

МЕТОД ОБНАРУЖЕНИЯ ОШИБОК В СПЕЦПРОЦЕССОРЕ ОБРАБОТКИ КРИПТОГРАФИЧЕСКОЙ ИНФОРМАЦИИ

МАРТЫНЕНКО С. О., КРАСНОБАЕВ В. А.

Предлагается метод обнаружения ошибок в модулярной системе счисления (МСС), основанный на использовании процедуры нулевизации. Сущность 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 $KN^{(i)}$ 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 $A^{(i)}$.

1. Введение

Криптографические методы и алгоритмы (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).

2. Актуальность исследования

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 направлением 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.

3. Анализ существующих литературных источников

В настоящее время для обнаружения ошибок в МСС наиболее часто используется процедура нулевизации. Суть процедуры заключается в последовательном вычитании из исходного числа $A=(a_1, a_2, \dots, a_n, a_{n+1})$ некоторых минимальных чисел $KN^{(i)}$ — констант нулевизации таких, что число A последовательно за n тактов преобразуется в число вида $A^{(n)}=(0, 0, \dots, 0, \gamma_{n+1})$. Если полученное значение остатка по контрольному основанию $\gamma_{n+1} \neq 0$, то считается, что число A ошибочно. При этом константы нулевизации должны быть выбраны таким образом, чтобы при вычитаниях вида $A - KN^{(i)}$ не имел бы место выход числа из рабочего $[0, M)$ диапазона $[1-3]$. Существенным недостатком методов обнаружения ошибок в МСС является необходимость значительных временных и аппаратных затрат при реализации КП, что и обуславливает большие непроизводительные вычислительные затраты [4, 5].

Цель исследования — разработка и изучение высокопроизводительного метода коррекции ошибок в МСС, основанного на применении процедуры нулевизации.

4. Основная часть

Процедура нулевизации состоит из последовательности следующих операций.

1 этап. Исходное проверяемое число

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

последовательно приводится к виду $A^{(H)}=(0, 0, \dots, 0, 0, \gamma_{n+1})$ 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 ($KN^{(i)}$) вида

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

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

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

...

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

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

Далее, исходное проверяемое число

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

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

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

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

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

$$A^{(3)} = (0, 0, 0, a_4^{(3)}, \dots, a_n^{(3)}, a_{n+1}^{(3)})$$

и так далее.

Продолжая вычитания n раз, получаем значение

$$A^{(H)} = (0, 0, \dots, 0, a_{n+1}^{(n)}),$$

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

где $\gamma_{n+1} = a_{n+1}^{(n)}$. Общая схема вычитания $A^{(i)} = A^{(i-1)} - KN^{(i)}$ представлена в следующем виде:

$$A^{(i-1)} = (0, 0, \dots, 0, a_i^{(i-1)}, a_{i+1}^{(i-1)}, \dots, a_n^{(i-1)}, a_{n+1}^{(i-1)})$$

$$- KN^{(i)} = (0, 0, \dots, 0, a_i^{(i-1)}, t_{i+1,i}, \dots, t_{n,i}, t_{n+1,i})$$

$$A^{(i)} = [0, \dots, 0, [a_i^{(i-1)} - a_i^{(i-1)}] \bmod m_i, [a_{i+1}^{(i-1)} - t_{i+1,i}] \bmod m_{i+1}, \dots, [a_{n+1}^{(i-1)} - t_{n+1,i}] \bmod m_{n+1}],$$

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

Обозначив время выборки КН из соответствующего блока нулевизации (БН) СОКИ как t_1 , а время вычитания из числа $A^{(i-1)}$ константы $KN^{(i)}$, т.е. выполнения операции $A^{(i)} = A^{(i-1)} - KN^{(i)}$ – 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 $t_1 = t_2 = \tau_{\text{нб}}$. В этом случае для метода ОН время нулевизации равняется значению $T_{H1} = 2n \tau_{\text{нб}}$, где $\tau_{\text{нб}}$ – время вычитания из числа $A^{(i-1)}$ константы нулевизации $KN^{(i)}$; 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 A находится в диапазоне $[0, M)$), то делается вывод, что число A не искажено (правильное), т.е. ошибок нет. Если $\gamma_{n+1} \neq 0$ (число A не находится в диапазоне $[0, M)$), то число A искажено (неправильное), т.е. присутствует ошибка по одному из оснований (модулей) m_i МСС.

Общее время T_1 обнаружения ошибки определяется как $T_1 = T_{H1} + T_{c1}$, где T_{c1} – время сравнения значения γ_{n+1} с нулем. Практически время T_{c1} сравнения выполняется за один такт, в этом случае можно считать, что $T_1 \gg T_{H1} = 2n \tau_{\text{нб}}$.

Суть предлагаемого в статье метода обнаружения ошибок информации в МСС состоит в реализации процедуры парной нулевизации чисел с предварительной выборкой цифр (ПНПВЦ).

Суть процедуры ПНПВЦ состоит в том, что операция нулевизации в БН совмещается во времени с операци-

ей выбора с БКН по цифрам $a_i^{(i-1)}$ и $a_{n-i+1}^{(i-1)}$ числа $A^{(i-1)}$ константы $KN^{(i)}$ и операцией 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 то же время совмещаются во времени операция вычитания из числа $A^{(i-1)}$ константы нулевизации $KN^{(i)}$ (т.е., операция $A^{(i-1)} - KN^{(i)}$) и операция выбора очередной константы нулевизации:

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

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 проводиться обращение к БКН за следующей константой нулевизации:

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

Действительно, значения Δa_{i+1} и Δa_{n-i} , которые будут вычтены соответственно из $a_{i+1}^{(i)}$ и $a_{n-i}^{(i)}$, чтобы получить $a_{i+1}^{(i+1)}$ и $a_{n-i}^{(i+1)}$, определяются только значениями $a_i^{(i-1)}$ и $a_{n-i+1}^{(i-1)}$.

Количество тактов, свободных от сложения, во время которых производится обращение в БКН СОКИ и образование очередного адреса, равняется значению $[(n+1)/2]$, где $[x]$ – целое, ближайшее к x 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 каждого двух вычитаний требуется еще один дополнительный временной такт для образования очередного адреса и обращения к накопителю констант нулевизации. В связи с этим на каждые два такта сложения ($\tau_{\text{нб}} = \tau_0$) 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 (времени обнаружения ошибок, т.е. времени нулевизации) введём понятие коэффициента эффективности [5]:

$$K_{j \text{ вб}}^{(n)} = \frac{T_{H1}/\tau_{\text{нб}} - T_{Hj}/\tau_{\text{нб}}}{T_{H1}/\tau_{\text{нб}}} \cdot 100\%, \quad (1)$$

где j – номер метода нулевизации ($j=2$, для парной нулевизации; $j=3$, для парной нулевизации с предварительной выборкой цифр; $j=4$, для парной нулевизации чисел с предварительной выборкой цифр).

Выражение (1) может быть также представлено в упрощенном виде:

$$K_{j \text{ вб}}^{(n)} = \frac{T_{H1} - T_{Hj}}{T_{H1}} \cdot 100\%. \quad (2)$$

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

Полученные расчётные данные поместим в табл. 1.

Таблица 1

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

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

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

5. Пример технической реализации метода обнаружения ошибок в МСС

Приведем примеры 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 однобайтовый ($l=1$) СОКИ (см. рисунок, где 1 – информационный вход устройства; 2 – регистр хранения числа $A=(a_1, a_2, \dots, a_{n+1})$; 3 – управляющий вход устройства; 4 – блок нулевизации; 5 – первая группа элементов ИЛИ; 6₁-6₂ – блок констант нулевизации; 7 – вторая группа элементов ИЛИ; 8 – группа элементов И; 9 – блок анализа значения γ_{n+1} ; 10 – выход устройства).

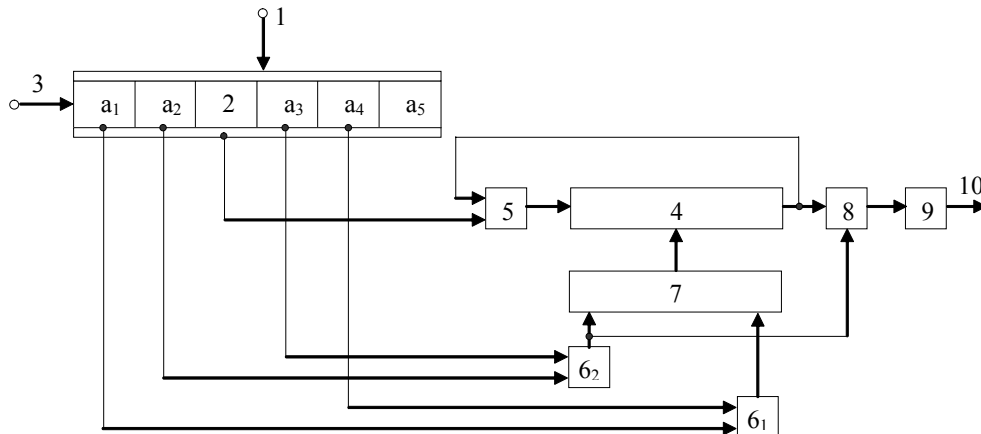
В этом случае рабочий числовой диапазон равен

$$M = \prod_{i=1}^4 m_i = 3 \cdot 4 \cdot 5 \cdot 7 = 420, \text{ а полный диапазон равен}$$

$$M_1 = M m_{n+1} = 420 \cdot 11 = 4620. \text{ Интервалы распределения ошибок представлены в табл. 2.}$$

Таблица 2

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



Устройство для обнаружения ошибок в МСС

Пример 1. Пусть надо проверить факт наличия или отсутствия ошибки, в числе в МСС $A=A^{(0)} = (a_1^{(0)}, a_2^{(0)}, a_3^{(0)}, a_4^{(0)}, a_5^{(0)}) = (1, 0, 0, 1, 4)$.

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

$$\begin{aligned} A^{(0)} &= (1, 0, 0, 1, 4) \\ - \quad КН^{(1)} &= (1, 1, 1, 1, 1) \\ \hline A^{(1)} &= (0, 3, 4, 0, 3) \end{aligned}$$

и, одновременно по времени, для числа $A^{(1)} = (0, 3, 4, 0, 3)$ с БН выбираем $КН^{(2)} = (0, t_{2,2}, t_{3,2}, 0, t_{5,2})$, вида $a_2^{(1)} = t_{2,2} = 3$ и $a_3^{(1)} = t_{3,2} = 4$. В этом случае (табл. 4) $КН^{(2)}$ определится в виде $КН^{(2)} = (0, 3, 4, 0, 3)$.

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

$$\begin{aligned} A^{(1)} &= (0, 3, 4, 0, 3) \\ - \quad КН^{(2)} &= (0, 3, 4, 0, 3) \\ \hline A^{(2)} &= (0, 0, 0, 0, 0). \end{aligned}$$

Таким образом, получено нулевизированное число $A^{(2)} = A^{(H)} = (0, 0, \dots, 0, \dots, 0, \gamma_{n+1}) = (0, 0, 0, 0, \gamma_5)$, 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.

Пример 2. Пусть необходимо проверить число

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

на наличие ошибки (табл. 3). В соответствии с методом ПНПВЦ определяем значение $A^{(1)} = A^{(0)} - КН^{(1)}$:

$$\begin{aligned} A^{(0)} &= (1, 1, 0, 1, 4) \\ - \quad КН^{(1)} &= (1, 1, 1, 1, 1) \\ \hline A^{(1)} &= (0, 0, 4, 0, 3). \end{aligned}$$

Таблица 3

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

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

Для полученного числа $A^{(1)}$ из БН СОКИ выбираем константу $KN^{(2)} = (0,0,4,0,7)$, для $a_2^{(1)} = t_{2,2} = 0$ и $a_3^{(1)} = t_{3,2} = 4$ (табл. 4).

Определяем $A^{(2)} = A^{(1)} - KN^{(2)}$:

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

$$- \quad KN^{(2)} = (0,0,4,0,7)$$

$$A^{(2)} = (0,0,0,0,7).$$

Таким образом, $A^{(2)} = A^{(H)} = (0,0,0,0,7)$, т.е. $\gamma_5 = 7$ ($\gamma_5 \neq 0$) (табл. 2). Вывод: число $A^{(0)} = (1,1,0,1,4)$ имеет ошибку по одному из оснований m_i ($i = \overline{1,4}$) МСС.

Проверка: число $A^{(0)}$ в ПСС равняется значению $A^{(0)} = 3865 > 420$ (табл. 2).

6. Выводы

Научная новизна полученных результатов исследований состоит в разработке метода обнаружения оши-

бок в информации в МСС. Сущность предложенного метода обнаружения ошибок состоит в использовании процедуры парной нулевизации чисел с предварительной выборкой цифр.

Практическая значимость полученных результатов состоит в том, что более чем в два раза, по сравнению с существующим методом коррекции ошибок, снижается время обнаружения ошибок в СОКИ, функционирующего в МСС.

Литература: 1. Барсов В.И., Краснобаев В.А., Сиора А.А., Авдеев И.В. Методы многоверсионной обработки информации в модулярной арифметике: Монография. Харьков: МОН, УИПА, 2008. 460с. 2. 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. Харьков: УИПА, 2008. 147с. 3. Барсов В.И., Краснобаев В.А., Фурман И.А., Малиновский М.Л., Шевченко В.В. Система обработки информации и управления АСУ ТП на основе применения кодов в модулярной арифметике: Монография. Харьков: МОН, УИПА, 2009. 159с. 4. Сиора А.А., Краснобаев В.А., Харченко В.С. Отказоустойчивые системы с версионно-информационной избыточностью в АСУ ТП: Монография. Харьков: МОН, НАУ им. Н.Е. Жуковского (ХАИ), 2009. 320с. 5. Барсов В.И., Сорока Л.С., Краснобаев В.А. Методология параллельной обработки информации в модулярной системе счисления: Монография. Харьков: МОН, УИПА, 2009. 268с.

Поступила в редколлегию 03.12.2009

Рецензент: д-р техн. наук, проф. Стасев Ю.В.

Мартыненко Сергей Олегович, инженер-программист ООО "Телерадиосвязь", г. Харьков. Научные интересы: создание спецпроцессора быстрой и достоверной обработки криптографической информации в реальном времени на основе использования модулярной системы счисления. Адрес: Украина, 61103, Харьков, ул. 23 августа, 25, кв. 9, тел. 740-00-00.

Краснобаев Виктор Анатольевич, д-р техн. наук, профессор кафедры автоматизации и компьютерных технологий Харьковского национального технического университета сельского хозяйства им. Петра Василенко. Научные интересы: теоретическое обоснование и практическое создание быстродействующих и отказоустойчивых вычислительных структур в модулярной системе счисления. Адрес: Украина, 61052, Харьков, ул. Кацарская, 9, тел. 712-35-37.