УДК 681.142

МЕТОД ОБРАБОТКИ КРИПТОГРАФИЧЕСКОЙ ИНФОРМАЦИИ В МОДУЛЯРНОЙ СИСТЕМЕ СЧИСЛЕНИЯ, ОСНОВАННЫЙ НА ПРИНЦИПЕ КОЛЬЦЕВОГО СДВИГА

В.А. КРАСНОБАЕВ, С.О. МАРТЫНЕНКО, Ж.В. ДЕЙНЕКО, А.А. ЗАМУЛА, А.А. БАКЛЫКОВ

Цель данной статьи – разработка метода реализации арифметических операций в модулярной системе счисления. Данный метод рекомендован для реализации сложных криптографических преобразований. При этом уменьшается время выполнения основных базовых операций криптографических преобразований: сложения, вычитания, умножения и возведения в квадрат.

The aim of this paper is development of the method of realizing arithmetic operations in the module number system. This method is recommended for realization of complex cryptographic transformations. Time of implementing basic operations of cryptographic transformations: addition, subtraction, multiplication and squaring – diminishes.

ВВЕДЕНИЕ

Характерным для технологических применений криптографических средств является возрастание требований к шифрам одновременно по стойкости, скорости, надежности и по простоте технической или программной реализации. Возросшие требования по скорости обработки криптографической информации связаны с необходимостью обеспечения (сохранения) высокой производительности автоматизированных систем после встраивания в них механизмов защиты.

В системах обработки криптографической 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.

В обычных двоичных позиционных системах счисления операция сложения двух чисел $A_{\text{ПСС}}$ и $B_{\text{ПСС}}$, где

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

и

$$B=b_{\rho-1}\cdot 2^{\rho-1}+b_{\rho-2}\cdot 2^{\rho-2},+\ \cdots\ +,b_1\cdot 2+b_0,$$

осуществляется посредством использования сумматора. Сумматор – это узел, выполняющий операцию арифметического сложения (суммирования) двух чисел (слов). Под сложением понимается процесс образования слов с числовыми значениями

$$S=s_{\rho-1}\cdot 2^{\rho-1}+s_{\rho-2}\cdot 2^{\rho-2},+\ \cdots\ +,s_1\cdot 2+s_0,\,.$$

Упрощенная схема организации процесса сложения двух чисел $A_{\text{ПСС}}+B_{\text{ПСС}}$ в ПСС представлена на рис. 1.

Значение S_{i+1} суммы $(i+1)$-го разряда сумматора, а также значение C_{i+1} переноса в соседний старший разряд сумматора определяются следующими соотношениями

$$\begin{cases} C_{i+1}=a_{i+1}\wedge b_{i+1}\vee\left(a_{i+1}\vee b_{i+1}\right)\wedge c_i;\\ S_{i+1}=\left(a_{i+1}\oplus b_{i+1}\right)\bmod 2\vee c_i. \end{cases} \qquad (3)$$

$$\begin{cases} C_0=a_0\wedge b_0;\\ S_0=\left(a_0\oplus b_0\right)\bmod 2, \end{cases} \qquad (4)$$

где a_{i+1}, b_{i+1} – значение $(i+1)$-х разрядов чисел, соответственно, A и B; a_0, b_0 – значения нулевых разрядов чисел, соответственно, A и B; C_0 – значение сигнала переноса нулевого разряда сум-

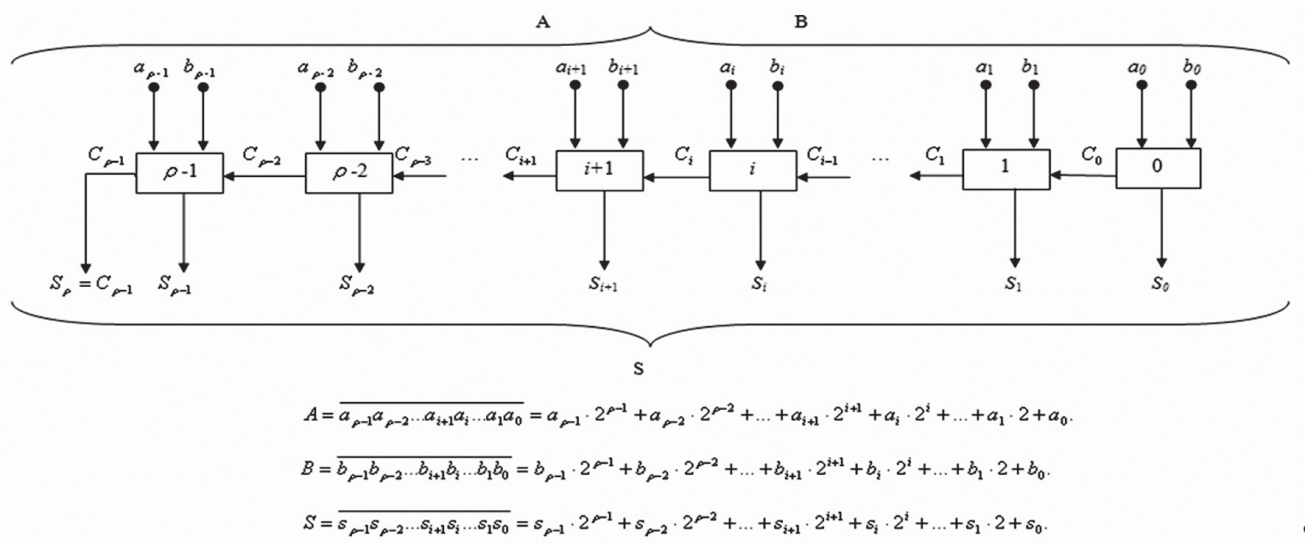


Рис. 1. Упрощенная схема двоичного сумматора в ПСС

матора; S_0 – значение суммы нулевого разряда $(a_i, b_i, c_i, s_i \in 0,1)$.

Схема организации сложения в i-м двоичном разряде $a_{i+1} + b_{i+1} + c_i$ представлена на рис. 2, а на рис. 3 представлена схема сложения в двухразрядном двоичном позиционном сумматоре.

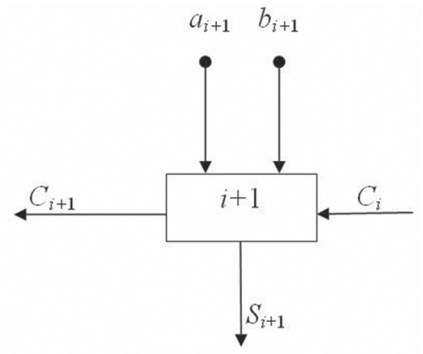


Рис. 2. Схема одного (i+1)-го разряда двоичного сумматора в ПСС

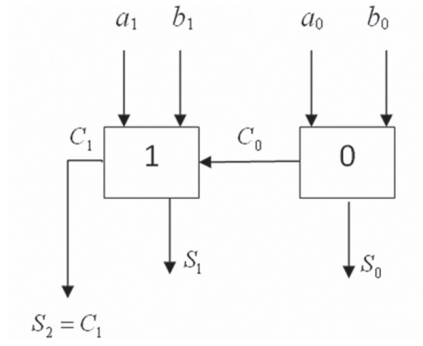


Рис. 3. Двухразрядный двоичный сумматор в ПСС

В табл. 1 и 2 представлены алгоритмы реализации арифметической операции сложения, соответственно, для $(i+1)$-го разряда сумматора и для двухразрядного двоичного сумматора в ПСС.

Соотношение, определяющее значения $C_{\rho-1} = S_\rho$, а также $S_{\rho-1}$ определяются, соответственно, формулами (5) и (6).

Таблица 1

Алгоритм обработки информации в i-м разряде сумматора в ПСС $(i = \overline{0,\rho-1})$

№ пп.	a_{i+1}	b_{i+1}	C_i	S_{i+1}	C_{i+1}
1	0	0	0	0	0
2	0	0	1	1	0
3	0	1	0	1	0
4	0	1	1	0	1
5	1	0	0	1	0
6	1	0	1	0	1
7	1	1	0	0	1
8	1	1	1	1	1

Таблица 2

Алгоритм обработки информации двухразрядного двоичного сумматора в ПСС

A		B		S_2	S_1	S_0
a_1	a_0	b_1	b_0			
0	0	0	0	0	0	0
0	0	0	1	0	0	1
0	0	1	0	0	1	0
0	0	1	1	0	1	1
0	1	0	0	0	0	1
0	1	0	1	0	1	0
0	1	1	0	0	1	1
0	1	1	1	1	0	0
1	0	0	0	0	1	0
1	0	0	1	0	1	1
1	0	1	0	1	0	0
1	0	1	1	1	0	1
1	1	0	0	0	1	1
1	1	0	1	1	0	0
1	1	1	0	1	0	1
1	1	1	1	1	1	0

На рис. 4 представлена общая схема обработки информации в $(i+1)$-м разряде двоичного сумматора в ПСС.

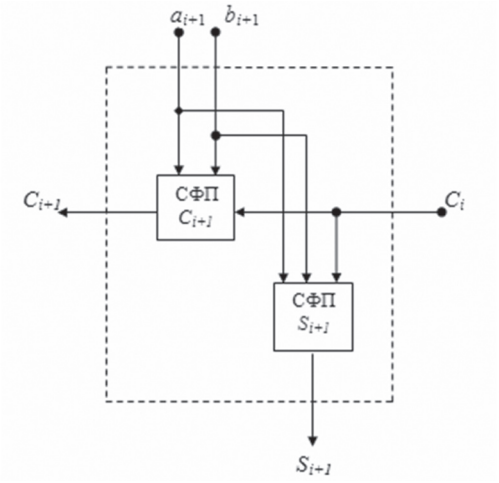


Рис. 4. Схема обработки информации в (i+1)-м разряде двоичного сумматора в ПСС

Схема состоит из двух отдельных схем обработки информации: схема формирования признака C_{i+1} переноса (СФП C_{i+1}); схема формирования признака S_{i+1} суммы (СФП S_{i+1}).

На рис. 5 представлена принципиальная схема обработки информации в $(i+1)$ -м разряде двоичного сумматора.

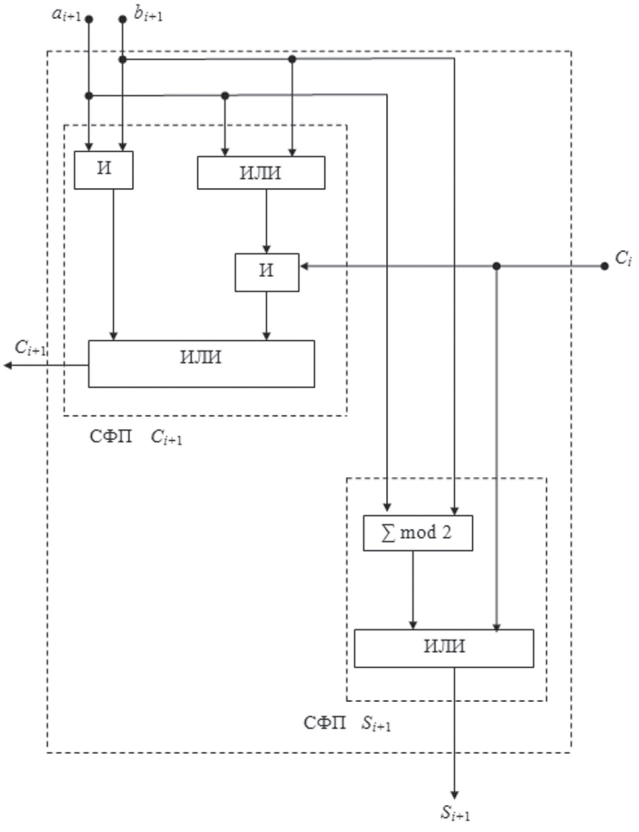


Рис. 5. Принципиальная схема обработки информации в $(i+1)$ -м разряде двоичного сумматора в ПСС

Анализ процесса сложения двух чисел посредством позиционного сумматора (см. рис. 1, 2 и 5), а также выражений (3) – (6), 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.

$$\begin{cases} C_{\rho-1} = S_{\rho} = a_{\rho-1} \wedge b_{\rho-1} \vee \left(a_{\rho-1} \vee b_{\rho-1}\right) \wedge c_{\rho-2} = \\ = a_{\rho-1} \wedge b_{\rho-1} \vee \left(a_{\rho-1} \vee b_{\rho-1}\right) \wedge \\ \wedge \left[a_{\rho-2} \wedge b_{\rho-2} \vee (a_{\rho-2} \vee b_{\rho-2}) \wedge c_{\rho-3}\right] = \\ = \overset{\rho-1}{\underset{i=1}{V}} (a_{\rho-i} \wedge b_{\rho-i} \vee a_{\rho-i} \vee b_{\rho-i}) \vee (a_0 \wedge b_0). \end{cases} \quad (5)$$

$$\begin{cases} S_{\rho-1} = (a_{\rho-1} + b_{\rho-1}) \bmod 2 \vee c_{\rho-2} = \\ = (a_{\rho-1} + b_{\rho-1}) \bmod 2 \vee (a_{\rho-2} \wedge b_{\rho-2} \vee a_{\rho-2} \vee b_{\rho-2}) \wedge \\ \wedge c_{\rho-3} = (a_{\rho-1} + b_{\rho-1}) \bmod 2 \vee (a_{\rho-2} \wedge b_{\rho-2} \vee a_{\rho-2} \vee b_{\rho-2}) \vee \\ \vee (a_{\rho-3} \wedge b_{\rho-3} \vee a_{\rho-3} \vee b_{\rho-3}) \wedge c_{\rho-4} = \\ = (a_{\rho-1} + b_{\rho-1}) \bmod 2 \vee (a_{\rho-2} \wedge b_{\rho-2} \vee a_{\rho-2} \vee b_{\rho-2}) \wedge \\ \wedge (a_{\rho-3} \wedge b_{\rho-3} \vee a_{\rho-3} \vee b_{\rho-3}) \wedge \ldots \wedge (a_0 \wedge b_0) = \\ = (a_{\rho-1} + b_{\rho-1}) \bmod 2 \cdot \\ \cdot \overset{\rho-2}{\underset{i=1}{V}} (a_{\rho-1-i} \wedge b_{\rho-1-i} \vee a_{\rho-1-i} \vee b_{\rho-1-i}) \vee (a_0 \wedge b_0). \end{cases} \quad (6)$$

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} (см. выражение (3), рис. 5). Схема формирования признака C_{i+1} определяет сигнал переноса в $(i+2)$ -й двоичный разряд сумматора (см.выражение (3), рис.5). 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} (см. рис. 5). 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} (рис. 5), 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.

Исходя из вышеизложенного, 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 (см. табл. 3). В этом аспекте в статье рассматривается малоизученный метод реализации арифметических операций, основанный на ПКС.

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 таблицей 4 (для $m_i = 5$ – табл. 5).

Одно 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. 4). Из существования нейтрального элемента в поле $GF(m_i)$ следует, что в табл. 4 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. 4 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 $S = \langle G, \otimes \rangle$, 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

Таблица 3

Методы технической реализации арифметических операций в МСС

№ пп.	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 операций не зависит от величины m_i модуля МСС. Оно равно времени срабатывания двухвходового элемента И.
3	Метод логических функций.	Время зависит от «длины» цепи логической функции.
4	Метод, основанный на использовании кольцевых сдвигающих регистров.	

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. 6).

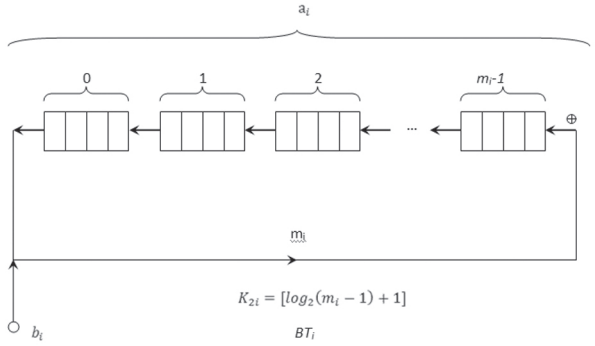


Рис. 6. Сумматор по модулю m_i в МСС (BT_i)

$$P_{\text{исх}}^{(m_i)} = \left[P_0(a_0) \middle\| \left(P_1(a_1) \middle\| \left(\ldots \middle\| \left(P_{m_i-1}(a_{m_i-1}) \right) \right] \right. \right. \right., \qquad (7)$$

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; $k = \left[\log_2(m_i - 1) + 1\right]$.

Таблица 4

Таблица Кэли для произвольного значения m_i

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

Таблица 5

Таблица Кэли для $m_i = 5$

	a_i				
b_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, исходя из (3), определяются следующими выражениями:

$$\left[P_0(\alpha_0) \| P_1(\alpha_1) \| \ldots \| P_{m_i-1}(a_{m_i-1}) \right] = \left[P_z(a_z) \| P_{z+1}(a_{z+1}) \| \ldots \| P_0(a_0) \| \ldots \| P_{m_i-1}(a_{m_i-1}) \right]^Z; \qquad (8)$$

$$\left[P_0(a_0) \| P_1(a_1) \| \ldots \| P_{m_i-1}(a_{m_i-1}) \right]^{-z} = \left[P_{m_i-1-z}(a_{m_i-1-z}) \| \ldots \| P_{m_i-z}(a_{m_i-z1}) \| \ldots \| P_0(a_0) \| P_1(a_1) \| \ldots \| P_{m_i-z-2}(a_{m_i-z-2}) \right]. \qquad (9)$$

Отметим, что

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

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. 7 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 ($b_i k$ – двоичных разрядов), на которые необходимо провести сдвиги исходного (7) содержимого КРС в соответствии с алгоритмами (8), (9). На рис. 8 представлена упрощенная схема операционного устройства для однобайтового $(l = 1)$ процессора в МСС.

Исходя из [4-6], время сложения двух остатков $(a_i + b_i) \bmod m_i$ в МСС определится математическим выражением

$$T_{\substack{\text{мсс} \\ m_i}}^{(+)} = K_{1i} \cdot K_{2i} \cdot t_{\text{сдв}}, \qquad (10)$$

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; $t_{\text{сдв}} = 3 \cdot \tau_B$ – 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

$$T_{\substack{\text{мсс} \\ m_i}}^{(+)} = 3 \cdot K_{1i} \cdot \left\{ \left[\log_2(m_i - 1) \right] + 1 \right\} \cdot \tau_B. \qquad (11)$$

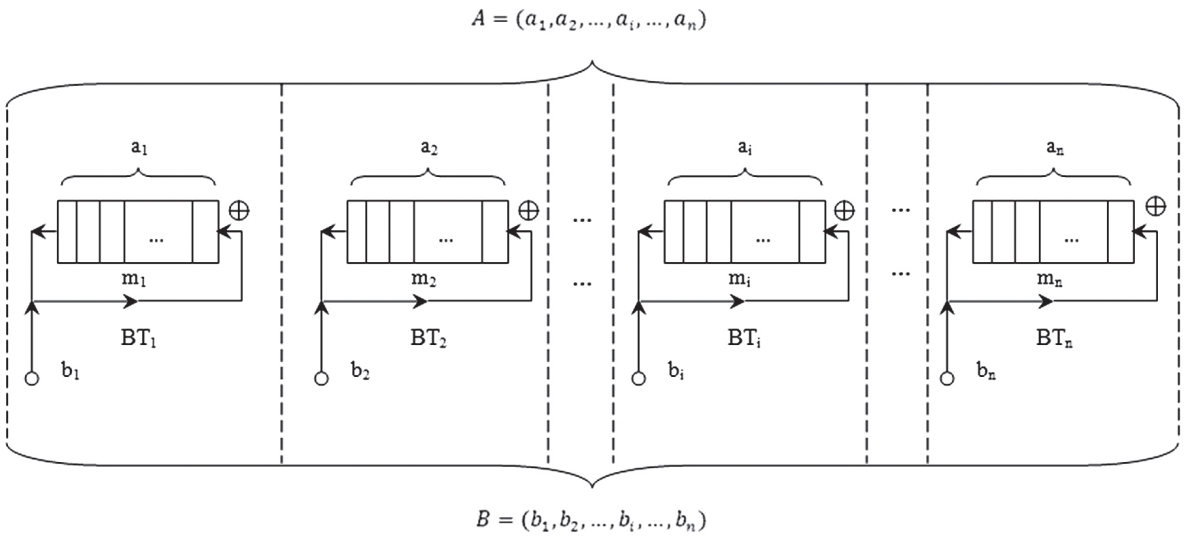


Рис. 7. Схема операционного устройства в МСС

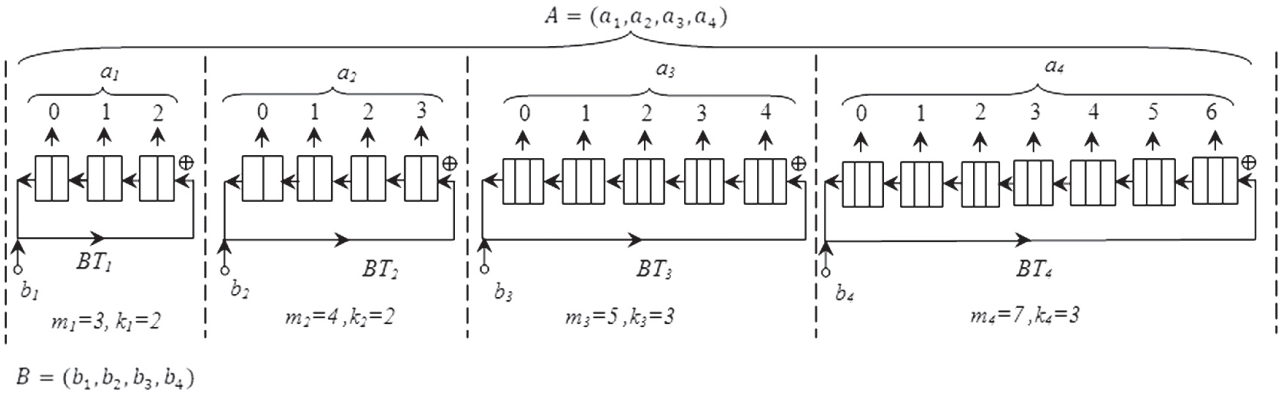


Рис. 8. Упрощенная схема операционного устройства в МСС для однобайтового $(l=1)$ процессора

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

$$T^{(+)}_{\substack{\text{мсс}\\ m_i\\ \max}} = 3\cdot(m_i-1)\cdot\left\{\left[\log_2(m_i-1)\right]+1\right\}\cdot\tau_B, \qquad (12)$$

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

$$T^{(+)}_{\substack{\text{мсс}\\ m_n\\ \max}} = 3\cdot(m_n-1)\cdot\left\{\left[\log_2(m_n-1)\right]+1\right\}\cdot\tau_B, \qquad (13)$$

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 $T^{(+)}_{\substack{\text{мсс}\\ m_i}}$ 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 $BT_j\,(j=\overline{1,n};\ i\neq j)$.

Приведем примеры конкретного выполнения операции сложения двух чисел в МСС для однобайтового $(l=1)$ процессора (см. рис. 8). Для $l=1$ основания МСС могут быть следующие $m_1=3,\ m_2=4,\ m_3=5$ и $m_4=7$.

Пример 1. Пусть второй операнд равен

$$B=(10,10,100,001).$$

Тогда для $BT_1(m_1=3)$ имеем

$$b_1=10,\ K_{11}=2,\ K_{21}=\left[\log(m_i-1)\right]+1=2,$$

$$\text{и}\ \ K_{11}\cdot K_{21}=2\cdot 2=4.$$

Для $BT_2(m_2=4)$ имеем

$$b_2=10,\ K_{12}=2,\ K_{22}=2,\ \text{и}\ \ K_{12}\cdot K_{22}=2\cdot 2=4.$$

Для $BT_3(m_3=4)$ –

$$b_3=100,\ K_{13}=4,\ K_{23}=3,\ \text{и}\ \ K_{13}\cdot K_{23}=4\cdot 3=12.$$

Для $BT_4(m_4=7)$ –

$$b_4=001,\ K_{14}=1,\ K_{24}=3,\ \text{и}\ \ K_{14}\cdot K_{24}=1\cdot 3=3.$$

Как видно наибольшее количество сдвигаемых двоичных разрядов производится в третьем BT_3, а именно 12.

Таким образом, время реализации двух чисел *A* и *B*, определяемое в МСС на основе принципа кольцевого сдвига количественным значением второго слагаемого *B*, равно

$$T^{(+)}_{\substack{\text{мсс}\\ m_3}} = K_{13}\cdot K_{23}\cdot 3\cdot\tau_B = 12\cdot 3\cdot\tau_B = 36\cdot\tau_B.$$

Пример 2. Пусть $B=(10,11,001,001)$. Тогда имеем:

– для $BT_1(m_1=3)$, $b_1=2(10)$, $K_{11}=2$, $K_{21}=2$ и $K_{11}\cdot K_{21}=2\cdot 2=4$;

– для $BT_2(m_2=4)$, $b_2=3(11)$, $K_{12}=3$, $K_{22}=2$ и $K_{12}\cdot K_{22}=3\cdot 2=6$;

– для $BT_3(m_3=5)$, $b_3=1(001)$, $K_{13}=1$, $K_{23}=3$ и $K_{13}\cdot K_{23}=1\cdot 3=3$;

– для $BT_4(m_4=7)$, $b_4=1(001)$, $K_{14}=1$, $K_{24}=3$ и $K_{14}\cdot K_{24}=1\cdot 3=3$.

Таким образом, время сложения чисел A и B определяется временем реализации операции $(a_2+b_2)\bmod m_2$ во втором вычислительном тракте BT_2 и равно

$$T^{(+)}_{\substack{\text{мсс}\\ m_2}}=K_{12}\cdot K_{22}\cdot 3\cdot\tau_B=3\cdot 2\cdot 3\cdot\tau_B=18\cdot\tau_B.$$

В соответствии с формулами (13) и (14) составим таблицу сравнительного анализа времени реализации операции сложения.

Проведем сравнительный анализ времени реализации операции сложения двух чисел A и B в ПСС и в МСС. Известно [7], что время $T^{(+)}_{\text{ПСС}}$ сложения чисел A и B в ПСС равно

$$T^{(+)}_{\text{ПСС}}=(2\cdot\rho-1)t_c=(16\cdot l-1)\cdot 3\cdot\tau_B, \quad (14)$$

где: $\rho=8\cdot l$ – l-байтовое машинное слово (разрядная сетка СОКИ для $l=\overline{1,4,8}$); $t_c=3\cdot\tau_B$ – время суммирования в $(i+1)$-м двоичном разряде позиционного сумматора значений $a_{i+1}+b_{i+1}+c_i$, т.е. определяется время нахождения значений C_{i+1} и S_{i+1}.

Учитывается, что существует метод уменьшения в два раза максимального времени реализации операции модульного сложения в МСС имеем для ПКС

$$T^{(+)}_{\substack{\text{мсс}\\ \max}}=T^{(+)}_{\substack{\text{мсс}\\ m_n}}/2. \quad (15)$$

Введем коэффициент α отношения времени реализации операции сложения в ПСС и в МСС, т.е.

$$\alpha=T^{(+)}_{\text{ПСС}}/T^{(+)}_{\substack{\text{мсс}\\ \max}}=\frac{(16\cdot l-1)\cdot 3\cdot\tau_B\cdot 2}{(m_n-1)\cdot\{[\log_2(m_n-1)]+1\}\cdot 3\cdot\tau_B}=$$
$$=\frac{2\cdot(16\cdot l-1)}{(m_n-1)\cdot\{[\log_2(m_n-1)]+1\}}.$$

ВЫВОДЫ

В статье рассмотрен метод реализации криптографических преобразований с открытым ключом. 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.

Литература.

[1] *Акушский И.Я., Юдицкий Д.И.* Машинная арифметика в остаточных классах. Москва: 1968. – 440 с.

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

[3] *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.

[4] *А.А. Сиора, В.А. Краснобаев, А.А. Замула, В.И. Барсов, Ж.В. Дейнеко, О.Е. Барыльник.* Концепция создания быстродействующих и надежных вычислительных систем и средств обработки цифровой информации на основе использования кодов модулярной ариф-

Таблица 6

Данные сравнительного анализа

l (ρ)	ПСС	МСС			Выигрыш в уменьшении времени [%]
	$T^{(+)}_{\text{ПСС}}/3\cdot\tau_B$	m_n	K	$T^{(+)}_{\substack{\text{МСЧ}\\ \max}}/3\cdot\tau_B$	
1 (8)	15	7	3	9	40
2 (16)	31	13	4	24	22
3 (24)	47	19	5	45	5
4 (32)	63	29	5	70	–
5 (64)	127	53	6	159	–

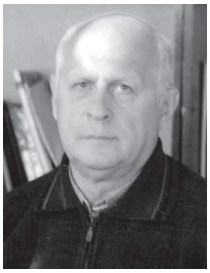
метики // Прикладная радиоэлектроника. Научно-технический журнал. Том 7. 2008. №3. С. 317-321.

[5] *Барсов В.И., Краснобаев В.А., Сиора А.А., Авдеев И.В.* Методы многоверсионной обработки информации в модулярной арифметике: Монография. – Х.: МОН, УИПА, 2008. – 460 с.

[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] *Сиора А.А., Краснобаев В.А., Харченко В.С.* Отказоустойчивые системы с версионно-информационной избыточностью в АСУ ТП: Монография. – Х.: МОН, НАУ им. Н.Е. Жуковского (ХАИ), 2009. – 320 с.

Поступила в редколлегию 25.09.2009



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

Мартыненко Сергей Олегович, руководитель предприятия, г. Харьков. В 1997 году с отличием окончил ХНУРЭ, а в 2000 году в ХНУРЭ окончил аспирантуру. Область научных интересов: создание систем быстрой обработки криптографической информации в реальном времени на основе кодов модулярной системы счисления.

Дейнеко Жанна Валентиновна, старший преподаватель факультета последипломного образования ХНУРЭ, соискатель кафедры информатики ХНУРЭ. Область научных интересов: математическое моделирование, изучение систем нелинейной динамики, построение фазовых портретов, проектирование многозначной логики.

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

Баклыков Александр Александрович, магистр кафедры БИТ ХНУРЭ, инженер 1 категории кафедры БИТ ХНУРЭ. Область научных интересов: системы и средства КЗИ, техническая защита информации.