УДК 681.3:681.04

МЕТОД СНИЖЕНИЯ ВЫЧИСЛИТЕЛЬНОЙ СЛОЖНОСТИ РЕАЛИЗАЦИИ RSA КРИПТОПРЕОБРАЗОВАНИЙ НА ОСНОВЕ ИСПОЛЬЗОВАНИЯ ПРИНЦИПА КОЛЬЦЕВОГО СДВИГА В МОДУЛЯРНОЙ СИСТЕМЕ СЧИСЛЕНИЯ

С.О. МАРТЫНЕНКО, В.А. КРАСНОБАЕВ, А.А. ЗАМУЛА, О.М. ХАЛИНА

В статье рассматривается метод аппаратной реализации арифметической модульной операции умножения в спецпроцессоре обработки криптографической информации (СОКИ). Метод основан на принципе кольцевого сдвига в модулярной системе счисления (МСС). Использование МСС позволяет эффективно, с точки зрения повышения быстродействия реализации криптографических преобразований, организовать процесс реализации модульной целочисленной арифметической операций умножения. Разработанный метод рекомендован к использованию в СОКИ при реализации криптографических RSA преобразований.

Ключевые слова: спецпроцессор обработки криптографической информации, модулярная система счисления.

ВВЕДЕНИЕ

Система RSA, входящая в стандарт X-509, широко используется в современных криптосистемах для реализации цифровой подписи и несимметричного шифрования. Основными операциями при реализации вычислений и проверки цифровой подписи являются операции модульного умножения и операция возведение чисел в квадрат по модулю [1-4]. Современные спецпроцессоры обработки криптографической информации (СОКИ) при реализации криптопреобразований с открытым ключом значительную часть времени тратят на реализацию операции модульного умножения. Так, если размерность обрабатываемых чисел равна m, то для RSA-криптопреобразований количество операций модульного умножения и операций возведения чисел в квадрат по модулю, выполняемых СОКИ, равно, соответственно, $m/2$ и m.

Известно, что вычислительная сложность (ВС) криптографического алгоритма определяется временем его реализации. В общем случае ВС определяется количеством входящих в алгоритм разнотипных операций и временем реализации каждой из операции. Таким образом, существуют два пути снижения ВС реализации алгоритма: частичное сокращение количества операций и уменьшение времени реализации операций. Первый путь предполагает изменение алгоритма, что вряд ли целесообразно и вообще возможно. Второй путь - основан на уменьшении времени выполнения модульных операций, которые в современных СОКИ (embedded processor, processor node) реализуются в обычной двоичной позиционной системе счисления (ПСС).

ОСНОВНАЯ ЧАСТЬ

Проведенные исследования показали, что двоичная ПСС, в которой представляется и обрабатывается информация в современных СОКИ, обладают существенным недостатком – наличием межразрядных связей. Данный недостаток накладывают свой отпечаток на методы реализации арифметических операций, усложняют аппаратуру, снижает достоверность вычислений, и ограничивают быстродействие реализации криптографических преобразований. Поэтому естественно изыскание возможностей построения такой арифметики, в которой бы поразрядные связи отсутствовали. В этом плане обращает на себя внимание модулярная система счисления (МСС). МСС обладает ценным свойством независимости друг от друга остатков по принятой системе оснований. Эта независимость открывает широкие возможности в построении не только новой машинной арифметики, но и принципиально новой схемной реализации СОКИ, которая в свою очередь заметно расширяет применение этой машинной арифметики. Во многих литературных источниках отмечается, что одним из практических направлений повышения пользовательской производительности вычислительных средств является внедрение нетрадиционных методов представления и параллельной обработки информации в числовых системах с параллельной структурой. В частности, в МСС, обладающих максимальным уровнем внутреннего параллелизма в организации процесса переработки информации [5, 6].

Цель статьи – разработка метода снижения вычислительной сложности RSA криптопреобразований на основе использования принципа кольцевого сдвига в модулярной системе счисления. В этом случае снижение вычислительной сложности RSA систем основано на использовании второго пути – уменьшения времени выполнения операций, входящих в алгоритмы криптопреобразований. В частности, уменьшение времени реализации операции модульного умножения.

Для исследования методов выполнения операции модульного умножения в МСС, на основе использования ПКС, введем и воспользуемся понятием оператора кольцевого сдвига (ОКС). ОКС – это оператор, определяющий величину (выраженную в количестве z одновременно

сдвигаемых разрядов КСР) и направление сдвига разрядов КСР при реализации арифметических операций и обозначается как $k^{(z)}$, где

$$z=\begin{cases}+z, & \text{при положительном направлении сдвига содержимого разрядов КСР,}\\ -z, & \text{при отрицательном (по часовой стрелке направлении сдвига содержимого разрядов КСР),}\end{cases}$$

а z – показатель оператора кольцевого сдвига (ПОКС).

Метод реализации операции модульного умножения $a_i \cdot \beta_i \pmod{m_n}$ на основе ПКС состоит в использовании набора из двух КСР с применением известного соотношения:

$$a_i\beta_i \pmod{m_n} = \left[\left\{(a_i+\beta_i)\bmod m_n\right]^2 \bmod m_n - \right.$$
$$\left. -\left[(a_i-\beta_i)\bmod m_n\right]^2 \bmod m_n\right\}\bmod m_n)/4\Big]\bmod m_n. \quad (1)$$

В этом случае ОКС для первого КСР представится в виде $k^{(+\beta_i)}$, а для второго – $k^{(-\beta_i)}$. Время t выполнения операции модульного умножения будет не намного больше того времени, что определяется выражением для сложения-вычитания [7, 8]. Недостаток данного варианта реализации операции модульного умножения – сравнительно большой объем оборудования операционного устройства СОКИ.

Рассмотрим предлагаемый в статье метод реализации операции модульного умножения, основанного на использовании двоичного представлении остатков числа в МСС [9]. Назовем разработанный метод для операции целочисленного модульного умножения – метод контуров (МК). В этом случае используется всего один КСР, с помощью которого определяется результат операций модульного сложения, вычитания и умножения. Для операции модульного умножения ОКС представляется в виде $K_{ij}^{(z_i)}$, где i – номер контура, в котором производится сдвиг содержимого разрядов КСР ($i=\overline{1,n}$); $n=m_n-1$ – количество контуров, по которым работает устройство; j – номер устанавливаемой строки матрицы значений $a\cdot\beta \pmod{m_n}$ (индекс i для операндов a и β опускается), $j=\overline{1,n}$; z_i – ПОКС, обозначающий количество сдвигов содержимого разрядов КСР в данном i-м контуре $\left(z_i=\overline{0,m_i-2}\right)$.

Сущность МК состоит в том, что по значению второго β операнда устанавливается β-я строка таблицы значений $a\cdot\beta \pmod{m_n}$ путем сдвига содержимого разрядов КСР по отдельным контурам (по отдельным модулям m_i, причем $m_i=i+1$, так как минимальный (первый) модуль равен двум, т.е. $m_i=2$. Поскольку нулевая строка таблицы значений $a\ \beta \pmod{m_n}$ не устанавливается ($j\neq 0$), то $j=\overline{2,n}$. Вместе с тем первый разряд КСР устанавливается одновременно со вторым и, таким образом, $i=\overline{2,n}$. Нулевой разряд КСР участия в реализации МК не принимает, так как операция умножения на ноль (a=0; β=0) проще организуется по отдельному алгоритму, например, путем вывода входных нулевых шин операндов a, β непосредственно на нулевой выход устройства. Установление значения содержимого разрядов КСР производится последовательно, начиная с (m–1)-го (старшего) разряда и до второго включительно, т.е. справа налево (табл. 1). На рис. 1 представлена схема реализации операции модульного умножения для произвольного модуля m_i МСС, а на рис. 2 представлена схема реализации операции модульного умножения для модуля $m_i=5$.

Таблица 1

Исходные данные для реализации операции модульного умножения в МСС

β_i	a_i				
	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

Введем понятие обобщенного операнда кольцевого сдвига (ООКС) в виде матрицы $\left\{K_{ij}\right\}=\left\{K_{ij}^{(z_{ij})}\right\}$, где показатель обобщенного операнда кольцевого сдвига (ПООКС) z_{ij} означает количество сдвигов содержимого разрядов КСР в i-м контуре при установлении j-й строки матрицы модульного произведения $a\cdot\beta \pmod{m_n}$. Таким образом, ООКС $\{K_{ij}\}$ будет состоять из набора (m_n-2)-х ОКС и может быть разложен либо по строкам $K_j\left(j=\overline{2,n}\right)$, либо по контурам $K\left(i=\overline{2,n}\right)$ в виде

$$\left\{K_{ij}\right\}=K_j=\left(K_{2j}^{(z_{2j})}K_{3j}^{(z_{3j})}\ \ldots\ K_{nj}^{(z_{nj})}\right), \quad (2)$$

$$\left\{K_{ij}\right\}=K_i=\left(K_{i2}^{(z_{i2})}K_{i3}^{(z_{i3})}\ \ldots\ K_{in}^{(z_{in})}\right). \quad (3)$$

Исходя из записи ООКС $\{K_{ij}\}$ (2), можно определить временную матрицу $\{T_j\}$:

$$\left\{T_j\right\}=\begin{vmatrix} z_{22} & z_{32} & \ldots & z_{n2}\\ \vdots & \vdots & & \vdots\\ z_{2n} & z_{3n} & \ldots & z_{nn}\end{vmatrix}. \quad (4)$$

Время t_j установления j-й строки матрицы (время реализации операции) значений $a\ \beta \pmod{m_n}$ равно сумме ПООКС для j-й строки матрицы (4), умноженной на величину

$$k\cdot\tau, \quad (5)$$

т.е.

$$t_j=\sum_{i=2}^{n} z_{ij}k\tau\,. \quad (6)$$

Очевидно, что $t\approx t_j$. Время t реализации модульной операции умножения можно так же определить, исходя из выражения (3). Действительно, в этом случае временная матрица $\{T_i\}$ по контурам будет совпадать с транспонированной матрицей $\left\{T_j\right\}$, т.е. определить, исходя из выра-

жения (3). Действительно, в этом случае временная матрица $\{T_i\}$ по контурам будет совпадать с транспонированной матрицей $\{T_j\}$, т.е.

$$\{T_i\}=\{T_j\}^T=\begin{vmatrix} z_{22} & z_{23} & \dots & z_{2n} \\ \vdots & \vdots & & \vdots \\ z_{n2} & z_{n3} & \dots & z_{nn} \end{vmatrix}, \qquad (7)$$

а время установления j-й строки матрицы равно сумме ПООКС для j-го столбца матрицы (7), умноженной на величину $k\tau$. Очевидно, что в общем случае время t реализации модульной операции $a\beta(\mathrm{mod}\ m_n)$ как и для операции модульного сложения и вычитания, зависит от величины операнда β (от номера j устанавливаемой строки), т.е.

$$t_{j\,\min} \le t \le t_{j\,\max}. \qquad (8)$$

Исходя из выражения (8), целесообразно оперировать средним $t_{\text{ср}}$ и максимальным $t_{\max}$ временем реализации модульных операций

$$t_{\max}^{(x)} = \sum_{i=2}^{n} t_{ij\ \max}, \qquad (9)$$

$$t_{\text{ср}}^{(x)} = \sum_{i=2}^{n} t_{ij\ \max}/(n-1). \qquad (10)$$

В соответствии с выражением (6) запишем формулы (9), (10) в следующем виде

$$t_{\max}^{(x)} = k\tau\cdot(m_n-1)m_n/2, \qquad (11)$$

$$t_{\text{ср}}^{(x)} = k\tau\sum_{i=2}^{n}(m_i-2)/2. \qquad (12)$$

Отметим, что в каждом из контуров можно применить разработанные алгоритмы сокращения времени установления нужной строки таблицы, которая реализует соответствующую модульную операцию [7]. В этом случае, результат операции модульного умножения будет определяться за время меньшее, чем то, что определяется выражениями (6)–(12). Известно [8], что время реализации операций сложения $t_{\text{слож}}$ и умножения $t_{\text{умн}}$ в ПСС определяться следующими выражениями:

$$t_{\text{слож}} = \tau + (\rho-1)(\tau_{\text{и}} + \tau_{\text{или}} + \tau), \qquad (13)$$

$$t_{\text{умн}} = \rho(\tau + t_{\text{слож}}), \qquad (14)$$

где: ρ – количество двоичных разрядов в представлении операндов (разрядная сетка СОКИ); $\tau_{\text{и}}$ ($\tau_{\text{или}}$) – время прохождения сигнала через эле-

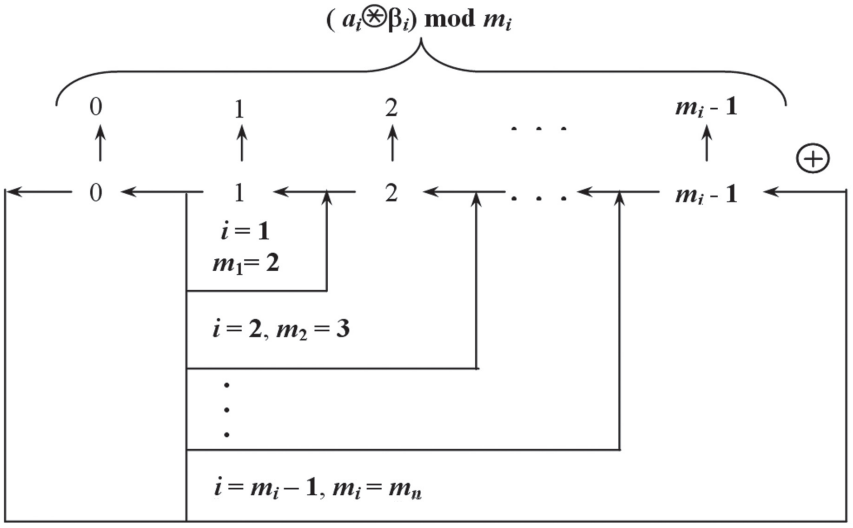

Рис. 1. Схема реализации операции модульного умножения для произвольного модуля mi МСС

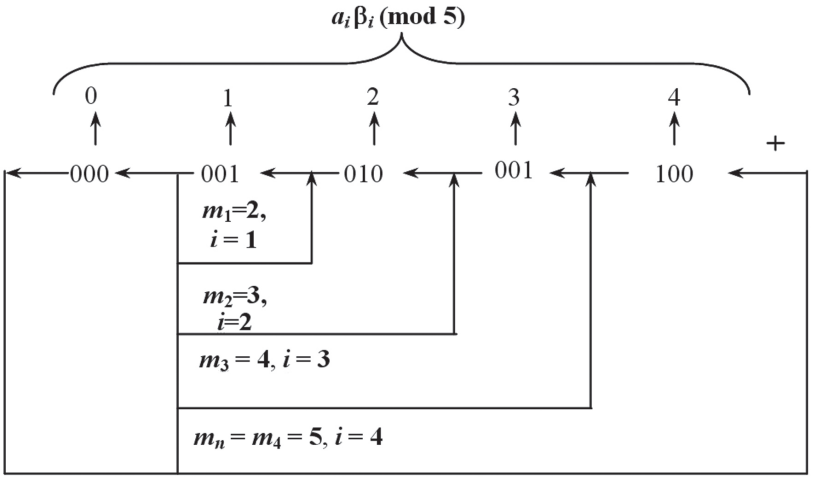

Рис. 2. Схема реализации операции модульного умножения для $m_i = 5$

мент И (ИЛИ) (время «срабатывания» соответствующего логического элемента, т.е. одного вентиля). Принимая во внимание, что $\tau_{и} \approx \tau_{или} \approx \tau/2$, запишем выражения (13) и (14) в виде

$$t_{слож} = \tau\,(2\rho - 1), \qquad (15)$$

$$t_{умн} = 2\tau\rho^2. \qquad (16)$$

Рассмотрим пример технической реализации операции модульного умножения в МСС для $m_n = 5$ (табл. 2). В соответствии с выражениями (2) и (3) ООКС для $m_n = 5$ представим в виде

$$\left\{K_{ij}\right\} = \left\{K_{2j}^{z_{2j}} K_{3j}^{z_{3j}} K_{4j}^{z_{4j}}\right\}. \qquad (17)$$

Разложим ООКС по строкам и контурам.

По строкам получим:

$$j = 2,\ K_2 = \left\{K_{22}^{z_{22}} K_{32}^{z_{32}} K_{42}^{z_{42}}\right\},$$

$$j = 3,\ K_3 = \left\{K_{23}^{z_{23}} K_{33}^{z_{33}} K_{43}^{z_{43}}\right\},$$

$$j = 4,\ K_4 = \left\{K_{24}^{z_{24}} K_{34}^{z_{34}} K_{44}^{z_{44}}\right\}.$$

По контурам имеем:

$$i = 2,\ K_2 = \left\{K_{22}^{z_{22}} K_{23}^{z_{23}} K_{24}^{z_{24}}\right\},$$

$$i = 3,\ K_3 = \left\{K_{32}^{z_{32}} K_{33}^{z_{33}} K_{34}^{z_{34}}\right\},$$

$$j = 4,\ K_4 = \left\{K_{42}^{z_{42}} K_{43}^{z_{43}} K_{44}^{z_{44}}\right\}.$$

На основании соотношения (17) ООКС для соответственно второй ($j = 2$), третьей ($j = 3$) и четвертой ($j = 4$) строк табл. 1 будет иметь следующий вид:

$$K_2 = \left\{K_{22}^{(0)} K_{32}^{(2)} K_{42}^{(3)}\right\},$$

$$K_3 = \left\{K_{23}^{(1)} K_{33}^{(2)} K_{43}^{(2)}\right\},$$

$$K_4 = \left\{K_{24}^{(1)} K_{34}^{(1)} K_{44}^{(1)}\right\}.$$

Общий алгоритм образования ПОКС и ООКС для $m_n = 5$ представлен в табл. 2 (см. рис. 2). Определим время t_j установления j-й строки табл. 1 в соответствии с выражением (6): $t_2 = 15\,\tau$, $t_3 = 15\,\tau$, $t_4 = 9\,\tau$ ($k = [\log_2(m_n - 1)] + 1 = 3$). Отметим, что в соответствии с выражением (14) максимальное время установления j-й строки равно $t_{\max}^{(x)} = 30\tau$ ($t_{ср}^{(x)} = 13{,}5\tau$). Данное обстоятельство подтверждает, что реальная эффективность применения ПКС в МСС выше, чем та, что определяется выражениями (11) и (12).

На рис. 3 и 4 представлены упрощенные варианты схем функционирования операционных устройств СОКИ в МСС при использовании ПКС.

Таблица 2

Алгоритмы образования ПОКС и ООКС для $m_n = 5$

Номер устанавливаемой строки матрицы $j = \beta = \overline{2,4}$	Номер контура $i = \overline{2,4}$	ПОКС $z_{i,j}$	Исходное содержимое КСР	ОКС (z_i) $K_{i,j}$	ООКС $\{K_{i,j}\}$
$j = 2$	$i = 4$	$z_{42} = 3$	0 2 3 4 1 0 3 4 1 2 0 4 1 2 3	$K_{42}^{(3)}$	$K_2 = \left\{K_{22}^{(0)} K_{32}^{(2)} K_{42}^{(3)}\right\}$
	$i = 3$	$z_{32} = 2$	0 1 2 4 3 0 2 4 1 3	$K_{32}^{(2)}$	
	$i = 2$	$z_{22} = 0$	0 2 4 1 3	$K_{22}^{(6)}$	
$j = 3$	$i = 4$	$z_{43} = 2$	0 2 3 4 1 0 3 4 1 2	$K_{43}^{(2)}$	$K_3 = \left\{K_{23}^{(1)} K_{33}^{(2)} K_{43}^{(2)}\right\}$
	$i = 3$	$z_{33} = 2$	0 4 1 3 2 0 1 3 4 2	$K_{33}^{(2)}$	
	$i = 2$	$z_{23} = 1$	0 3 1 4 2	$K_{23}^{(1)}$	
$j = 4$	$i = 4$	$z_{44} = 1$	0 2 3 4 1	$K_{44}^{(1)}$	$K_4 = \left\{K_{24}^{(1)} K_{34}^{(1)} K_{44}^{(1)}\right\}$
	$i = 3$	$z_{34} = 1$	0 3 4 2 1	$K_{34}^{(1)}$	
	$i = 2$	$z_{24} = 1$	0 4 3 2 1	$K_{24}^{(1)}$	

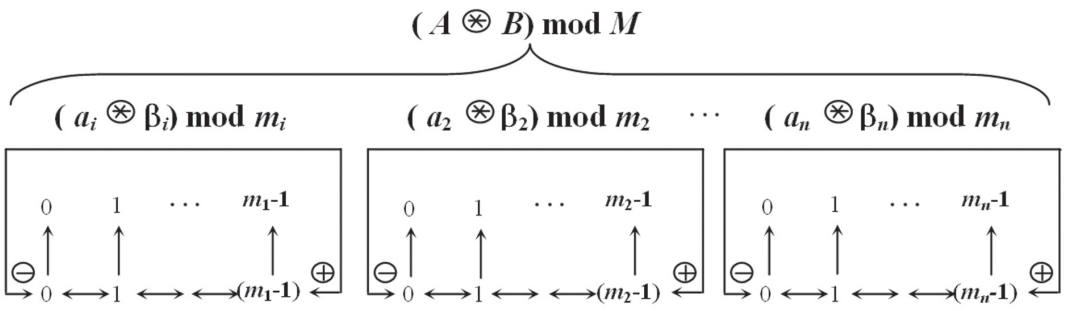

Рис. 3. Операционного устройства СОКИ в МСС

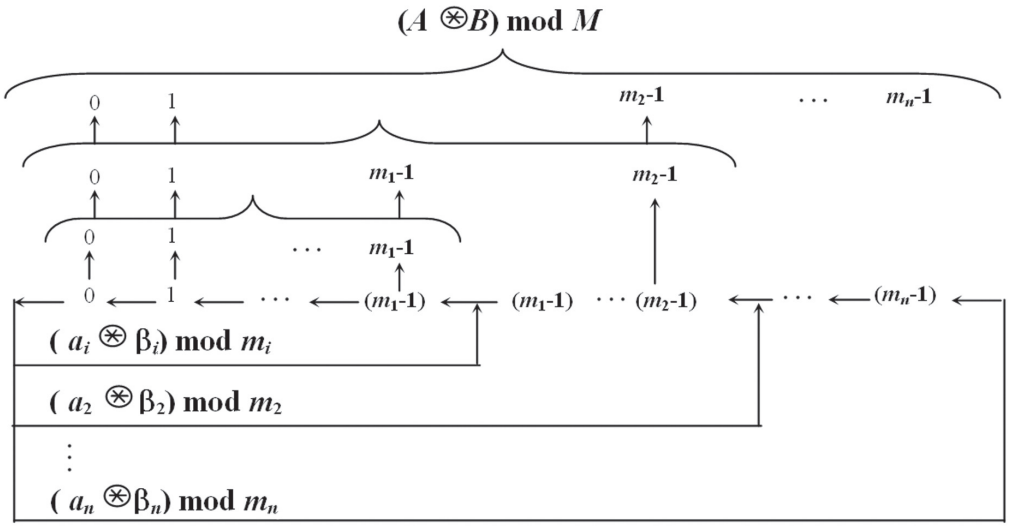

Рис. 4. Операционного устройства СОКИ в МСС

ВЫВОДЫ

В статье предложен метод уменьшения вычислительной сложности реализации алгоритмов RSA на основе использования ПКС в МСС. На основании данного метода разработаны алгоритмы его реализации, а также структуры операционных устройств СОКИ в МСС. Проведенный расчет времени реализации арифметической операции модульного умножения, даже без учета влияний алгоритмов повышения быстродействия, показал высокую эффективность использования предложенного метода. Разработанный метод, алгоритмы и структуры могут быть рекомендованы к практическому использованию для снижения вычислительной сложности реализации криптопреобразований в СОКИ.

Литература.

[1] *Е.Г. Качко, С.С. Батюшко.* Оптимизация алгоритмов для современных стандартов метода RSA // Прикладная радиоэлектроника. Научно-технический журнал. Тематический выпуск, посвященный проблемам обеспечения безопасности информации. – Том 7. 2008. № 3. – С. 252-255.

[2] *Грайворонський М.В., Новіков О.М.* Безпека інформаційно-комунікаційних систем. – К.: Видавнича група BHV, 2009. – 608 с.

[3] *Шнайер Б.* Прикладная криптография. – М.: Издво. «Триумф», 2002. – 797 с.

[4] *Горбенко И.Д., Збитнев С.И., Поляков А.А.* Криптоанализ криптографических преобразований в группах точек эллиптических кривых методом Полларда // Радиотехника: Всеукр. межвед. научн-тех. сб. 2001. Вып. 119. – С. 43-50.

[5] *V.A. Krasnobayev.* Method for Realization of Transformations in Public-Key Cryptography, Telecommunications and Radio Engineering (USA), 2007, Vol. 66, Issue 17, pp. 1559-1572.

[6] *Барсов В.И., Сорока Л.С., Краснобаев В.А., Хери Али Абдуллах.* Модели и методы повышения отказоустойчивости и производительности управляющих вычислительных комплексов специализированных систем управления реального времени на основе применения непозиционных кодовых структур модулярной арифметики. Монография. – Х.: УИПА, 2008. – 147 с.

[7] *Барсов В.И., Сорока Л.С., Краснобаев В.А.* Методология параллельной обработки информации в модулярной системе счисления: Монография. – Х.: МОН, УИПА, 2009. – 268 с.

[8] *В. А. Краснобаев, С.О. Мартыненко, Ж.В. Дейнеко, А.А. Замула, А.А. Баклыков.* Метод обработки криптографической информации в модулярной системе счисления, основанный на принципе кольцевого сдвига // Прикладная радиоэлектроника. Научно-технический журнал. Тематический выпуск, посвященный проблемам обеспечения безопасности информации. – Том 8. 2009. № 3. – С. 343-350.

[9] *Есин В.И., Кузнецов А.А., Сорока Л.С.* Безопасность информационных систем и технологий. – Харьков. ООО “ЭДЭНА”, 2010. – 656 с.

Поступила в редколлегию 21.06.2010.

Мартыненко Сергей Олегович, руководитель предприятия, г. Харьков. Область научных интересов: создание систем быстрой обработки криптографической информации в реальном времени на основе кодов модулярной системы счисления.

Краснобаев Виктор Анатольевич, профессор кафедры автоматизации и компьютерных технологий Харьковского национального технического университета сельского хозяйства им. Петра Василенко, доктор техн. наук, профессор, Заслуженный изобретатель Украины, Почётный радист СССР. Область научных интересов: теоретическое обоснование и практическое создание сверхбыстродействующих и высокоотказоустойчивых вычислительных структур в модулярной арифметике.

Замула Александр Андреевич, профессор кафедры БИТ ХНУРЭ, канд. техн. наук, доцент. Область научных интересов: технологии защиты информации в информационно-телекоммуникационных системах.

Халина Ольга Михайловна, инженер ЗАО «ИИТ». Область научных интересов: защита информации в информационно-телекомуникационных системах.

УДК 681.3:681.04

Метод зниження обчислювальної складності реалізації RSA криптоперетворень на основі використання принципу кільцевого зсуву в медулярній системі числення / С. О. Мартиненко, В. А. Краснобаєв, О.А. Замула, О.М. Халіна // Прикладна радіоелектроніка: наук.-техн. журнал. – 2010. Том 9. № 3. – С. 454-459.

В статті розглядається метод апаратної реалізації арифметичної модульної операції множення у спец процесорі обробки криптографічної інформації (СОКІ). Метод заснований на принципі кільцевого зсуву в модулярній системі числення (МСЧ). Використання МСЧ дозволяє ефективно, з точки зору підвищення швидкодії реалізації криптографічних перетворень, організувати процес реалізації модульної цілочисельної арифметичної операції множення. Розроблений метод рекомендований до використання в СОКІ при реалізації криптографічних RSA перетворень.

Ключові слова: спецпроцесор обробки криптографічної інформації, модулярная система числення.

Табл. 02. Іл.04. Бібліогр.: 09 найм.

UDC 681.3:681.04

Method of reducing computational complexity for realizing RSA cryptotransformations on the basis of using the principle of circular shift in the modular number system / C.O. Martynenko, V.A. Krasnobaev, A.A. Zamula, O.M. Halina // Applied Radio Electronics: Sci. Mag. – 2010. Vol. 9. № 3. – P. 454-459.

The paper considers the method of hardware implementation of an arithmetic modular multiplication operation in a special processor of cryptographic information processing (SPCIP). The method is based on the principle of circular shift in modular number system (MNS). The use of MNS allows effectively, from the point of view of increasing the speed of realizing cryptographic transformations, to organize the process of realizing a modular arithmetic multiplication operation. The developed method is recommended to be used in a SPCIP during realization of cryptographic RSA transformations.

Key words: special processor for cryptographic information processing, modular system of notation.

Tab. 02. Fig. 04. Ref.: 09 items.