УДК 004.052.2

РАЗРАБОТКА МЕТОДА ВЫЧИСЛЕНИЯ ДИНАМИЧЕСКИ ИЗМЕНЯЕМОГО КОРТЕЖА ОРТОГОНАЛЬНЫХ БАЗИСОВ, ПОЗВОЛЯЮЩЕГО ПОВЫСИТЬ ОТКАЗОУСТОЙЧИВОСТЬ СИСТЕМЫ ОПОЗНАВАНИЯ СПУТНИКА

Калмыков И.А., Степанова Е.П., Калмыкова Н.И., Павлюк Д.Н., Слюсарев Г.В.
ФГАОУ ВО «Северо-Кавказский федеральный университет», Ставрополь, e-mail: kia762@yandex.ru

Использование систем «свой – чужой» в низкоорбитальных системах спутниковой связи является одним из эффективных способов повышения из информационной скрытности. В этом случае спутник-нарушитель не сможет навязать приемнику несанкционированный контент. Одним из способов, позволяющим повысить производительность выполнения аутентификации спутника, является использование параллельных алгебраических систем. Для достижения этой цели можно использовать полиномиальные модулярные коды (ПМК). Особенностью кода ПМК является возможность проведения параллельных вычислений на уровне арифметических операций с использованием малоразрядных остатков. При этом полиномиальные модулярные коды обладают возможностью повышения отказоустойчивости системы опознавания «свой – чужой». Так как остатки кода несут информацию обо всём числе, представленном в ПМК, то существует возможность сохранять работоспособное состояние запросно-ответной системы при возникновении потока отказов за счет снижения в допустимых пределах основных показателей качества функционирования. Однако изменение количества работоспособных вычислительных каналов, соответствующих основаниям ПМК, требует пересчета ортогональных базисов для выполнения обратного преобразования из полиномиальных модулярных кодов в позиционный код. Поэтому разработка метода вычисления динамически изменяемого кортежа ортогональных базисов ПМК является актуальной задачей.

Ключевые слова: отказоустойчивая система опознавания спутника, полиномиальные модулярные коды, метод вычисления динамически изменяемого кортежа ортогональных базисов

DEVELOPMENT OF A METHOD FOR CALCULATING A DYNAMICALLY CHANGEABLE ORTHOGONAL BASIS TORTURE, ALLOWING TO INCREASE THE FAILURE RESISTANCE OF THE SATELLITE RECOGNITION SYSTEM

Kalmykov I.A., Stepanova E.P., Kalmykova N.I., Pavlyuk D.N., Slyusarev G.V.
Federal State Autonomous Educational Institution of Higher Professional Education «North-Caucasian Federal University», Stavropol, e-mail: kia762@yandex.ru

The use identification-friend-or-foe systems in low-orbit satellite communications systems is one of the effective ways to increase information security. In this case, the intruder satellite will not be able to impose unauthorized content on the receiver. One way to improve satellite authentication performance is to use parallel algebraic systems. To achieve this, polynomial modular codes (PMC) can be used. A feature of the PMC code is the ability to perform parallel calculations at the level of arithmetic operations using low-bit residuals. Moreover, the PMC codes have the ability to increase the fault tolerance of the friend-or-foe recognition system. Since the remnants of the code carry information about the entire number presented in the PMC, it is possible to maintain a healthy state of the system of the interrogation-response system when a flow of failures occurs due to a decrease in the acceptable limits of the main indicators of the quality of functioning. However, a change in the number of workable computing channels corresponding to the PMC bases requires the recalculation of orthogonal bases to perform the inverse transformation from the PMC to the positional code. Therefore, the development of a method for calculating a dynamically changing tuple of orthogonal bases is an urgent task.

Keywords: fault-tolerant satellite identification system, polynomial modular codes, method for calculating a dynamically changing tuple of orthogonal bases

В последние годы разработчики проектов, связанных с глобальным освоением территорий Российской Федерации, расположенных за Полярным кругом, особое внимание уделяют низкоорбитальным системам спутниковой связи (НССС). Это связано с тем, что только НССС способны обеспечить обмен данными между абонентами, которые находятся в районах Крайнего Севера [1]. При этом современные низкоорбитальные системы спутниковой связи должны иметь высокую помехозащищенность, которая базируется на информационной, структурной и энергетической скрытностях. В работах [2, 3] показано, что использование систем опознавания спутника «свой – чужой» позволяет повысить информационную скрытность НССС. При этом построение протокола аутентификации на основе параллельных вычислений с применением полиномиальных модулярных кодов (ПМК) обеспечивает сокращение времени необходимого на вычисление статуса спутника. Кроме того, ПМК позволяют системам опознавания сохранять работоспособное состояние при выходе из строя нескольких вычислительных трак-

тов. Но при этом необходимо пересчитывать значения ортогональных базисов, которые применяются в Китайской теореме об остатках (КТО) при выполнении обратного перевода из ПМК в позиционную систему счисления (ПСС). Поэтому разработка метода вычисления динамически изменяемого кортежа ортогональных базисов является актуальной задачей.

Применение полиномиальных модулярных кодов в системах опознавания «свой – чужой» позволяет решить следующие задачи. Во-первых, это повышение производительности проверки статуса спутника за счет применения параллельных методов вычислений [3]. Во-вторых, это повышение отказоустойчивости путем коррекции ошибок в процессе функционирования за счет введения избыточности в ПМК. В-третьих, это возможность системы опознавания сохранять работоспособное состояние при выходе из строя нескольких вычислительных трактов за счет перераспределения оставшихся вычислительных ресурсов. Но при реконфигурации системы опознавания, реализованной с использованием ПМК, необходимо производить пересчет ортогональных базисов для работоспособных оснований. Цель исследования – разработать метод вычисления динамически изменяемого кортежа ортогональных базисов, применение которого позволит обеспечить сохранение работоспособного состояния системы опознавания при постепенной деградации основных показателей в заданных пределах.

Материалы и методы исследования

Полиномиальные модулярные коды являются непозиционными кодами, в которых числа A, представленные в виде многочленов $A(x)$, задаются кортежем остатков [4]. То есть в виде

$$A(x) = (a_1(x), a_2(x), ..., a_k(x)), \quad (1)$$

где $a_i(x) \equiv A(x) \bmod m_i(x)$; $m_1(x), m_2(x), ..., m_k(x)$ – основания ПМК, в качестве которых выбираются неприводимые многочлены; $i = 1, 2, ..., k$.

Произведение кортежа оснований дает рабочий диапазон

$$\hat{M}(x) = \prod_{i=1}^{k} m_i(x). \quad (2)$$

Использование ПМК позволяет осуществлять параллельные вычисления согласно

$$Y(x) \oplus Z(x) = (\left| y_1(x) \circ z_1(x) \right|_{p_1(x)}, ..., \left| y_k(x) \circ z_k(x) \right|_{p_k(x)}), \quad (3)$$

где $Z(x) \equiv z_i(x) \bmod p_i(x)$; $\circ$ – операции модульного сложения и умножения.

В работе [3] был представлен протокол аутентификации спутника, который использует полиномиальные модулярные коды. В работе показано, что это позволило сократить временные затраты на проверку статуса спутника. Но согласно [4] полиномиальные модулярные коды могут повысить отказоустойчивость устройства. Чтобы исправить ошибку, возникшую в одном остатке, необходимо два контрольных модуля

$$\deg m_{k-1}(x) + \deg m_k(x) \le \deg m_{k+1}(x) + \deg m_{k+2}(x). \quad (4)$$

Однако в процессе длительного использования отказы в системе опознавания могут накапливаться. С целью противодействия такой последовательности отказов ПМК предлагают провести отключение отказавших вычислительных трактов (оснований). В этом случае динамически изменяется кортеж оснований ПМК, а это требует вычисления новых значений ортогональных базисов. При этом наибольшие сложности связаны с вычислением веса ортогонального базиса $g_i(z)$.

Известно, что обратное преобразование ПМК-ПСС реализуется на основе КТО

$$A(x) = \sum_{i=1}^{k+r} a_i(x) B_i(x) \bmod M(x), \quad (5)$$

где $B_i(x)$ – ортогональный базис; $M(x) = \prod_{i=1}^{k+r} m_i(x) = \hat{M} \prod_{i=k+1}^{r} m_i(x)$ – полный диапазон ПМК.

При этом ортогональные базисы определяются следующим образом:

$$B_i(x) = g_i(x) \frac{M(x)}{m_i(x)} = g_i(x) M_i(x), \quad (6)$$

где $g_i(z)$ – вес базиса $B_i(x)$; $i = 1, 2, ..., k + r$; r – количество контрольных оснований.

Значение $M_i(x)$ достаточно просто вычисляется для любого кортежа оснований. При этом необходимо определить вес ортогонального базиса $g_i(x)$ для выполнения условия

$$B_i(x) \equiv 1 \bmod m_i(x). \quad (7)$$

В работе [5] для вычисления динамически изменяемого кортежа ортогональных базисов предлагается сначала определить значение

$$M_i \equiv \frac{\hat{M}}{m_i} = \prod_{\substack{j=1 \\ j \neq i}}^{k+r} m_i \ . \quad (8)$$

После этого реализуется выражение для вычисления остатка

$$\delta_i \equiv M_i \bmod m_i \ , \quad (9)$$

с помощью которого определяется мультипликативно обратный элемент – вес базиса:

$$g_i \equiv \delta_i^{-1} \bmod m_i \ , \quad (10)$$

Проведенный анализ показал, что этот метод требует значительных вычислительных затрат. Устранить данный недостаток позволяет разработанный метод пересчета базисов.

Если решить, что ортогональный базис можно вычислить, используя равенство

$$B_i(x) \equiv g_i(x) \prod_{\substack{j=1 \\ i \neq j}}^{k+r} m_j(x), \quad (11)$$

то справедливо выражение

$$g_i(x) \prod_{\substack{j=1 \\ i \neq j}}^{k+r} m_j(x) \equiv 1 \bmod m_i(x). \quad (12)$$

Разделим обе стороны последнего равенства на константу $M_i(x) = \prod_{\substack{j=1 \\ i \neq j}}^{k+r} m_j(x)$. Тогда

$$g_i(x) = \frac{1}{M_i(x)} \bmod m_i(x) = \frac{1}{\prod_{\substack{j=1 \\ i \neq j}}^{k+r} m_j(x)} \bmod m_i(x). \quad (13)$$

Так как в модулярных полиномиальных кодах основаниями являются взаимно простые неприводимые многочлены, то вес ортогонального базиса будет определяться

$$g_i(x) = \left(\prod_{\substack{j=1 \\ i \neq j}}^{k+r} g_j^i(x) \right) \bmod m_i(x). \quad (14)$$

где $g_j^i(x) = m_j(x)^{-1} \bmod m_i(x)$; $i = 1, 2, ..., k+r$.

Результаты исследования и их обсуждение

Рассмотрим разработанный метод, используя $p_1(x) = x^5 + x^2 + 1$, $p_2(x) = x^5 + x^3 + 1$, $p_3(x) = x^5 + x^3 + x^2 + x + 1$, $p_4(x) = x^5 + x^4 + x^2 + x + 1$, $p_5(x) = x^5 + x^4 + x^3 + x + 1$, $p_6(x) = x^5 + x^4 + x^3 + x^2 + 1$. В таблице приведены константы $g_j^i(x) = p_j(x)^{-1} \bmod p_i(x)$.

Пусть кортеж ПМК состоит из полиномов $m_1(x) = x^5 + x^2 + 1$, $m_2(x) = x^5 + x^3 + 1$, $m_3(x) = x^5 + x^3 + x^2 + x + 1$, $m_4(x) = x^5 + x^4 + x^3 + x + 1$, $m_5(x) = x^5 + x^4 + x^3 + x^2 + 1$.

Вычислим вес ординального базиса $B_1(x)$. Для этого необходимо найти произведение констант, которые располагаются в первом столбце таблицы. Тогда получаем

$$g_1^{12345}(x) = \left| (x^2 + x + 1)(x^4 + x^3 + 1)(x^4 + x^2)(x^4 + 1) \right|_{m_i(x)}^{+} = x^4 + x^2 + 1.$$

Константы для вычисления веса ортогонального базиса

	Основания $m_i(x)$ полиномиального модулярного кода					
	$p_1(x)$	$p_2(x)$	$p_3(x)$	$p_4(x)$	$p_5(x)$	$p_6(x)$
$g_1^i(x)$	–	x^2+x	$x^4+x^3+x^2+x$	$x+1$	x^4+x^3+1	$x^4+x^3+x^2$
$g_2^i(x)$	x^2+x+1	–	x^3+x^2+1	x^4	x^4+x^3+x	$x+1$
$g_3^i(x)$	x^4+x^3+1	x^3+x^2	–	x^4+x^2	x^3	x^4
$g_4^i(x)$	x	x^4+x^3+x+1	$x^4+x^3+x^2+x+1$	–	x^4+x^3	x^2+x
$g_5^i(x)$	x^4+x^2	x^4+1	x^3+x^2+x+1	$x^4+x^3+x^2+x+1$	–	x^3+x
$g_6^i(x)$	x^4+1	x	$x^4+x^3+x^2+1$	x^2+x+1	x^3+x+1	–

Выполним проверку с использованием [черв].

1. $M_1^{12345}(x)=\prod_{j=2}^{5} m_j(x)=x^{20}+x^{18}+x^{16}+x^{14}+x^{13}+x^{11}+x^{19}+x^7+x^3+x^2+1$.
2. $\delta_1(x)=M_1^{12345}(x)\bmod m_1(x)=x^4+x^3+x=11010_2$.
3. $g_1^{12345}(x)=\delta_1^{-1}(x)\bmod m_1(x)=x^4+x^2+1=10101_2$.

Используя разработанный метод, вычислим оставшиеся веса базисов ПМК

$$g_2^{12345}(x)=\left|(x^2+x)(x^3+x^2)(x^4+1)\cdot x\right|^{+}_{m_2(x)}=x^3+1,$$

$$g_3^{12345}(x)=\left|(x^4+x^3+x^2+x)(x^3+x^2+1)(x^3+x^2+x+1)(x^4+x^3+x^2+1)\right|^{+}_{m_3(x)}=x^4+x^3+x+1,$$

$$g_4^{12345}(x)=\left|(x^4+x^3+1)(x^4+x^3+x)(x^3+x+1)\cdot x^3\right|^{+}_{m_4(x)}=x^4+x^2+x,$$

$$g_5^{12345}(x)=\left|(x^4+x^3+x^2)(x+1)(x^3+x)\cdot x^4\right|^{+}_{m_5(x)}=x^4+x^2.$$

Пусть в процессе функционирования из строя последовательно вышли два первых основания. После их отлучения ПМК состоит из оснований $m_3^{345}(x)=x^5+x^3+x^2+x+1$, $m_4^{345}(x)=x^5+x^4+x^3+x+1$, $m_5^{345}(x)=x^5+x^4+x^3+x^2+1$, где верхний индекс показывает оставшиеся работоспособные основания. Используя разработанный метод, вычислим веса динамически изменившегося кортежа ортогональных базисов ПМК

$$g_3^{345}(x)=\left|(x^3+x^2+x+1)(x^4+x^3+x^2+1)\right|^{+}_{m_3(x)}=x^2+x+1,$$

$$g_4^{345}(x)=\left|(x^3+x+1)\cdot x^3\right|^{+}_{m_4(x)}=x^4+x^2+1,\quad g_5^{12345}(x)=\left|(x^3+x)\cdot x^4\right|^{+}_{m_5(x)}=x^4+x+1.$$

Выполним проверку с использованием [черв].

1. Вычислим константы согласно (8). Получаем

$$M_3^{345}(x)=m_4^{345}(x)m_5^{345}(x)=x^{10}+x^8+x^7+x^6+x^4+x^3+x^2+x+1;$$
$$M_4^{345}(x)=m_3^{345}(x)m_5^{345}(x)=x^{10}+x^9+x^7+x^6+x^5+x^4+x^3+x+1;$$
$$M_5^{345}(x)=m_3^{345}(x)m_4^{345}(x)=x^{10}+x^9+x^4+x^3+1.$$

2. Вычислим остатки констант согласно (9). Тогда

$$\delta_3^{345}(x) = \left|M_3^{345}(x)\right|^{+}_{m_3(x)} = \left|x^{10}+x^8+x^7+x^6+x^4+x^3+x^2+x+1\right|^{+}_{m_3(x)} = x^4;$$

$$\delta_4^{345}(x) = \left|M_4^{345}(x)\right|^{+}_{m_4(x)} = \left|x^{10}+x^9+x^7+x^6+x^5+x^4+x^3+x+1\right|^{+}_{m_4(x)} = x^3+x^2+x;$$

$$\delta_5^{345}(x) = \left|M_5^{345}(x)\right|^{+}_{m_5(x)} = \left|x^{10}+x^9+x^4+x^3+1\right|^{+}_{m_5(x)} = x^4+x^2+x.$$

3. Вычислим веса ортогональных базисов согласно (10). Получаем

$$g_3^{345}(x) = \left|\frac{1}{x^4}\right|_{m_3^{345}(x)} = x^2+x+1;\ g_4^{345}(x) = \left|\frac{1}{(x^3+x^2+x)}\right|_{m_4^{345}(x)} = x^4+x^2+1;$$

$$g_5^{345}(x) = \left|\frac{1}{(x^4+x^2+x)}\right|_{m_5^{345}(x)} = x^4+x+1.$$

Тогда пересчитанные ортогональные базисы равны

$$B_3^{345}(x) = g_3^{345}(x)M_3^{345}(x) = x^{12}+x^{11}+x^8+x^4+x^3+x^2+1;$$

$$B_4^{345}(x) = g_4^{345}(x)M_4^{345}(x) = x^{14}+x^{13}+x^{12}+x^9+x^7+x^5+x^2+x;$$

$$B_5^{345}(x) = g_5^{345}(x)M_5^{345}(x) = x^{14}+x^{13}+x^{11}+x^9+x^8+x^7+x^5+x^4+x^3+x.$$

Проверка ортогональных базисов

$$B_3^{345}(x)+B_4^{345}(x)+B_5^{345}(x) = 1.$$

Анализ разработанного метода показал, что для получения веса базиса необходимо выполнить (n^*-1) операцию умножений, где n^* – количество работоспособных оснований ПМК, которые можно выполнять параллельно с вычислением констант $M_i^{n^*}(x)$. А при использовании метода [5] необходимо сначала выполнить (n^*-1) операцию умножений для вычислений констант $M_i^{n^*}(x)$, затем одну операцию деления и вычисления веса с использованием LUT-таблицы. В работе [6] показано, что для выполнения операций умножение/деление необходимо 4 такта, а на команду типа регистр-память 6 тактов CPU. В этом случае при пересчете кортежа из трех ортогональных базисов метода [5] потребуется 18 тактов CPU, что при использовании процессора Intel(R) Core™ i5-3470 CPU соответствует 5,625 нс. А разработанный метод для этого потребует 8 тактов CPU, затратив на это 2,5 нс, что в 2,25 раз меньше.

Заключение

Применение ПМК в протоколе аутентификации спутника позволяет не только снизить временные затраты на опознавание, но и повысить отказоустойчивость системы «свой – чужой». При этом ПМК позволяют системе опознавания сохранять работоспособное состояние при выходе из строя нескольких вычислительных трактов за счет перераспределения оставшихся вычислительных ресурсов. Но при реконфигурации системы опознавания, реализованной с использованием ПМК, необходимо производить пересчет ортогональных базисов. В работе представлен разработанный метод вычисления динамически изменяемого кортежа ортогональных базисов, применение которого требует в 2,25 раз меньше временных затрат по сравнению с методом, приведенным в работе [5].

Исследование выполнено при финансовой поддержке РФФИ в рамках научного проекта № 18-07-01020.

Список литературы

1. Кукк К.И. Спутниковая связь: прошлое, настоящее, будущее. М.: Горячая линия – Телеком, 2017. 256 с.

2. Калмыков И.А., Науменко Д.О., Калмыков М.И., Вельц О.В. Алгоритм имитозащиты для систем удаленного мониторинга и управления критическими технологиями // Известия ЮФУ. Технические науки. 2014. № 2. С. 181–187.

3. Pashintsev V.P., Zhuk F.P., Chistousov N.K. Development of Satellite Authentication System for Low Earth Orbit Satellite Communication System on the Basis of Polynomial Residue Number System. International Journal of Engineering and Advanced Technology (IJEAT). 2019. Vol. 8. Issue 5. P. 2557–2562.

4. Горденко Д.В., Резеньков Д.Н., Саркисов А.Б. Методы и алгоритмы реконфигурации непозиционных вычислительных структур для обеспечения отказоустойчивости спецпроцессоров. Ставрополь: Изд-во Фабула, 2014. 180 с.

5. Червяков Н.И., Коляда А.А., Ляхов П.А. Модулярная арифметика и ее приложения в инфокоммуникационных технологиях. М.: ФИЗМАТЛИТ, 2017. 400 с.

6. Infographics. Operation Costs in CPU Clock Cycles. [Электронный ресурс]. URL: http://ithare.com/infographics-operation-costs-in-cpu-clock-cycles (дата обращения: 14.03.2020).