УДК 681.142

В.А. Краснобаев[1], С.А. Кошман[2], С.В. Сомов[1], Е.А. Крючко[1]

[1] *Полтавский национальный технический университет имени Юрия Кондратюка, Полтава*
[2] *Харьковский национальный технический университет сельского хозяйства имени Петра Василенко, Харьков*

МЕТОД БЫСТРОЙ ОБРАБОТКИ КРИПТОГРАФИЧЕСКОЙ ИНФОРМАЦИИ В МОДУЛЯРНОЙ СИСТЕМЕ СЧИСЛЕНИЯ

В предлагаемой статье разработан метод быстрой реализации арифметических операций сложения, вычитания, умножения и возведения в квадрат по модулю в модулярной системе счисления. Данный метод рекомендован для реализации целочисленных криптографических преобразований. При этом существенно уменьшается время выполнения основных базовых операций криптоалгоритмов: сложения, вычитания, умножения и возведения в квадрат по модулю простого числа.

***Ключевые слова**: модулярная система счисления, арифметические модульные операции, криптографические преобразования.*

Введение

В системах обработки информации (СОКИ) действия производятся над числами, представленными в виде специальных машинных кодов в принятой системе счисления. Под системой счисления (СС) понимается способ обозначения чисел с целью определения их количественного значения посредством символов, имеющих определенные количественные признаки. Символы, применяемые для изображения чисел, называются цифрами. В зависимости от способа изображения чисел посредством цифр существующие СС условно делят на позиционные и непозиционные системы.

Позиционной называется СС (ПСС), в которой количественное значение каждой цифры разряда зависит от ее места (позиции) в исходном числе. В ПСС любое число изображается в виде последовательности цифр заданной СС

$$A = (a_{\rho-1}, a_{\rho-2}, \ \cdots \ , a_1, a_0), \qquad (1)$$

где ρ – разрядность операндов. Причем каждая цифра a_i (1) может принимать одно из возможных значений $0 \le a_i \le q-1$. Количество q различных цифр, используемых для изображения чисел в ПСС, называются основаниями q-ичной системы счисления ($q=2$ – двоичная СС; $q=3$ – троичная СС; $q=10$ – десятичная СС и т.д.) [1, 2].

В СОКИ наиболее просто реализуются процессы выполнения арифметических операций над операндами, представленными в двоичном коде ($q=2$), т.е. в двоичной позиционной системе счисления.

В этом случае операнд (1) представляется в виде

$$A = a_{\rho-1} \cdot 2^{\rho-1} + a_{\rho-2} \cdot 2^{\rho-2}, + \ \cdots \ +, a_1 \cdot 2 + a_0, \qquad (2)$$

где $a_i = \overline{0,1}$ $(i = \overline{0,\rho-1})$.

Многоразрядные двоичные числа складываются, вычитаются, умножаются и делятся по тем же правилам, что и в десятичной СС. Так как операция сложения играет основную роль в вычислительном процессе СОКИ, то рассмотрим ее более подробно.

Анализ процесса сложения двух чисел посредством позиционного сумматора, показал, что основная сложность при реализации арифметических операций в ПСС – это организация процесса образования и распространения цифр C_i переноса от младшего разряда сумматора к старшему разряду. Наличие межразрядных связей сумматора в ПСС обусловливает следующие недостатки:

– длительность выполнения арифметических операций, которая зависит от величины l разрядной сетке сумматора (для получения конечного результата операции приходится ожидать конца распространения переносов C_i на всю длину машинного слова);

– ошибка, возникшая в одном двоичном разряде сумматора, в процессе переноса от младших разрядов к старшим распространяется по всей длине машинного слова; это обстоятельство обусловливает тот факт, что отказ (сбой) схемы обработки информации одного двоичного разряда сумматора способен вызвать не только однократные, но и многократные ошибки в полученном результате суммирования.

$$\begin{cases} C_{\rho-1} = S_\rho = a_{\rho-1} \wedge b_{\rho-1} \vee \left(a_{\rho-1} \vee b_{\rho-1}\right) \wedge c_{\rho-2} = a_{\rho-1} \wedge b_{\rho-1} \vee \left(a_{\rho-1} \vee b_{\rho-1}\right) \wedge \\ \wedge \left[a_{\rho-2} \ \wedge \ b_{\rho-2} \ \vee \ (a_{\rho-2} \ \vee \ b_{\rho-2}) \ \wedge \ c_{\rho-3} \right] = \bigvee_{i=1}^{\rho-1} (a_{\rho-i} \ \wedge \ b_{\rho-i} \vee a_{\rho-i} \vee b_{\rho-i}) \ \vee \ (a_0 \wedge b_0). \end{cases} \qquad (3)$$

$$\begin{cases} S_{\rho-1} = (a_{\rho-1} + b_{\rho-1}) \bmod 2 \vee c_{\rho-2} = (a_{\rho-1} + b_{\rho-1}) \bmod 2 \vee (a_{\rho-2} \wedge b_{\rho-2} \vee a_{\rho-2} \vee b_{\rho-2}) \wedge c_{\rho-3} = \\ = (a_{\rho-1} + b_{\rho-1}) \bmod 2 \vee (a_{\rho-2} \wedge b_{\rho-2} \vee a_{\rho-2} \vee b_{\rho-2}) \vee (a_{\rho-3} \wedge b_{\rho-3} \vee a_{\rho-3} \vee b_{\rho-3}) \wedge c_{\rho-4} = \\ = (a_{\rho-1} + b_{\rho-1}) \bmod 2 \vee (a_{\rho-2} \wedge b_{\rho-2} \vee a_{\rho-2} \vee b_{\rho-2}) \wedge (a_{\rho-3} \wedge b_{\rho-3} \vee a_{\rho-3} \vee b_{\rho-3}) \wedge \ldots \wedge (a_0 \wedge b_0) = \\ = (a_{\rho-1} + b_{\rho-1}) \bmod 2 \cdot \overset{\rho-2}{\underset{i=1}{\mathrm{V}}} (a_{\rho-1-i} \wedge b_{\rho-1-i} \vee a_{\rho-1-i} \vee b_{\rho-1-i}) \vee (a_0 \wedge b_0). \end{cases} \quad (4)$$

Искажение результата S_{i+1} операции $a_{i+1} + b_{i+1} + c_i$ в $(i+1)$-м двоичном разряде сумматора (т.е. $S_{i+1} \to \overline{S}_{i+1}$ $1 \to 0$ или $0 \to 1$) зависит от функционирования СФП S_{i+1}. Схема формирования признака C_{i+1} определяет сигнал переноса в $(i+2)$-й двоичный разряд сумматора. Таким образом, искажение результата (т.е. значений $S_{i+1} \to \overline{S}_{i+1}$ или $C_{i+1} \to \overline{C}_{i+1}$) операции суммирования в $(i+1)$-м двоичном разряде сумматора в ПСС происходит за счет отказов (сбоев) схем формирования значений S_{i+1} и C_{i+1}. Ошибка вида $C_{i+1} \to \overline{C}_{i+1}$) возникает как за счет переноса ошибки $\overline{C}_{i+1}$, возникшей в СФП C_{i+1}, так и в процессе переноса $(C_{i+1} \to \overline{C}_{i+1})$ значения $\overline{C}_{i+1}$ от $(i+1)$-го разряда к $(i+2)$-у разряду сумматора (см. (3), (4)).

Исходя из вышеизложенного материала, можно сделать следующие выводы:

1. Недостатки вычислительных средств в ПСС – значительное время реализации арифметических операций и низкая достоверность функционирования операционных устройств. Это обусловлено «сильными» межразрядными связями.

2. Один из возможных путей решения этой проблемы – это привлечение новых, нестандартных, оригинальных идей в области машинной арифметики, например использование недвоичных ПСС и т.д., которые позволили бы ослабить либо вообще устранить все межразрядные связи.

3. Один из эффективных путей ослабления либо устранения межразрядных связей – создание машинной арифметики на основе использования некоторых разделов теории чисел (теория делимости, теория сравнения и т.п.). Опираясь на фундаментальные понятия, положения и результаты теории чисел, была создана модулярная система счисления (МСС), использование которой позволило получить интересные результаты в области реализации арифметических операций.

Цель данной статьи – разработка метода реализации криптографических преобразований в МСС на основе принципа кольцевого сдвига (ПКС).

Основная часть

Известно, что в МСС существует четыре метода реализации арифметических операций (табл. 1).

Таблица 1

Методы технической реализации арифметических операций в МСС

№ п.п.	Методы	
1	Метод основан на использовании малоразрядных двоичных сумматоров по модулю m_i.	Время реализации арифметических операций определяется временем выполнения модульной операции по наибольшему по величине m_n модулю МСС.
2	Табличный (матричный) метод реализации арифметических операций.	Время выполнения арифметических операций не зависит от величины m_i модуля МСС. Оно равно времени срабатывания двухвходового элемента И.
3	Метод логических функций.	Время реализации арифметических операций зависит от «длины» цепи логической функции.
4	Метод, основанный на использовании кольцевых сдвигающих регистров.	Время выполнения арифметических операций зависит от величин входных операндов.

В [3] сформулирован принцип реализации целочисленных арифметических операций в МСС – принцип кольцевого сдвига (ПКС), особенность которого заключается в том, что результат арифметической операции $(a_i \pm b_i) \bmod m_i$ по произвольному m_i модулю МСС, заданной совокупностью $\{m_j\}$ $(j = \overline{1,n})$ оснований, определяется без вычисления значений величин S_i и C_i, а только за счет циклических сдвигов заданной цифровой структуры. Действительно, известная теорема Кэли устанавливает изоморфизм между элементами конечной абелевой группы и элементами группы перестановок. В этом случае матрица сложения для произвольного m_i модуля МСС будет задана табл. 2 (для $m_i = 5$ – табл. 3).

Одним из следствий теоремы Кэли является вывод о том, что отображение элементов абелевой группы на группу всех целых чисел является гомоморфным. Это обстоятельство позволяет организовать процесс определения результата арифметических операций в МСС посредством использования ПКС. Так, операнд в МСС представляется набором из n остатков $\{a_i\}$, образованных путем последовательного деления исходного числа A на n попарно простых чисел $\{m_i\}$, для $(i=\overline{1,n})$. В этом случае совокупность остатков $\{m_i\}$ непосредственно отождествляется с суммой n простых полей Галуа вида $\sum_{i=1}^{n} GF(m_i)$.

При рассмотрении метода реализации арифметических операций в МСС удобно и достаточно рассмотреть вариант для произвольного конечного поля Галуа $GF(m_i)$ при i=const, т.е. для конкретной приведенной системы вычетов по модулю m_i. Пусть для заданной операции модульного сложения $(a_i + b_i) \bmod m_i$ в поле $GF(m_i)$ составлена таблица Кэли (табл. 2). Из существования нейтрального элемента в поле $GF(m_i)$ следует, что в табл. 2 есть строка (столбец), в которой элементы данного поля стоят в порядке возрастания, а из того факта, что в поле вычетов $GF(m_i)$ эти элементы различны (порядок группы равен m_i), следует, что в каждой строке (столбце) табл. 2 содержатся все элементы поля ровно по одному разу. Использование перечисленных свойств позволяет реализовать операции модульного сложения и вычитания в МСС путем применения ПКС посредством n кольцевых $M = m_i([\log_2(m_i - 1)] + 1)$-разрядных сдвигающих регистров (КСР).

Пусть произвольная алгебраическая система представлена в виде $S = (G, \otimes($, где G – непустое множество; $\otimes$ – тип операции, определенной для любых двух элементов a_i, $b_i \in G$.

Операция $\oplus$ сложения в множестве классов вычетов R, порожденных идеалом J, образует новое кольцо, называемое кольцом классов вычетов R/J. Его можно представить в виде Z/m_i, где Z – множество целых чисел 0, ±1, ±2,... . (Если основание МСС m_i – простое число, то Z/m_i – поле). Данное обстоятельство обусловливает возможность реализации арифметической операции сложения в МСС без межразрядных переносов (как в ПСС) путем кольцевого сдвига содержимого разрядов КСР.

На основе предложенного в [3] принципа предлагается метод реализации арифметических операций в МСС (метод двоичного позиционно-остаточного кодирования). Суть разработанного в статье метода состоит в том, что исходная цифровая структура для каждого модуля (основания) МСС представляется в виде содержимого первой строки (столбца) таблицы модульного сложения (вычитания) $(a_i \pm b_i) \bmod m_i$ вида (см. рис. 1).

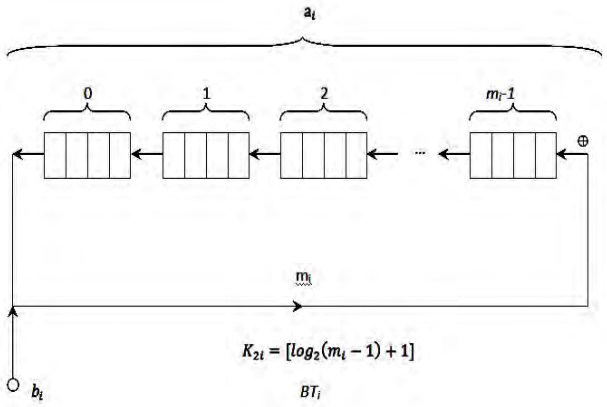

Рис. 1. Сумматор по модулю m_i в МСС

$$P_{\text{исх}}^{(m_i)} = \left[P_0(a_0) \left(P_1(a_1) \left(\ldots \left(P_{m_i-1}(a_{m_i-1}) \right) \right] \right., \quad (5)$$

где (– операция конкатенации (присоединения); $P_v(a_v)$ – k-разрядный двоичный код, соответствующий значению a_v-го остатка $(a_v = \overline{0, m_i - 1})$ числа по модулю m_i; $k = [\log_2(m_i - 1) + 1]$.

Таблица 2

Таблица Кэли для произвольного значения m_i

a_i				
0	1	2	...	$m_i - 1$
0	1	2	...	$m_i - 1$
1	2	3	...	0
2	3	4	...	1
...	...	...	...	...
$m_i - 1$	0	1	...	$m_i - 2$

Таблица 3

Таблица Кэли для $m_i = 5$

b_i	a_i				
	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

Для заданного конкретного модуля m_i =5, исходная цифровая структура содержимого КСР имеет вид

$$P_{\text{исх}}^{(5)} = \left[000 \| 001 \| 010 \| 011 \| 100 \right].$$

Таким образом, посредством используемых в ПСС кольцевых регистров сдвига, легко реализовать целочисленные арифметические операции в МСС. При этом степени циклических перестановок определяется следующими выражениями:

$$\left[P_0(\alpha_0) \| P_1(\alpha_1) \| ... \| P_{m_i-1}(a_{m_i-1}) \right] = \\ = \left[P_z(a_z) \| P_{z+1}(a_{z+1}) \| ... \| P_0(a_0) \| ... \| P_{m_i-1}(a_{m_i-1}) \right]^{Z}; \quad (6)$$

$$\left[P_0(a_0) \| P_1(a_1) \| ... \| P_{m_i-1}(a_{m_i-1}) \right]^{-z} = \\ = \left[P_{m_i-1-z}(a_{m_i-1-z}) \| ... \| P_{m_i-z}(a_{m_i-z1}) \| \right. \quad (7) \\ \left. \| ... \| P_0(a_0) \| P_1(a_1) \| ... \| P_{m_i-z-2}(a_{m_i-z-2}) \right].$$

Отметим, что

$$\left[P_0(a_0) \left(P_1(a_1) \left(... \left(P_{m_i-1}(a_{m_i-1}) \right) \right) \right) \right]^{m_i} = \varepsilon,$$

т.е. при $z = m_i$ все элементы упорядоченного множества $\left\{ P_j(a_i) \right\}$ $(j = \overline{0, m_i - 1})$ остаются на исходном месте. На рис. 2 представлена упрощенная схема операционного устройства в МСС на основе использования ПКС.

При технической реализации данного метода первый операнд a_i определяет номер a_{a_i} разряда $P_{a_i}(a_{a_i})$, с содержимым результата модульной операции по модулю m_i, а второй операнд b_i – число разрядов КРС (b_ik -двоичных разрядов), на которые необходимо провести сдвиги исходного (5) содержимого КРС. На рис. 3 представлена упрощенная схема операционного устройства для однобайтового $(l = 1)$ процессора в МСС.

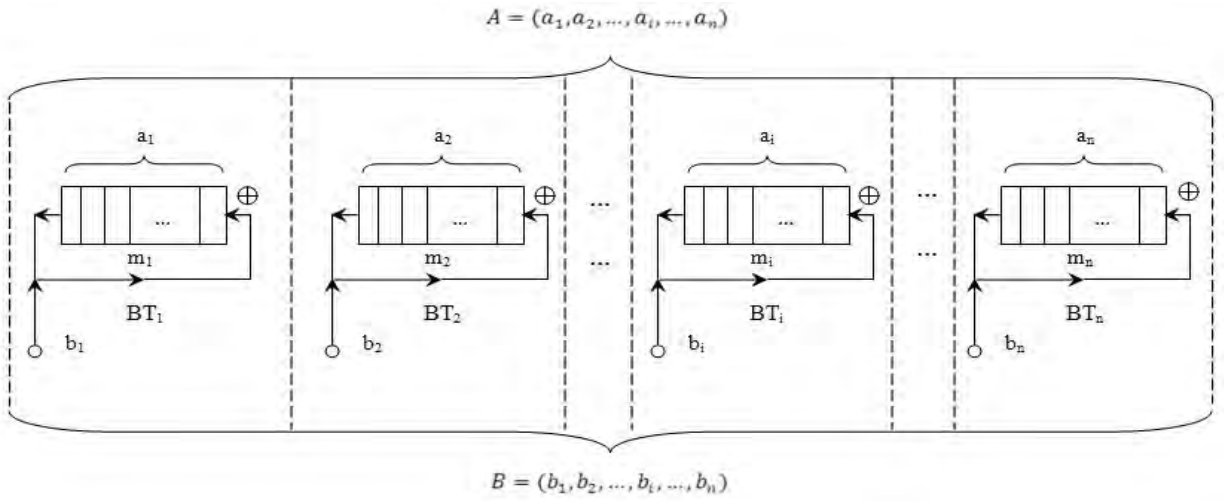

Рис. 2. Схема операционного устройства в МСС

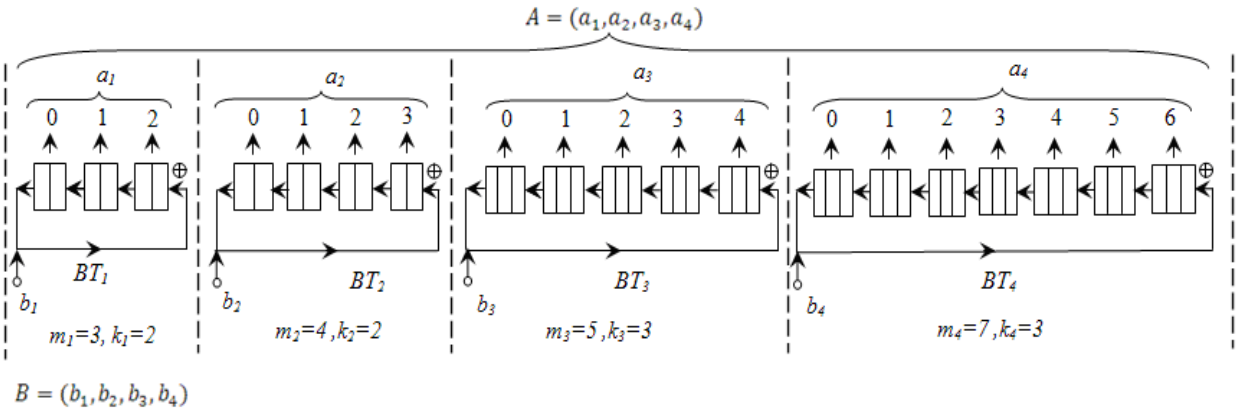

Рис. 3. Упрощенная схема операционного устройства в МСС для однобайтового процессора

Время сложения двух остатков $(a_i + b_i) \bmod m_i$ в МСС определится математическим выражением

$$T_{\substack{\text{мсс} \\ m_i}}^{(+)} = K_{1i} \cdot K_{2i} \cdot t_{\text{сдв}}, \quad (8)$$

где K_{1i} – значение второго b_i слагаемого в сумме $(a_i + b_i) \bmod m_i$ (количество разрядов КРС на которое в положительном направлении сдвигается исходное содержимое КРС), т. е $K_{1i} = \overline{0, m_i - 1}$;

K_{2i} – количество двоичных разрядов в одном разряде КРС по модулю m_i, т.е. $K_{2i} = \left[\log(m_i - 1)\right] + 1$;

$K_{1i} \cdot K_{2i}$ – количество сдвигаемых в положительном (против часовой стрелки) направлении двоичных разрядов КРС;

$t_{сдв} = 3 \cdot \tau_B$ – время сдвига одного двоичного разряда;

τ_B – время срабатывания одного логического вентиля (элемента И, ИЛИ).

Таким образом, для произвольного модуля m_i МСС время сложения двух остатков a_i и b_i равно

$$T^{(+)}_{\substack{мсс \\ m_i}} = 3 \cdot K_{1i} \cdot \left\{\left[\log_2(m_i - 1)\right] + 1\right\} \cdot \tau_B. \quad (9)$$

В этом случае максимально возможное значение $T^{(+)}_{\substack{мсс \\ m_i}}$ для произвольного модуля m_i МСС равно

$$T^{(+)}_{\substack{мсс \\ m_i \\ max}} = 3 \cdot (m_i - 1) \cdot \left\{\left[\log_2(m_i - 1)\right] + 1\right\} \cdot \tau_B, \quad (10)$$

а для данной МСС максимальное время сложения двух чисел $A = (a_1, a_2, \cdots, a_n)$ и $B = (b_1, b_2, \cdots, b_n)$ равно

$$T^{(+)}_{\substack{мсс \\ m_n \\ max}} = 3 \cdot (m_n - 1) \cdot \left\{\left[\log_2(m_n - 1)\right] + 1\right\} \cdot \tau_B. \quad (11)$$

В общем случае время сложения двух чисел $A = (a_1, a_2, \cdots, a_n)$ и $B = (b_1, b_2, \cdots, b_n)$ в МСС определится временем $T^{(+)}_{\substack{мсс \\ m_i}}$ реализации модульной операции $(a_i + b_i) \bmod m_i$ в BT_i, для которого выполняется условие $K_{1i} \cdot K_{2i} = \max$ из всех $BT_j (j = \overline{1, n};\ i \neq j)$.

Выводы

В статье рассмотрен метод реализации криптографических преобразований. Данный метод основан на представлении и обработке целочисленной цифровой информации, представленной в модулярной арифметике. Основное преимущество предложенного метода, по сравнению с ПСС, состоит в возможности достижения высокого быстродействия обработки информации, а также уменьшением вероятности возникновения ошибок за счет или в процессе определений значений S_i и C_i. Результаты изложенных исследований целесообразно также использовать в системах и устройствах обработки больших массивов цифровой информации, представленной в целочисленном виде. В, частности, данный метод рекомендован для использования в системах и устройствах для повышения производительности криптографических преобразований с открытым ключом.

Список литературы

1. Акушский И.Я. Машинная арифметика в остаточных классах / И.Я. Акушский, Д.И. Юдицкий. – М., 1968. – 440 с.

2. Краснобаев В.А. Методы реализации модульных операций в системах цифровой обработки информации / В.А. Краснобаев // Радиотехника. – 2001. – Вып. 119. – С. 130-134.

3. Krasnobayev V.A. Method for Realization of Transformations in Public-Key Cryptography / V.A. Krasnobayev // Telecommunications and Radio Engineering (USA). – 2007. – Vol. 66, Issue 17. – P. 1559-1572.

Поступила в редколлегию 18.06.2013

Рецензент: д-р техн. наук, проф. В.С. Харченко, Национальный аэрокосмический университет им. Н.Е. Жуковского "ХАИ", Харьков.

МЕТОД ШВИДКОЇ ОБРОБКИ КРИПТОГРАФІЧНОЇ ІНФОРМАЦІЇ У МОДУЛЯРНІЙ СИСТЕМІ ЧИСЛЕННЯ

В.А. Краснобаєв, С.О. Кошман, С.В. Сомов, Є.О. Крючко

У запропонованій статті розроблено метод швидкої реалізації арифметичних операцій додавання, віднімання, множення та зведення у квадрат за модулем у модулярній системі числення. Даний метод рекомендований для реалізації цілочисельних криптографічних перетворень. При цьому істотно зменшується час виконання основних базових операцій криптоалгоритмів: додавання, віднімання, множення та зведення у квадрат за модулем простого числа.

Ключові слова: *модулярна система числення, арифметичні модульні операції, криптографічні перетворювання.*

THE METHOD OF RAPID PROCESSING OF CRYPTOGRAPHIC INFORMATION IN A MODULAR NUMBER SYSTEM

V.A. Krasnobayev, S.A. Koshman, S.V. Somov, Y.O. Kriuchko

In this paper we developed a method for rapid implementation of the arithmetic operations of addition, subtraction, multiplication and squaring modulo value in a modular number system. This method is recommended for the implementation of integral cryptographic transformations. This significantly reduces the time to perform basic operations of basic cryptographic algorithms such as addition, subtraction, multiplication and squaring modulo a prime number.

Keywords: *modular number system, modular arithmetic operations, cryptographic transformations.*