УДК 681.142

В.А. Краснобаев[1], С.А. Кошман[2], В.Н. Курчанов[1], А.В. Гарамась[1]

[1] *Полтавский национальный технический университет имени Ю. Кондратюка, Полтава*
[2] *Харьковский национальный технический университет сельского хозяйства имени П. Василенка, Харьков*

МЕТОД КОНТРОЛЯ КРИПТОГРАФИЧЕСКОЙ ИНФОРМАЦИИ, ПРЕДСТАВЛЕННОЙ В МОДУЛЯРНОЙ СИСТЕМЕ СЧИСЛЕНИЯ

Предлагается метод контроля ошибок в модулярной системе счисления (МСС), основанный на использования процедуры нулевизации. Суть предложенного метода состоит в том, что при осуществлении процедуры нулевизации в МСС, совмещается во времени операция определения, по цифрам $a_i^{(i-1)}$ и $a_{n-i+1}^{(i-1)}$ числа $A^{(i-1)}$, константы нулевизации $КН^{(i)}$ и операция вычисления по значениям $a_i^{(i-1)}$ и $a_{n-i+1}^{(i-1)}$ следующих цифр $a_{i+1}^{(i)}$ и $a_{n-i}^{(i)}$ числа $A^{(i)}$. Это дает возможность повысить оперативность контроля криптографической информации, представленной в модулярной системе счисления.

Ключевые слова: *модулярная система счисления, контроль криптографической информации*

Введение

Криптопреобразования (КП) нашли широкое применение не только непосредственно для защиты информации от несанкционированного доступа, но и в качестве основы многих новых электронных информационных технологий — электронного документооборота, электронных денег, тайного электронного голосования и др. Современная криптография решает следующие три основные задачи: обеспечение конфиденциальности (секретности); обеспечение аутентификации информации и источника сообщений; обеспечение анонимности (например, сокрытие перемещения электронных денег от одного субъекта к другому). Очевидно, что эффективность реализации КП полностью зависит от качества функционирования спецпроцессора обработки криптографической информации (СОКИ).

Анализ литературных источников. В настоящее время ведутся интенсивные поиски путей повышения эффективности реализации КП за счет разработки и внедрения, надежных и быстродействующих СОКИ реального времени.

Результаты исследований, посвященные улучшению характеристик СОКИ, показали, что одним реально практическим направлениям является подход, основанный на использовании кодов модулярной системы счисления (МСС) [1]. Один из недостатков МСС состоит в том, что отсутствуют простые признаки выхода результата операций за пределы рабочего диапазона [0, M), где $M=\prod_{i=1}^{n} m_i$ – рабочий диапазон; m_i – i-е основание МСС; n – количество рабочих оснований МСС. Это требует дополнительного времени на реализацию процесса коррекции ошибок. Данное обстоятельство снижает эффективность использования в СОКИ МСС.

Для обнаружения ошибок в МСС наиболее часто используется процедура нулевизации. Суть процедуры заключается в последовательном вычитании из исходного числа $A=(a_1, a_2, \ldots, a_n, a_{n+1})$ некоторых минимальных чисел $КН^{(i)}$ – констант нулевизации таких, что число А последовательно за n тактов преобразуется в число вида $A^{(n)}=(0, 0, \ldots, 0, \gamma_{n+1})$. Если полученное значение остатка по контрольному основанию $\gamma_{n+1}\neq 0$, то считается что, число А ошибочно. При этом константы нулевизации должны быть выбраны таким образом, чтобы при вычитаниях вида $A - КН^{(i)}$ не имело бы место выход числа из рабочего [0, M) диапазона [1 – 3]. Существенным недостатком методов обнаружения ошибок в МСС является необходимость значительных временных и аппаратурных затрат при реализации КП, что и обуславливает значительные непроизводительные вычислительные затраты [4 – 6].

Цель данной статьи – разработка и исследования метода контроля ошибок в МСС, основанного на применении процедуры нулевизации.

Основная часть

В общем случае суть процедуры процесса нулевизации состоит из последовательности следующих операций.

1 этап. Исходное проверяемое число

$$A=A^{(0)}=(a_1^{(0)}, a_2^{(0)}, \ldots a_i^{(0)}, a_{i+1}^{(0)}, \ldots a_n^{(0)}, a_{n+1}^{(0)})$$

последовательно приводится к виду

$$A^{(H)}=(0,0,\ldots,0,0,\gamma_{n+1})$$

с помощью такой последовательности операций вычитаний, которая не приведет к выходу числового

значения числа $A^{(0)}$ за рабочий диапазон [0, M) МСС. Как отмечалось ранее, эта операция в МСС называется нулевизацией, и состоит в последовательном вычитании (по одному из оснований МСС) из исходного числа $A^{(0)}$ минимальных чисел, так называемых констант нулевизации ($КН^{(i)}$) вида:

$$КН^{(1)} = (t_{1,1}, t_{2,1}, t_{3,1}, ..., t_{n,1}, t_{n+1,1}), t_{1,1} = \overline{1, m_1 - 1};$$

$$КН^{(2)} = (0, t_{2,2}, t_{3,2}, ..., t_{n,2}, t_{n+1,2}), t_{2,2} = \overline{1, m_2 - 1};$$

$$КН^{(3)} = (0, 0, t_{3,3}, ..., t_{n,3}, t_{n+1,3}), t_{3,3} = \overline{1, m_3 - 1};$$

$$\dots$$

$$КН^{(i)} = (0, 0, ..., 0, t_{i,i}, t_{i+1,i}, ..., t_{n,i}, t_{n+1,i}), t_{i,i} = \overline{1, m_i - 1};$$

$$\dots$$

$$КН^{(n)} = (0, 0, ..., 0, t_{n,n}, t_{n+1,n}), t_{n,n} = \overline{1, m_n - 1}.$$

Далее, исходное проверяемое число А

$$A=A^{(0)} = (a_1^{(0)}, a_2^{(0)}, ...a_i^{(0)}, a_{i+1}^{(0)}, ...a_n^{(0)}, a_{n+1}^{(0)})$$

последовательно приводится к виду $A^{(H)}$, т.е.

$$A=A^{(0)} = (a_1^{(0)}, a_2^{(0)}, ...a_i^{(0)}, a_{i+1}^{(0)}, ...a_n^{(0)}, a_{n+1}^{(0)})$$

$$A^{(1)} = (0, a_2^{(1)}, a_3^{(1)}, ..., a_n^{(1)}, a_{n+1}^{(1)}),$$

$$A^{(2)} = (0, 0, a_3^{(2)}, ..., a_n^{(2)}, a_{n+1}^{(2)}),$$

$$A^{(3)} = (0, 0, 0, a_4^{(3)}, ..., a_n^{(3)}, a_{n+1}^{(3)}) \text{ и т.д.}$$

Продолжая вычитания *n* раз получим значение $A^{(H)} = (0, 0, ..., 0, a_{n+1}^{(n)})$, или $A^{(H)} = (0, 0, ..., 0, \gamma_{n+1})$, где $\gamma_{n+1} = a_{n+1}^{(n)}$.

Общая схема вычитания $A^{(i)}=A^{(i-1)}-КН^{(i)}$ представлена в следующем виде:

$$\begin{array}{r} A^{(i-1)} = (0, 0, ..., 0, a_i^{(i-1)}, a_{i+1}^{(i-1)}, ..., a_n^{(i-1)}, a_{n+1}^{(i-1)}) \\ - \\ КН^{(i)} = (0, 0, ..., 0, a_i^{(i-1)}, t_{i+1,i}, ..., t_{n,i}, t_{n+1,i}) \\ \hline \end{array}$$

$$A^{(i)} = [0, ..., 0, [a_i^{(i-1)} - a_i^{(i-1)}] \bmod m_i,$$

$$[a_{i+1}^{(i-1)} - t_{i+1,i}] \bmod m_{i+1}, ..., [a_{n+1}^{(i-1)} - t_{n+1,i}] \bmod m_{n+1}],$$

где $a_{i+1}^{(i)} = (a_{i+1}^{(i-1)} - t_{t+1,i}) \bmod m_{i+1}$.

Обозначив время выборки КН из соответствующего блока нулевизации (БН) СОКИ как t_1, а время вычитания из числа $A^{(i-1)}$ константы $КН^{(i)}$, т.е. выполнения операции $A^{(i)} = A^{(i-1)}-КН^{(i)}$ - через t_2, получим общее время выполнения операции нулевизации в виде $T_{H1} = n (t_1 + t_2)$.

При выполнении БН в табличном варианте можно предположить, что практически $t_1 = t_2 = \tau_{сл}$.

В этом случае для метода ОН время нулевизации равняется значению $T_{H1}=2n\tau_{сл}$, где: $\tau_{сл}$ - время вычитания из числа $A^{(i-1)}$ константы нулевизации $КН^{(i)}$; n – количество информационных оснований МСС.

2 этап. После нахождения на первом этапе значения γ_{n+1}, на втором этапе проводится сравнение с нулем этого значения γ_{n+1}. Если $\gamma_{n+1}=0$ (число А находится в диапазоне [0,M)), то делается вывод, что число А не искажено (правильное), т.е. ошибок нет. Если $\gamma_{n+1} \neq 0$ (число А не находится в диапазоне [0,M)), то число А искажено (неправильное), т.е. присутствует ошибка по одному из оснований (модулей) m_i МСС. Общее время T_1 обнаружения ошибки определяется как $T_1=T_{H1}+Tc_1$, где Tc_1- время сравнения значения γ_{n+1} с нулем. Практически время Tc_1 сравнение выполняется за один такт, в этом случае можно считать, что $T_1 \approx T_{H1}=2n\tau_{сл}$.

Суть предлагаемого в статье метода контроля ошибок информации в МСС основана на реализации процедуры парной нулевизации чисел с предварительной выборкой цифр (ПНПВЦ). Процедура ПНПВЦ состоит в том, что операция нулевизации в БН, совмещаются во времени с операцией выбора с БКН по цифрам $a_i^{(i-1)}$ и $a_{n-i+1}^{(i-1)}$ числа $A^{(i-1)}$ константы $КН^{(i)}$ и операция создания по значениям $a_i^{(i-1)}$ и $a_{n-i+1}^{(i-1)}$ следующих цифр $a_{i+1}^{(i)}$ и $a_{n-i}^{(i)}$. В тоже время совмещаются во времени операция вычитания из числа $A^{(i-1)}$ константы нулевизации $КН^{(i)}$ (т.е., операция $A^{(i-1)}- КН^{(i)}$) и операция выбора очередной константы нулевизации

$$КН^{(i+1)}=(0,\dots,0, t_{i+1,i+1}, t_{i+2,i+1},\dots, t_{n-I,i+1}, 0,\dots 0, t_{n+1,i+1}).$$

По значениям $a_{i+1}^{(i)}$ и $a_{n-i}^{(i)}$ на следующем этапе нулевизации, по основаниям m_{i+1} и $m_{n-i,}$ будет проводится обращение к БКН за следующей константой нулевизации

$$КН^{(i+1)}= (0,\dots, 0, t_{i+1,i+1}, t_{i+2,i+1},\dots, t_{n-I,i+1}, 0,\dots, 0, t_{n+1,i+1}).$$

Действительно, значение Δa_{i+1} и Δa_{n-i}, которые будут вычтены соответственно с $a_{i+1}^{(i)}$ и $a_{n-i}^{(i)}$, чтобы получить $a_{i+1}^{(i+1)}$ и $a_{n-i-1}^{(i+1)}$, определяются только значениями $a_i^{(i-1)}$ и $a_{n-i+1}^{(i-1)}$. Количество тактов, свободных от сложения, во время которых производиться обращение в БКН СОКИ и образования очередного адреса равняется значению [(n+1)/2], ([x] - целое, ближайшее к х число, но его не превосходящее). При этом нулевизация проводится одновременно по двум информационным основаниям МСС a_1,a_n; a_2,a_{n-1} и т.д. После каждых двух вычитаний требуется еще один дополнительный временной такт для образования очередного адреса и обращение к накопителю констант нулевизации. В связи с этим на каждые два такта сложения ($\tau_{сл} = \tau_0$) приходится один такт свободный от сложения. Оценим эффективность предложенного в статье метода обнаружения ошибок в МСС по отношению к существующему методу, основанного на процедуре обычной нулевизации.

Для количественной оценки эффективности предложенного метода контроля введём понятие коэффициента эффективности:

$$K^{(n)}_{j\,эф} = \frac{T_{H1}/\tau_{сл} - T_{Hj}/\tau_{сл}}{T_{H1}/\tau_{сл}} \cdot 100\%, \qquad (1)$$

где j – номер метода нулевизации:

j=2, для парной нулевизации;

j=3, для парной нулевизаци с предварительной выборкой цифр;

j=4, для парной нулевизации чисел с предварительной выборкой цифр).

Выражение (1) может быть также представлено в виде (2)

$$K^{(n)}_{j\,эф} = \frac{T_{H1}\text{-}T_{Hj}}{T_{H1}} \cdot 100\%. \qquad (2)$$

В соответствии с выражением (2) определим количественное значение $K^{(n)}_{j\,эф}$ для $j=\overline{2,4}$ при n=4, n=6, n=8, n=10 и n=16, т.е. для l-байтовых машинных слов (l = 1, 2, 3, 4 и 8) СОКИ.

Полученные расчётные данные поместим в табл. 1.

Таблица 1

Расчётные данные (выражение (2))

l(n) / $K_{эф}$	1(4)	2(6)	3(8)	4(10)	8(16)
$K^{(n)}_{эф}$,[%]	62	66	62	65	62

В табл. 1 приведены расчетные данные $T/\tau_{сл}$ относительного времени обнаружения ошибок информации в МСС для значения количества n оснований.

Количество информационных оснований МСС $\overline{n=1,16}$ обеспечивает диапазон представления чисел в современных СОКИ, что позволяет использовать полученные данные при их проектировании.

Приведем пример конкретной технической реализации операции обнаружения ошибок в СОКИ, который функционирует в МСС.

Пусть МСС задана основаниями m_1=3, m_2=4, m_3=5, m_4=7, m_5=11 (n=4), т.е. рассматривается однобайтовая (l=1) СОКИ. В этом случае рабочий числовой диапазон равен

$$M = \prod_{i=1}^{4} m_i = 3\cdot 4\cdot 5\cdot 7 = 420,$$

а полный диапазон равен

$$M_1 = M\, m_{n+1} = 420\cdot 11 = 4620.$$

Интервалы распределения ошибок представлены в табл. 2.

Таблица 2

Интервалы распределения ошибок

$[0,M_i)$, $i=\overline{0,10}$	γ_{n+1}	$[0,M_i)$, $i=\overline{0,10}$	γ_{n+1}
0 ÷ 419	0	2520 ÷ 2939	1
420 ÷ 839	2	2940 ÷ 3359	3
840 ÷ 1259	4	3360 ÷ 3779	5
1260 ÷ 1679	6	3780 ÷ 4199	7
1680 ÷ 2099	8	4200 ÷ 4619	9
2100 ÷ 2519	10		

Пусть необходимо провести контроль (проверить факт наличия или отсутствия ошибки) числа

$$A=A^{(0)} = (a_1^{(0)}, a_2^{(0)}, a_3^{(0)}, a_4^{(0)}, a_5^{(0)}) = (1,0,0,1,4),$$

представленного в МСС.

Для этого по значениям цифр $a_1^{(0)}=1$ и $a_4^{(0)}=1$ числа А выбираем из БН (см. табл. 3) константу нулевизации в виде $KH^{(1)}$ = ($t_{1,1}$, $t_{2,1}$, $t_{3,1}$, $t_{4,1}$, $t_{5,1}$), где $t_{1,1}=a_1^{(0)}=1$ и $t_{4,1}=a_4^{(0)}=1$. В этом случае с БН выбираем $KH^{(1)}$ = (1,1,1,1,1), табл. 3. Далее, в соответствии с предлагаемым методом ПНПВЦ, проводим операцию $A^{(1)} = A^{(0)} - KH^{(1)}$:

$$\begin{array}{rl} & A^{(0)} = (1,0,0,1,4) \\ - & KH^{(1)} = (1,1,1,1,1) \\ \hline & A^{(1)} = (0,3,4,0,3) \end{array}$$

и, одновременно по времени, для числа

$$A^{(1)} = = (0,3,4,0,3)$$

с БН выбираем

$$KH^{(2)} = (0, t_{2,2}, t_{3,2}, 0, t_{5,2}),$$

вида

$$a_2^{(1)} = t_{2,2} = 3 \text{ и } a_3^{(1)} = t_{3,2} = 4.$$

В этом случае (табл. 4) $KH^{(2)}$ определится в виде

$$KH^{(2)} = (0,3,4,0,3).$$

Далее определяем разность $A^{(1)} - KH^{(2)}$:

$$\begin{array}{rl} & A^{(1)} = (0,3,4,0,3) \\ - & KH^{(2)} = (0,3,4,0,3) \\ \hline & A^{(2)} = (0,0,0,0,0). \end{array}$$

Таким образом, получено нулевизированное число

$$A^{(2)} = A^{(H)} = (0,0,...,0,...,0,\gamma_{n+1}) = (0,0,0,0,\gamma_5),$$

где $\gamma_5 = 0$. Вывод: число $A^{(0)}$ = (1,0,0,1,4) не имеет ошибок (табл. 2).

Проверка: число $A^{(0)}$ в ПСС равняется $A^{(0)}$ = 400, т.е. находится в пределах рабочего числового [0,419) интервала.

Таблица 3

Блок нулевизации

ПСС	m_1=3, m_4=7
1	1,1,1,1,1
2	2,2,2,2,2
3	0,3,3,3,3
4	1,0,4,4,4
5	2,1,0,5,5
6	0,2,1,6,6
7	1,3,2,0,7
8	2,0,3,1,8
9	0,1,4,2,9
10	1,2,0,3,10
11	2,3,1,4,0
12	0,0,2,5,1
13	1,1,3,6,0
14	2,2,4,0,3
15	0,3,0,1,4
16	1,0,1,2,5
17	2,1,2,3,6
18	0,2,3,4,7
19	1,3,4,5,8
20	2,0,0,6,9

Таблица 4

Блок нулевизации

ПСС	m_2=4, m_3=5
21	0,1,1,0,10
84	0,0,4,0,7
105	0,1,0,0,6
42	0,2,2,0,9
63	0,3,3,0,8
126	0,2,1,0,5
147	0,3,2,0,4
168	0,0,3,0,3
189	0,1,4,0,2
252	0,0,2,0,10
273	0,1,3,0,9
210	0,2,0,0,1
231	0,3,1,0,0
294	0,2,4,0,8
315	0,3,0,0,7
336	0,0,1,0,6
357	0,1,2,0,5
378	0,2,3,0,4
399	0,3,4,0,3

Выводы

Суть метода контроля ошибок состоит в использовании процедуры парной нулевизации чисел с предварительной выборкой цифр. Практическая значимость полученных результатов состоит в том, что, по сравнению с существующим методом контроля ошибок в МСС, время обнаружения ошибок снижается более чем в два раза. Данное обстоятельство позволяет повысить общую эффективность использования МСС при создании СОКИ.

Список литературы

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

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

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

4. Материалы Международной научно-технической конференции "50 лет модулярной арифметике". МИЭТ, г. Зеленоград. Моск. обл. 23-25 ноября 2005г.

5. Акушский И.Я. Машинная арифметика в остаточных классах / И.Я. Акушский, Д.И. Юдицкий. – М.: Сов. радио, 1968. – 440 с.

6. Краснобаев В.А. Отказоустойчивые вычислительные системы на основе модулярной арифметики: концепции, методы и средства / В.А. Краснобаев, В.И. Барсов, Е.В. Яськова // Радіоелектронні і комп'ютерні системи. – 2007. – № 8 (27). – С. 82-90.

Поступила в редколлегию 22.08.2013

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

МЕТОД КОНТРОЛЮ КРИПТОГРАФІЧНОЇ ІНФОРМАЦІЇ, ЩО ПРЕДСТАВЛЕНА У МОДУЛЯРНІЙ СИСТЕМІ ЧИСЛЕННЯ

В.А. Краснобаєв, С.О. Кошман, В.Н. Курчанов, А.В. Гарамась

Пропонується метод контролю помилок у модулярній системі числення (МСЧ), заснований на використання процедури нулевізації. Суть запропонованого методу полягає в тому, що при здійсненні процедури нулевізації у МСЧ, поєднується в часі операція визначення, по цифрах $a_i^{(i-1)}$ і $a_{n-i+1}^{(i-1)}$ числа $A^{(i-1)}$, константи нулевізації $КН^{(i)}$ і операція обчислення за значеннями $a_i^{(i-1)}$ і $a_{n-i+1}^{(i-1)}$ наступних цифр $a_{i+1}^{(i)}$ та $a_{n-i}^{(i)}$ числа $A^{(i)}$. Це дає можливість підвищити оперативність контролю криптографічної інформації, що представлена у модулярній системі числення.

***Ключові слова**: модулярна система числення, контроль криптографічної інформації.*

METHOD FOR CONTROL OF CRYPTOGRAPHIC INFORMATION PROVIDED IN A MODULAR NUMBER SYSTEM

V.A. Krasnobaeyv, S.A. Koshman, V.N. Kurchanov, A.V. Haramas

Propose a method for error control in a modular number system (MNS) based on the use of the procedure of nullification. The essence of the proposed method consists in that in the procedure of nullification MNS combined time determination operation, the figures $a_i^{(i-1)}$ and $a_{n-i+1}^{(i-1)}$ number of $A^{(i-1)}$, constants nullification $CN^{(i)}$ and the operation of calculating the values $a_i^{(i-1)}$ and $a_{n-i+1}^{(i-1)}$ of the following figures $a_{i+1}^{(i)}$ and $a_{n-i}^{(i)}$ numbers $A^{(i)}$. This makes it possible to increase the efficiency of cryptographic control information presented in a modular number system.

***Keywords:** modular number system, control of cryptographic information.*