}^{l-1} M_{i,l-1} \cdot \pi_{i,l-1} + M_{l-1} \cdot I_l(p) \right) = \\ &= \sum_{i=1}^{l-1} M_{i,l-1} \left(m \cdot \upsilon_{i,l-1} - f \cdot \pi_{i,l-1} \right) + \\ &+ M_{l-1} \left(m \cdot I_l(n) - f \cdot I_l(p) \right) = \\ &= \sum_{i=1}^{l-1} M_{i,l-1} \left(\left| m \cdot \upsilon_{i,l-1} - f \cdot \pi_{i,l-1} \right|_{m_i} + \right. \\ &\left. + \left\lfloor \left(m \cdot \upsilon_{i,l-1} - f \cdot \pi_{i,l-1} \right) / m_i \right\rfloor \cdot m_i \right) + \\ &+ M_{l-1} \left(m \cdot I_l(n) - f I_l(p) \right) = \\ &= \sum_{i=1}^{l-1} M_{i,l-1} \left| m \cdot \upsilon_{i,l-1} - f \cdot \pi_{i,l-1} \right|_{m_i} + \\ &+ M_{l-1} \left(m \cdot I_l(n) - f I_l(p) + \sum_{i=1}^{l-1} \left\lfloor \left(m \cdot \upsilon_{i,l-1} - f \cdot \pi_{i,l-1} \right) / m_i \right\rfloor \right). \end{aligned} \tag{16}$$

Из (15)-(16) следует, что

$$\upsilon'_{i,l-1} = \left| m \upsilon_{i,l-1} - f \pi_{i,l-1} \right|_{m_i} \left(i = \overline{1, l-1} \right), \tag{17}$$

$$I_l(n') = m \cdot I_l(n) - f I_l(p) + \\ + \sum_{i=1}^{l-1} \left\lfloor \left(m \cdot \upsilon_{i,l-1} - f \cdot \pi_{i,l-1} \right) / m_i \right\rfloor. \tag{18}$$

Согласно теореме 2, число n' и его главный ИИ $G_l(n')$ – см. (6), который, в соответствии с (18), вычисляется по формуле

$$J_l(n') = \left\lfloor I_l(n') / m_l \right\rfloor = \\ = \left\lfloor \left(m I_l(n) - f I_l(p) + \sum_{i=1}^{l-1} \left\lfloor \left(m \cdot \upsilon_{i,l-1} - f \cdot \pi_{i,l-1} \right) / m_i \right\rfloor \right) / m_l \right\rfloor, \tag{19}$$

имеют одинаковые знаки, если $J_l(n') \neq -1$, то есть

$$\mathbf{sn}(n') = \mathbf{sn}(J_l(n')) \quad (J_l(n') \neq -1). \tag{20}$$

Случай $J_l(n') = -1$ отвечает неопределенной ситуации при детектировании знака ЦЧ n' по правилу (20) с использованием (19). Возникновение указанной ситуации на той или иной итерации вычислительной схемы (11) маловероятно и не является критичным. На последующих итерациях возможная неопределенность устраняется с вероятностью практически близкой к единице.

Цель анализа знаков ЦЧ (12) состоит в отыскании значения $\tilde{f}$ параметра $f \in Z_m$, которое обеспечивает выполнение условия:

$$\begin{cases} nm - \tilde{f}p \geq 0; \\ nm - (\tilde{f} + 1)p < 0. \end{cases} \tag{21}$$

Поскольку в (12) $n \in \mathbf{Z}_p$, то $nm \geq 0$, а $nm - mp = m(n - p) < 0$. Следовательно, в $\mathbf{Z}_m$ всегда существует единственный элемент $\tilde{f}$, удовлетворяющий (21).

Мультипликативно-субстрактивный алгоритм расчета денормирующего коэффициента для криптографических RSA-преобразований

На базе изложенных теоретико-методологических положений синтезирован алгоритм расчета денормирующего коэффициента, состоящий в нижеследующем.

Параметры алгоритма:

Модуль p криптосистемы.

Набор $\mathbf{M} = \{m_1, m_2, \ldots, m_l, m_{l+1}, \ldots, m_k\}$ из k 16-битовых простых модулей, который объединяет базисы $\mathbf{M}_1 = \{m_1, m_2, \ldots, m_l\}$ и $\mathbf{M}_2 = \{m_{l+1}, m_{l+2}, \ldots, m_k\}$ $(1<l<k)$ МИМСС с диапазонами $\mathbf{Z}^{-}_{2m_0M_{l-1}}$ и $\mathbf{Z}^{-}_{2m_0M_{k-1}/M_l}$, удовлетворяющие условиям

$$m_l \ge 2m_0 + l - 2,\ m_k \ge 2m_0 + k - l - 2,$$
$$m_0 \ge \mathbf{max}\{l-2, k-l-2\},$$
$$2p < \mathbf{min}\{m_0 \cdot M_{l-1},\ m_0 \cdot M_{k-1}/M_l\}.$$

Входные данные алгоритма: МК $(\pi_1, \pi_2, \ldots, \pi_l)$ модуля p в базисе $\mathbf{M}_1(\pi_i = |p|_{m_i}\ (i = \overline{1, l}))$.

Выходные данные:

МК $(\nu_1, \nu_2, \ldots, \nu_l, \nu_{l+1}, \ldots, \nu_k)$ денормирующего коэффициента $N = |M_l^2|_p$ по полному базису $\mathbf{M}\left(\upsilon_i = |N|_{m_i}\ (i = \overline{1,k})\right)$.

Предварительно получаемые данные:

Коэффициенты нормировки цифр МК в базисе $\mathbf{M}_1$: $\widetilde{C}_i = \left|M_{i,l-1}^{-1}\right|_{m_i}\ (i = \overline{1,l-1})$.

Коэффициенты денормировки цифр МК в базисе $\mathbf{M}_1$: $C_i = |M_{i,l-1}|_{m_i}\ (i = \overline{1,l-1})$.

Коэффициенты для операции расширения интервально-модулярного кода по базису $\mathbf{M}_1$ на модули $m_l, m_{l+1}, \ldots, m_k$: $C_{i,j} = |M_{i,l-1}|_{m_j}\ (i = \overline{1,l-1})$, $C_{l,j} = |M_{l-1}|_{m_j}$, где $j = \overline{l,k}$.

Таблицы *TIIi* интервального индекса, генерируемые по правилу:

$$TIIi[\chi] = R_{i,l}(\chi) = \left|-m_i^{-1}\left|M_{i,l-1}^{-1} \cdot \chi\right|_{m_i}\right|_{m_l}$$
$$(\chi = \overline{0, m_i - 1},\ i = \overline{1, l-1}),$$
$$TIIl[\chi] = R_{l,l}(\chi) = \left|M_{l-1}^{-1} \cdot \chi\right|_{m_l}\ (\chi = \overline{0, m_l - 1}).$$

Тело алгоритма расчета денормирующего коэффициента.

РДНК.1. Для модуля $p = (\pi_1, \pi_2, \ldots, \pi_{l-1}, \pi_l)$ криптосистемы сформировать интервально-модулярный код $(\pi_{1,\ l-1}, \pi_{2,\ l-1}, \ldots, \pi_{l-1,\ l-1}, I_l(p))$ согласно формулам

$$\pi_{i,l-1} = \left|\widetilde{C}_i \cdot \pi_i\right|_{m_i}\ (i = \overline{1,l-1}),$$
$$I_l(p) = \begin{cases} \hat{I}_l(p), \text{ если } \hat{I}_l(p) < m_0, \\ \hat{I}_l(p) - m_l, \text{ если } \hat{I}_l(p) \ge m_0; \end{cases}$$
$$\hat{I}_l(p) = \left|\sum_{i=1}^{l} TIIi[\pi_i]\right|_{ml} \text{ (см. (2)-(4)).}$$

РДНК.2. Сформировать интервально-модулярный код $\left(\widetilde{C}_1, \widetilde{C}_2, ..., \widetilde{C}_{l-1}, I_l(1)\right)$ числа 1, где

$$I_l(1) = \begin{cases} \hat{I}_l(1), \text{ если } \hat{I}_l(1) < m_0, \\ \hat{I}_l(1) - m_l, \text{ если } \hat{I}_l(1) \ge m_0; \end{cases}$$
$$\hat{I}_l(1) = \left|\sum_{i=1}^{l} TIIi[1]\right|_{m_l}.$$

РДНК.3. Выполнить операцию присвоения:

$$n = \left(\upsilon_{1,l-1},\ \upsilon_{2,l-1},\ ...,\ \upsilon_{l-1,l-1},\ I_l(n)\right) =$$
$$= \left(\widetilde{C}_1,\ \widetilde{C}_2,\ ...,\ \widetilde{C}_{l-1} \text{ и } I_l(1)\right) = 1.$$

РДНК.4. Положить $f = 1$.

РДНК.5. Порядковому номеру текущего модуля базиса $\mathbf{M}_1 = \{m_1, m_2, \ldots, m_l\}$ присвоить начальное значение: $j = 1$.

РДНК.6. Применяя (22)-(23) при $f = 0$, рассчитать цифры интервально-модулярного кода $\left(\upsilon'_{1,l-1}, \upsilon'_{2,l-1}, ..., \upsilon'_{l-1,l-1}, I_l(n')\right)$ ЦЧ $n' = n \cdot m_j$:

$$\upsilon'_{i,l-1} = \left|m_j \cdot \upsilon_{i,l-1}\right|_{m_i}\ (i = \overline{1,l-1}),$$
$$I_l(n') = m_j \cdot I_l(n) + \sum_{i=1}^{l-1}\left\lfloor m_j \cdot \upsilon_{i,l-1} / m_i \right\rfloor.$$

РДНК.7. Выполнить операцию присваивания:

$$n = n' \Leftrightarrow (\upsilon_{1,l-1}, \upsilon_{2,l-1}, ..., \upsilon_{l-1,l-1}, I_l(n)) =$$
$$= (\upsilon'_{1,l-1}, \upsilon'_{2,l-1}, ..., \upsilon'_{l-1,l-1}, I_l(n')).$$

РДНК.8. Получить интервально-модулярный код $\left(\upsilon'_{1,l-1}, \upsilon'_{2,l-1}, ..., \upsilon'_{l-1,l-1}, I_l(n')\right) =$
$= \left(\upsilon'_{1,l-1}, \upsilon'_{2,l-1}, ..., \upsilon'_{l-1,l-1}, I_l(n')\right) - (\pi_{1,\ l-1}, \pi_{2,\ l-1}, \ldots, \pi_{l-1,\ l-1}, I_l(p))$ разности $n' = n' - p$, используя формулы типа (17)-(18):

$$\upsilon'_{i,l-1} = \left|\upsilon'_{i,l-1} - \pi_{i,l-1}\right|_{m_i}\ (i = \overline{1,l-1}),$$
$$I_l(n') = I_l(n') + \sum_{i=1}^{l-1}\left\lfloor\left(\upsilon'_{i,l-1} - \pi_{i,l-1} - \pi_{i,l-1}\right)/ m_i\right\rfloor.$$

РДНК.9. Вычислить главный ИИ числа n: $J_l(n') = \lfloor I_l(n')/m_l \rfloor$.

РДНК.10. Если $J_l(n') < -1$ (ЦЧ $n' < 0$) или $J_l(n') = -1$ (случай неопределенности знака ЦЧ n'), то при $j \ne l$ увеличить j на 1 $(j = j + 1)$ и перейти к РДНК.6, а по достижении равенства $j = l$ перейти к РДНК.12.

РДНК.11. В случае $J_l(n') \ge 0$, указывающем на $n' \ge 0$, перейти к РДНК.7.

РДНК.12. При $S=2$ инкрементировать S $(S=S+1)$ и перейти к РДНК.5.

РДНК.13. Полученный интервально-модулярный код $\left(\upsilon_{1,l-1}, \upsilon_{2,l-1}, ..., \upsilon_{l-1,l-1}, I_l(n)\right)$ ЦЧ $n=N=\left|M_l^2\right|_p$ на модули $m_l, m_{l+1}, ..., m_k$ согласно правилу:

$$\upsilon_j=\left|\sum_{i=1}^{l-1}\left|C_{i,j}\cdot\upsilon_{i,l-1}\right|_{m_j}+\left|C_{l,j}\cdot I_l(n)\right|_{m_j}\right|_{m_j}.$$

РДНК.14. Получить цифры МК числа $N=n$ по модулям $m_1, m_2, ..., m_{l-1}$: $\upsilon_i=\left|C_i\cdot\upsilon_{i,l-1}\right|_{m_i}$ $(i=\overline{1,l-1})$.

РДНК. 15. Зафиксировать МК $(\upsilon_1, \upsilon_2, ..., \upsilon_k)$ по полному базису $\mathbf{M}=\{m_1, m_2, \ldots, m_k\}$ в качестве искомого кода денормирующего коэффициента $N=\left|M_l^2\right|_p$ и завершить работу алгоритма.

Общие временные затраты на реализацию приведенного алгоритма ограничены сверху оценкой

$$t_{\text{РДНК, МАКС}}=2\sum_{i=1}^{l}(m_i-1)((3l-1)(t_{\text{СЛ}}+t_{\text{УМ}})+l\cdot t_{\text{ДЕЛ}}, \quad (22)$$

где $t_{\text{СЛ}}, t_{\text{УМ}}$ и $t_{\text{ДЕЛ}}$ – длительности операций сложения и вычитания, умножения и деления 32-битовых ЦЧ соответственно. Пусть в качестве инструментальной базы для реализации схемы (11) используется ПВМ Intel Core i5, тактовая частота которого составляет 2,27 ГГц. Согласно тестам скоростных характеристик для данного процессора $t_{\text{УМ}}>\frac{25}{3}\cdot t_{\text{СЛ}}$, $t_{\text{ДЕЛ}}>2{,}7t_{\text{УМ}}>22{,}5t_{\text{СЛ}}$, $t_{\text{СЛ}}=5$ нс. С учетом этого при p разрядностью 2462 бита оценка (22) дает $t_{\text{РДНК, МАКС}}<13{,}25$ мин. Время расчета ДНК N по схеме (11) сокращается в $\sum_{i=1}^{l}((m_i-1)/\lceil\log_2 m_i\rceil)=\frac{1}{16}\sum_{i=1}^{l}(m_i-1)$ раз, если для поиска $\tilde{f}\in\mathbf{Z}_m$ вместо простого перебора элементов последовательности 1, 2, …, $m-1$ применить процедуру направленного поиска, основанную на делении отрезков, начиная с $[1;\ m-1]$, пополам с последующим переходом к одному из получаемых отрезков.

Заключение

Основные результаты представленной разработки по проблематике создания и параметризации математического обеспечения криптографических RSA-преобразований, базирующихся на МА-алгоритмах умножения и возведения в степень по большим модулям, кратко можно охарактеризовать следующим образом.

1. Рассмотрены важнейшие отличительные свойства МИМА на диапазонах больших чисел, обеспечивающие ей существенные преимущества над неизбыточными аналогами при выполнении криптографических преобразований в системах RSA и решении задач параметризации систем данного класса. Главным из таких преимуществ является снижение до предельно низкого уровня сложности и времени вычисления базовых интегральных характеристик МК – интервально-индексных характеристик, а также синтезированных на их основе процедур расширения кода и сравнения больших чисел.

2. На базе метода умножения с квадрированием, выполняемых по оптимизированной мультипликативной МИМА-схеме Монтгомери, синтезирован алгоритм возведения в степень по большим модулям. Реализация криптографического RSA-преобразования по модулям разрядностью 1024…2048 бит с помощью этого алгоритма на ПЭВМ с процессором Intel Core i5 (тактовая частота 2,27 ГГц) в среднем занимает время порядка 0,56…5,67 с.

3. Проведена математическая формализация нового мультипликативно-субстрактивного метода вычисления денормирующего коэффициента для криптографических RSA-преобразований, осуществляемых применением МИМА. Теоретическую базу метода составляет аппарат ИМФ чисел, который позволяет определять знаки чисел в рамках реализуемой вычислительной схемы с помощью интервально-индексных характеристик по упрощенной процедуре.

4. Предложен эффективный алгоритм формирования минимально избыточного МК денормирующего коэффициента для криптографических RSA-преобразований. Разработанный алгоритм имеет рекурсивную организацию, требуя выполнения на каждой итерации простых операций умножения малоразрядных вычетов на основание МСС и серии вычитаний чисел в интервально-модулярном коде. На множестве модулей криптосистемы разрядности порядка 2462 бита время работы алгоритма не превышает 13,3 мин.

Литература

1. Bajard J.-C., Imbert L. A Full RNS Implementation of RSA // IEEE Trans. Comp. V. 53, N 6, 2004. – P. 769-774. doi: 10.1109/TC.2004.2
2. Lim Z., Phillips B.J. An RNS-Enhanced microprocessor implementation of public key cryptography // Signals, Systems and Computers. ACSSC 2007. Conf. Rec. of the forte-first

Asilomar Conf. 2007. – P. 1430-1434. doi: 10.1109/ACSSC.2007.4487465
3. «Параллельная компьютерная алгебра. Всероссийская НК с элементами научной школы для молодежи». Ставрополь, октябрь, 2010. Сборник научных трудов. Ставрополь: ИИЦ «Фабула», 2010. – 364 с.
4. Червяков Н.И. Применение искусственных нейронных сетей и системы остаточных классов в криптографии. Москва: Физматлит, 2012. – 280 с.
5. Лавриненко А.Н., Червяков Н.И. Округление чисел по модулю поля эллиптической кривой при выполнении криптографических преобразований в системе остаточных классов // Инфокоммуникационные технологии. Т.12, №2, 2014. – С. 4-7.
6. 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. V. 250, 2014. – P. 233-245.
7. Schinianakis D., Stouraitis T. Multifunction recidue architectures for cryptography // IEEE Trans. Circuits and Syst. I., 2014. – P. 1156-1169. doi: 10.1109/TCSI.2013.2283674
8. Bigou K., Tisserand A. RNS modular multiplication through reduced base extensions // 25 Int. Conf. «Application specific systems, architectures and processors (ASSAP 2014)». Zurich, Switzerland, June, 2014. – P. 57-62.
9. 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.
10. Первая МК «Параллельная компьютерная алгебра и ее приложения в новых инфокоммуникационных системах». Ставрополь, октябрь, 2014. Сборник научных трудов. Ставрополь: ИИЦ «Фабула», 2014. – 568 с.
11. Коляда А.А., Чернявский А.Ф. Умножение по большим модулям с использованием минимально избыточной модулярной схемы Монтгомери // Информатика. № 3, 2010. − С. 31-48.
12. Чернявский А.Ф., Коляда А.А., Коляда Н.А. и др. Умножение по большим модулям методом Монтгомери с применением минимально избыточной модулярной арифметики // Нейрокомпьютеры: разработка, применение. № 9, 2010. − С. 3-8.
13. Каленик А.Н., Коляда А.А., Коляда Н.А., Чернявский А.Ф., Шабинская Е.В. Умножение и возведение в степень по большим модулям с использованием минимально избыточной модулярной арифметики // Информационные технологии. № 4, 2012. − С. 37-44.
14. 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.
15. Коляда А.А., Пак И.Т. Модулярные структуры конвейерной обработки цифровой информации. Минск: Университетское, 1992. – 256 с.
16. Коляда А.А., Чернявский А.Ф. Интегральнохарактеристическая база модулярных систем счисления // Информатика. № 1, 2013. − С. 106-119.
17. Коляда А.А., Чернявский А.Ф. Интервальноиндексный метод четного модуля для расчета интегральных характеристик кода неизбыточной МСС с симметричным диапазоном // Доклады НАН Беларуси, 2013. Т. 57, № 1. − С. 38-45.
18. Kawamura S., Koike Masanobu, Sano Fumihiko, Shimbo Atsushi. Cox-Rower architecture for fast parallel Montgomery multiplication. // Eurocrypt, 2000, LNCS. Vol. 1807. Berlin, 2000. − P. 523-538.

Поступило 20.04.2016

Коляда Андрей Алексеевич, д.ф.-м.н., доцент, научно-исследовательское учреждение «Институт прикладных физических проблем им. А.Н. Севченко» Белорусского государственного университета (НИИ ПФП им. А.Н. Севченко БГУ). Тел. 8-10-375-17-212-47-45, +375-29-255-35-84. E-mail: razan@tut.by

Кучинский Петр Васильевич, д.ф.-м.н., доцент, директор НИИ ПФП им. А.Н. Севченко БГУ). Тел. 8-10-375-17-212-48-16, +375-29-161-12-84. E-mail: niipfp@bsu.by,

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.: +78652354861; E-mail: chervyakov@yandex.ru

APPLICATION OF MINIMALLY REDUNDANT MODULAR ARITHMETIC TO PERFORM THE CRYPTOGRAPHIC TRANSFORMATIONS IN RSA-SYSTEM

Kolyada A.A.[1], Kuchynski P.V.[1], Chervyakov N.I.[2]
[1]Institute of Applied Physics Problems of A.N. Sevchenko Belarusian State University, Minsk, Belarus
[2]North-Caucasus Federal University, Stavropol, Russia Federation
E-mail: razan@tut.by

The article presents the methodological and algorithmic means of implementation of cryptographic RSA-transformations with the usage of minimally redundant modular arithmetic. Proposed solution contains redundant modular arithmetic algorithm of multiplication with squaring for exponentiation on a modular of cryptosystem and synthesis algorithm for evaluation of denormalization coefficient of computing scheme for this operation. Described exponentiation algorithm is based on optimized multiplicative minimally redundant modular arithmetic procedure of Montgomery multiplication. Cryptographic transformation realized by proposed solution takes about 0.56…5.67 seconds for modules with digital capacity 1024…2048 bits under PC with processor Intel Core i5 (2,27 HHz). We developed new multiplicative-substractive method for denormalization coefficient calculation and fast and simple algorithm that takes nor more 13.3 minutes by conventional PC.

Keywords: RSA-cryptosystem, RSA cryptographic RSA-transformation, modular arithmetic, interval-index characteristics, minimumally redundant modular arithmetic, Montgomery multiplication

DOI: 10.18469/ikt.2016.14.3.01

Kolyada Andrey Alekseevich, Institute of Applied Physics Problems of A.N. Sevchenko, Belarusian State University, 7 Kurchatov str., Minsk, 220045, Belarus; Chief Researcher of the Laboratory of Specialized Computer Systems, Doctor of Physical and Mathematical Sciences, Associate Professor. Tel.: +375172124745. E-mail: razan@tut.by.

Kuchynski Petr Vasiljevich, Institute of Applied Physics Problems of A.N. Sevchenko, Belarusian State University, 7 Kurchatov str., Minsk, 220045, Belarus; Director; Doctor of Physical and Mathematical Sciences, Associate Professor. Tel.: +375172124816. E-mail: niipfp@bsu.by.

Chervyakov Nikolay Ivanovich, North-Caucasus Federal University, 1 Pushkina str., Stavropol, 355029, Russian Federation; the Head of Department of Applied Mathematics and Mathematical Modeling, Doctor of Technical Science, Professor. Tel.: +78652354861. E-mail: k-fmf-primath@stavsu.ru.

References

1. Bajard J.-C., Imbert L. A Full RNS Implementation of RSA. *IEEE Trans. Comp*., 2004, vol. 53, no 6, pp. 769-774. doi: 10.1109/TC.2004.2
2. Lim Z., Phillips B.J. An RNS-Enhanced microprocessor implementation of public key cryptography. Signals, Systems and Computers, 2007. *ACSSC* 2007. Conf. Rec. of the forte-first Asilomar Conf, 4-7 November, 2007, pp. 1430-1434. doi: 10.1109/ACSSC.2007.4487465
3. *Parallel Computer Algebra*. Proceedings of Russian Research. Conf. with elements of scientific school for youth. (Stavropol, Russian Federation, 11-15 October 2010, Stavropol, Fabula Publ., 2010. 364 p. (In Russian)
4. Chervjakov N.I. *Primenenie iskusstvennyh nejronnyh setej i sistemy ostatochnyh klassov v kriptografii* [Application of artificial neural network and residual classes system in cryptography]. Moskva, Fizmatlit, 2012, 280 p.
5. Lavrinenko A.N., Chervjakov N.I. Okruglenie chisel po modulju polja jellipticheskoj krivoj pri vypolnenii kriptograficheskih preobrazovanij v sisteme ostatochnyh klassov [Rounding numbers modulo field elliptic curve when performing cryptographic transformations in the residue number system]. *Infokommunikacionnye tehnologii*, 2014, vol. 12, no 2, pp. 4-7.
6. 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
7. Schinianakis D., Stouraitis T. Multifunction recidue architectures for cryptography. *IEEE Trans. Circuits and Syst, I*., 2014, 61, 4, pp. 1156-1169. doi: 10.1109/TCSI.2013.2283674

8. Bigou K., Tisserand A. RNS modular multiplication through reduced base extensions. *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
9. Chervjakov N.I., Derjabin M.A., Lavrinenko I.N. Realizacija algoritma Montgomeri v sisteme ostatochnyh klassov na baze jeffektivnogo algoritma rasshirenija sistemy osnovanij [Implementation of Montgomery algorithm in the system of residual classes on the basis of an efficient algorithm for the expansion of the system bases]. *Nejrokomp'jutery: razrabotka, primenenie*, 2014, no 9, pp. 37-45.
10. *Parallel computer algebra and its application in the new info-communication systems*. Proceedings of The First International Conference, Stavropol, Russia, 20-24 October 2014, Fabula Publ., 2014. 568 p. (In Russian)
11. Koljada A.A., Chernjavskij A.F. Umnozhenie po bol'shim moduljam s ispol'zovaniem minimal'no izbytochnoj moduljarnoj shemy Montgomeri [Multiplication by a large module with minimal excess Montgomery modular scheme]. *Informatika*, 2010, no 3, pp. 31-48.
12. Chernjavskij A.F., Koljada A.A., Koljada N.A. i dr. Umnozhenie po bol'shim moduljam metodom Montgomeri s primeneniem minimal'no izbytochnoj moduljarnoj arifmetiki [Multiplication by high modulus Montgomery method using a minimum excess of modular arithmetic]. *Nejro-komp'jutery: razrabotka, primenenie,* 2010, no 9, Moskva, 2010, pp. 3-8.
13. Kalenik A.N., Koljada A.A., Koljada N.A., Chernjavskij A.F., Shabinskaja E.V. Umnozhenie i vozvedenie v stepen' po bol'shim moduljam s ispol'zovaniem minimal'no izbytochnoj moduljarnoj arifmetiki [The multiplication and exponentiation over large modules using the minimum excess modular arithmetic]. *Informacionnye tehnologii*, 2012, no 4, pp. 37-44.
14. Koljada A.A., Koljada N.A., Mazurenko P.A., Chernjavskij A.F., Shabinskaja 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 on a large modules]. *Nauka i voennaja bezopasnost'*, 2013, no 3, pp. 40-45.
15. Koljada A.A., Pak I.T. *Moduljarnye struktury konvejernoj obrabotki cifrovoj informacii* [Modular structure of the pipeline processing of the digital information]. Minsk, Universitetskoe , 1992. 256 p.
16. Koljada A.A., Chernjavskij A.F. Integral'no-harakteristicheskaja baza moduljarnyh sistem schislenija [Integrated-characteristic modular base number systems]. *Informatika*, 2013, no 1, pp. 106-119.
17. Koljada A.A., Chernjavskij A.F. Interval'no-indeksnyj metod chetnogo modulja dlja rascheta integral'nyh harakteristik koda neizbytochnoj MSS s simmetrichnym diapazonom [Interval-index method is even a module for the calculation of the integral characteristics of non-redundant MSN with a symmetrical range of code]. *Doklady NAN Belarusi*, 2013, vol. 57, no 1, pp. 38-45.
18. Kawamura S., Koike Masanobu, Sano Fumihiko, Shimbo Atsushi. Cox-Rower architecture for fast parallel Montgomery multiplication. *Eurocrypt 2000*, LNCS, vol. 1807, pp. 523-538. doi: 10.1007/3-540-45539-6_37.

Received 20.04.2016

УДК 621.396.677; 621.397.671

СУБЪЕКТИВНЫЕ ФАКТОРЫ СТАТИСТИЧЕСКОЙ ТЕОРИИ АНТЕНН: АНАЛИЗ И МОДЕЛИРОВАНИЕ

Маслов О.Н., Шаталов И.С.
Поволжский государственный университет телекоммуникаций и информатики, Самара, РФ
E-mail: maslov@psati.ru

Представлена проблема конвергенции объективной и субъективной теорий вероятностей с теорией случайных антенн (СА) для исследования СА методом статистического имитационного моделирования (СИМ). Рассмотрены перспективы применения СИМ-моделей при разработке систем активной защиты конфиденциальной информации от утечки во внешнюю среду через СА.

Ключевые слова: теория случайных антенн, объективная и субъективная теории вероятностей, проблема уменьшения неопределенности знаний, метод статистического имитационного моделирования, исследование случайных антенн.