УДК 621.391

М.В. Дугин, В.А. Краснобаев

Харьковский национальный технический университет сельского хозяйства им. Петра Василенка, Харьков

МЕТОД КОНТРОЛЯ И КОРРЕКЦИИ ОШИБОК КРИПТОГРАФИЧЕСКОЙ ИНФОРМАЦИИ НА ОСНОВЕ ИСПОЛЬЗОВАНИЯ КЛАССА ВЫЧЕТОВ

В статье рассматривается метод контроля и коррекции ошибок криптографической информации на основе использования непозиционной системы счисления в классе вычетов (КВ). Использования непозиционных кодовых структур в КВ позволяет создать эффективную систему контроля и коррекции ошибок криптографической информации. Существенное отличие системы контроля и коррекции от известной в двоичной позиционной системе счисления состоит в аппаратной и временной простоте процедуры контроля и коррекции ошибок.

***Ключевые слова**: позиционная система счисления, контроль и коррекция ошибок информации, непозиционная система счисления в классе вычетов, криптографическая информация, система цифровой обработки криптографической информации.*

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 существующих и перспективных электронных информационных технологий – электронного документооборота, электронных денег, тайного электронного голосования и пр. Характерным для современных технологических применений криптографических технических средств (embedded processor, processor node) реализации КП является существенное возрастание требований к скорости обработки КП, надежности и их функционирования и к достоверности вычислений. Так, например, для КП в группе точек эллиптических кривых, при вычислении порядка эллиптической кривой над полем размерностью 160 бит необходимое время равно 9с. Для поля в 240 бит – 25с, для поля в 500 бит – 5 мин., для поля в 1000 бит – 1 час, для поля 2000 бит – 14 часов (вычисления КП производились с помощью процессора PENTIUM с тактовой частотой 500 МГц). Возрастание, например, порядка RSA криптосистемы или поля эллиптической кривой вычислительная сложность КП существенно возрастает [1].

Основной материал

Исходя из вышеизложенного, очевидна актуальность и важность исследований, посвященных поискам путей повышения производительности и достоверности обработки цифровой целочисленной (криптографической) информации.

Известно [2, 3], что использования непозиционной системы счисления класса вычетов (КВ) позволяет улучшить такие характеристики систем цифровой обработки криптографической информации (СЦОИ), как пользовательская производительность, надежность и отказоустойчивость при решении определенного класса задач (для определенного типа операций). В предлагаемой статье рассматривается метод контроля и коррекции ошибок дискретной целочисленной информации в СЦОИ посредством применения кодов КВ.

Известно, что [3] в КВ произвольный операнд А представляется в виде набора остатков $\{a_i\}$ от последовательного деления его на совокупность $\{m_i\}$ натуральных чисел, называемыми модулями или основаниями КВ. В этом случае число А в позиционной системе счисления (ПСС) представится в КВ следующим виде:

$$A_{KB} = [A(\mathrm{mod}\ m_1), A(\mathrm{mod}\ m_2),\ldots, A(\mathrm{mod}\ m_n)]$$

или

$$A_{KB} = (a_1, a_2,..., a_n),$$

где $a_i \equiv A(\mathrm{mod}\ m_i)$.

Диапазон представимых чисел в данном КВ определяется как (0, M], где $M = [\ m_1, m_2,\ldots,m_n\ ]$ – НОК оснований КВ. Метод контроля и коррекции основывается на результатах доказательств следующих теорем.

Для контроля и обнаружения исправления ошибок информации в КВ рассмотрим теоремы 1 и 2.

Первая теорема. Для любого целого числа A_{KB}, заданного в КВ с основаниями $\{m_i\}$, $i = \overline{1,n}$ и для любой пары оснований m_i, m_j ($i,j = \overline{1,n}$; $i \neq j$) должно выполнятся следующее условие

$(a_i - a_j) \bmod d_{ij} = 0$,

где $d_{ij} = (m_i, m_j)$ – НОД оснований m_i и m_j.

Вторая теорема. Для обнаружения ошибки в остатке по произвольному основанию m_i числа A_{KB}, заданного в КВ совокупностью оснований $\{m_i\}$,

$i = \overline{1,n}$, необходимо, чтобы произвольное основание m_i имело хотя бы один, отличный от единицы, общий делитель с каждым из остальных оснований m_j ($j = \overline{1,n}$; $j \neq i$).

Для исправления ошибок в КВ воспользуемся доказательством следующей теоремы.

Третья теорема. Для исправления ошибки в остатке по произвольному основанию m_i ($i = \overline{1,n}$) числа $A_{КВ}$, заданного в КВ основаниями $\{m_i\}$, необходимо выполнение следующего условия:

$$(d_{ik} - 1) \cdot (d_{ij} - 1) \geq \delta(\Delta a_i),$$

где $\delta(\Delta a_i) = m_i - 1 - (K_{d_{ik}} + K_{d_{ij}} - K_{[d_{ik}, d_{ij}]})$.

При этом $K_{d_{ik}}$ – число возможных делителей значения ошибки Δa_i по основанию m_i, кратных значению d_{ik}; $K_{d_{ij}}$ – число возможных делителей значения ошибки Δa_i по основанию m_i, кратных значению d_{ij}; $K_{[d_{ik}, d_{ij}]}$ – число возможных делителей ошибки Δa_i по основанию m_i, кратных значению НОК чисел d_{ik}, d_{ij}.

Условие третьей теоремы является и достаточным, если различным возможным значениям $\delta(\Delta a_i)$ ошибок соответствуют различные пары величин a_{ik}, a_{ij}.

На основании вышеприведенных теорем построим алгоритмы контроля, обнаружения и исправления однократных (по одному из оснований КВ) ошибок.

1. Алгоритмы контроля и обнаружения ошибок

Алгоритм 1. Пусть необходимо проверить факт наличия ошибок в операнде $A_{КВ} = (a_1, a_2, \ldots, a_n)$.

1. Определим следующую совокупность значений

$$\begin{cases} a_{12} = (a_1 - a_2) \bmod d_{12}, \\ a_{13} = (a_1 - a_3) \bmod d_{13}, \\ \quad . \quad . \quad . \\ a_{1n} = (a_1 - a_n) \bmod d_{1n}. \end{cases}$$

Если вся совокупность значений a_{1i} ($i = \overline{1,n}$; $i \neq 1$) равно нулю, то далее вычисляется и проверяется совокупность значений

$a_{2i} = (a_2 - a_1) \bmod d_{2i} (i \neq 2)$ и т.д.

2. При получении всех возможных значений a_{ij} ($j \neq j$) составляем матрицу G вида

$$G = \begin{vmatrix} a_{12} & a_{13} & \ldots & a_{1n} \\ a_{21} & a_{23} & \ldots & a_{2n} \\ \vdots & & & \vdots \\ a_{n1} & a_{n2} & \ldots & a_{nn} \end{vmatrix}.$$

При составлении матрицы G нет необходимости указывать истинное числовое значение элементов a_{ij}, а достаточно представить элементы матрицы в виде единицы или нуля, т.е.

$$a_{ij} = \begin{cases} 0, \text{при } a_{ij} = 0, \\ 1, \text{при } a_{ij} \neq 0. \end{cases}$$

3. Если определитель $|G| = 0$, то $A_{КВ}$ считается неискаженным, а если $|G| \neq 0$ - число $A_{КВ}$ искажено.

Если воспользоваться соотношением

$$(a_i - a_j) \equiv [d_{ij} - (a_j - a_i)] \bmod d_{ij},$$

то для определения правильности или неправильности операнда А достаточно определить лишь следующую совокупность чисел:

$$a_{12}, a_{23}, a_{34}, \ldots, a_{n-1n}, a_{n1}.$$

Алгоритм 2. Приведем некоторые соображения, позволяющие упростить вышеприведенный алгоритм обнаружения ошибок. Покажем, что

$$[(a_1 + \overline{a_j}) + (\overline{a_1} + a_j)] \equiv 0 \pmod{d_{1j}},$$

где: $\overline{a_j} = m_j - a_j$; $\overline{a_1} = m_1 - a_1$.

Пусть в операнде $A_{КВ} = (a_1, a_2, \ldots, a_j, \ldots, a_n)$ искажен остаток a_j по основанию m_j, т.е.

$$\tilde{a}_j = (a_j + \Delta a_j) \bmod m_j.$$

Запишем очевидную систему следующих равенств

$$\begin{cases} K_1 = a_i - \tilde{a}_j = a_i + (m_j - \tilde{a}_j) = a_i + m_j - a_j - \Delta a_j; \\ K_2 = \tilde{a}_j - a_i = a_j + \Delta a_j - a_i = a_j - a_i + \Delta a_j. \end{cases}$$

Сложив эти два равенства, получим:

$$K_1 + K_2 = m_j$$

или

$$K_1 + K_2 \equiv 0 \pmod{m_j}.$$

Таким образом, очевидно, что

$$a_1 + \overline{a}_j = d_{1j} - (\overline{a}_1 + a_j),$$

т.е. для определения факта наличия или отсутствия ошибок нет необходимости вычисления точного значения величины $(a_1 + \overline{a}_j) \bmod d_{1j}$, а достаточно знать факт равенства или неравенства этого значения нулю.

Это в свою очередь позволит в техническом устройстве для контроля ошибок в классе вычетов вместо (n – 1) – го сумматоров по модулям m_j ($j = \overline{2,n}$), которые определяют совокупность значений $\overline{a}_j = m_j - a_j$, использовать всего один сумматор по модулю m_1, определяющий значение $\overline{a}_1 = m_1 - a_1$.

2. Алгоритм коррекции ошибок

1. Определим все возможные значения вида $a_{i,i+1} = (a_1 - a_{i+1}) \bmod d_{i,i+1}$:

$$\begin{cases} a_{12} = (a_1 - a_2) \bmod d_{12}, \\ a_{23} = (a_2 - a_3) \bmod d_{23}, \\ \quad \dots \\ a_{n-1,n} = (a_{n-1} - a_n) \bmod d_{n-1,n}, \\ a_{n1} = (a_n - a_1) \bmod d_{n1}. \end{cases}$$

2. Если вся совокупность значений принимает нулевое значение, то ошибка отсутствует, либо она кратна одному из делителей $d_{i-1,i}, d_{i,i+1}$, что противоречит условию ограничения класса возможных корректируемых ошибок. Таким образом, считается, что ошибка отсутствует.

3. Если одновременно выполняются условия $a_{i-1,i} \neq 0$ и $a_{i,i+1} \neq 0$, а все остальные значения в совокупности принимают значения ноль, то считается, что ошибка имеется в остатке по модулю m_i, т.е.

$$\tilde{a}_i = (a_i + \Delta a_i) \bmod m_i (0 < \Delta a_i \le m_{i-1}).$$

4. В соответствии с известным алгоритмом производится коррекция ошибок по i–у основанию КВ.

На основании рассмотренного метода разработан класс устройств для контроля и коррекции ошибок криптографической информации в КВ [4 – 7]. Кратко рассмотрим обобщенный алгоритм контроля и коррекции ошибок.

Пусть дан КВ с основаниями

$$m_1 = 4, m_2 = 6, m_3 = 12.$$

Совокупность кодовых слов представлена в табл. 1. В этом случае НОК значений 4, 6 и 12 равно $M = [4, 6, 12] = 12$.

Определим следующее значение НОД:

$d_{12} = (4, 6) = 2$; $d_{23} = (6, 12) = 6$; $d_{31} = (4, 12) = 4$;

$\delta(\Delta a_1) = 2$ (табл. 2); $\delta(\Delta a_2) = 3$ (табл. 3);

$\delta(\Delta a_3) = 8$ (табл. 4).

Таблица 1

Совокупность кодовых слов

$A_{ПСС}$	Кодовые числа		
	$A_{КВ}$		
	m_1	m_2	m_3
0000	00	000	0000
0001	01	001	0001
0010	10	010	0010
0011	11	011	0011
0100	00	100	0100
0101	01	101	0101
0110	10	000	0110
0111	11	001	0111
1000	00	010	1000
1001	01	011	1001
1010	10	100	1010
1011	11	101	1011

Таблица 2

Значения $\Delta\bar{a}_1$

a_{31}	$a_{12}=1$
1	$\Delta\bar{a}_1=1$
2	—
3	$\Delta\bar{a}_1=3$

Таблица 3

Значения $\Delta\bar{a}_2$

a_{23}	$a_{12}=1$
1	$\Delta\bar{a}_2=5$
2	—
3	$\Delta\bar{a}_2=3$
4	—
5	$\Delta\bar{a}_2=1$

Таблица 4

Значения $\Delta\bar{a}_3$

a_{31}	a_{23}				
	1	2	3	4	5
1	$\Delta\bar{a}_3=7$	—	$\Delta\bar{a}_3=3$	—	$\Delta\bar{a}_3=11$
2	—	$\Delta\bar{a}_3=2$	—	$\Delta\bar{a}_3=10$	—
3	$\Delta\bar{a}_3=1$	—	$\Delta\bar{a}_3=9$	—	$\Delta\bar{a}_3=5$

Пусть искажено правильное число

$$A_{КВ} = (11, 001, 0111)$$

по основанию m_2.

В этом случае на вход системы контроля и коррекции подается операнд вида $\tilde{A}_{кв} = (11, 100, 0111)$. Необходимо определить правильность числа $\tilde{A}_{кв}$ и при необходимости провести его коррекцию. В этом случае операнд $\tilde{A}_{кв}$ записывается в первый и второй входные регистры. На выходах соответствующих сумматоров первой группы по модулям $m_1 \div m_3$ получим инвертированные значения соответствующих остатков $\bar{a}_i = m_i - a_i (i = \overline{1,3})$. На выходах сумматоров второй группы получим такие значения:

$(a_3 + \bar{a}_1) \bmod d_{31} = 0000$;

$(a_1 + \bar{a}_2) \bmod d_{12} = 001$;

$(a_2 + \bar{a}_3) \bmod d_{23} = 0011$,

которые через соответствующие дешифраторы в унитарном коде поступают на соответствующие входы коммутаторов.

Коммутаторы определяют значения $\delta(\Delta a_i)$ ошибок, соответствующие табл. 2, 3 и 4. В этом случае только на выходе второго (табл. 3) коммутатора имеется ненулевое значение (это факт наличия ошибки в операнде $\tilde{A}$кв), которое поступает через второй шифратор (который преобразует его в двоичный код) на первый вход сумматора по модулю m_2. На второй вход этого сумматора с выхода второ-

го регистра поступает значение искаженного остатка $\bar{a}_2 = 100$. С выхода сумматора по модулю m_2 в выходной регистр поступит значение исправленного остатка

$$(\tilde{a}_2 + \overline{\Delta a_2}) \bmod m_2 = (a_2 + \Delta a_2) + (m_2 - \Delta a_2) = \\ = a_2 (\bmod m_2) = 001.$$

В этом случае в выходном регистре устройства содержится исправленный операнд

$$A_{KB} = (11, 001, 0111).$$

Выводы

Таким образом, в статье предложен метод контроля и коррекции ошибок криптографической информации, основанный на использовании непозиционных кодовых структур КВ. В соответствии с рассмотренным методом разработаны алгоритмы обнаружения и исправления ошибок в СЦОИ, на основании которых разработаны патентоспособные технические устройства. Использование этих устройств в СЦОИ показали высокую эффективность применения непозиционного кодирование информации в КВ.

Исходя из вышеизложенного очевидно, что посредством предлагаемого метода кодирования информации в КВ исключительно просто реализуется процесс контроля и коррекции ошибок криптографической информации. При этом время контроля и коррекции ошибок составляет четыре условных временных такта и постоянно для любого числа оснований КВ.

Список литературы

1. Краснобаев В.А. Методы реализации криптографических RSA преобразований на основе использования модулярной системы счисления / В.А. Краснобаев, С.О. Мартыненко, Л.С. Сорока // Вісник ХНУ ім. В. Н. Каразіна. Серія "Математичне моделювання. Інформаційні технології. Автоматизовані системи управління". – Х.: ХНУ ім. В.Н. Каразіна, 2010. – № 890. – С. 132-144.

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. ДП на корисну модель № 49711 України, МПК (2009.01) G 06 F 11/08 Горбенко І.Д., Мартиненко С.О., Замула О.А., Краснобаєв В.А., Горбенко Ю.І. Спосіб виявлення помилок у системі обробки цифрової інформації, що функціонує у модулярній системі числення. № и 2009 11295. Заявл. 06.11.2009. Опубл. 11.05.2010, Бюл. № 9. – 4 с.

5. ДП на корисну модель № 42463 України, МПК (2009) G 06 F 11/08 Барсов В.І., Сіора О.А., Краснобаєв В.А., Хері А.А. Пристрій для виявлення помилок в модулярній системі числення. № и 2008 15296. Заявл. 30.12.2008. Опубл. 10.07.2009, Бюл. № 13. – 8 с.

6. ДП на корисну модель № 49054 України, МПК (2009.01) G 06 F 11/08 Горбенко І.Д., Мартиненко С.О., Замула О.А., Краснобаєв В.А., Горбенко Ю.І., Дейнеко Ж.В. Пристрій для виявлення помилок у модулярній системі числення. № и 2009 12062. Заявл. 24.11.2009. Опубл. 12.04.2010, Бюл. № 7. – 10 с.

7. ДП на корисну модель № 47563 України, МПК (2009.01) G 06 F 11/08 Мартиненко С.О., Кошман С.О., Барсов В.І., Краснобаєв В.А., Сорока Л.С. Пристрій для виявлення та виправлення помилок у модулярній системі числення. № и 2009 09006. Заявл. 31.08.2009. Опубл. 10.02.2010, Бюл. № 3. – 6 с.

Поступила в редколлегию 4.06.2010

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

МЕТОД КОНТРОЛЮ І КОРЕКЦІЇ ПОМИЛОК КРИПТОГРАФІЧНОЇ ІНФОРМАЦІЇ НА ОСНОВІ ВИКОРИСТАННЯ КЛАСУ ВИРАХУВАНЬ

М.В. Дугін, В.А. Краснобаєв

У статті розглядається метод контролю і корекції помилок криптографічної інформації на основі використання непозиційної системи числення в класі вирахувань (КВ). Використання непозиційних кодових структур в КВ дозволяє створити ефективну систему контролю і корекції помилок криптографічної інформації. Істотна відмінність системи контролю і корекції від відомої в двійковій позиційній системі числення полягає в апаратній і тимчасовій простоті процедури контролю і корекції помилок.

***Ключові слова**: позиційна система числення, контроль і корекція помилок інформації, непозиційна система числення в класі вирахувань, криптографічна інформація, система цифрової обробки криптографічної інформації.*

METHOD OF CONTROL AND CORRECTION OF ERRORS OF CRYPTOGRAPHIC INFORMATION ON BASIS OF THE USE OF CLASS OF DEDUCTIONS

M.B. Dugin, B.A. Краснобаев

In the article the method of control and correction of errors of cryptographic information is examined on the basis of the use of unbase notation in a class deductions (CD). Uses of structures of codes of unpositions in CD allows to create the effective checking and correction of errors of cryptographic information system. The substantial difference of the checking and correction system om known in binary base notation consists of instrument room and temporal simplicity of procedure of control and correction of errors.

***Keywords**: base notation, control and correction of errors of information, unbase notation in a class deductions, cryptographic information, system of digital treatment of cryptographic information.*