



УДК 004.052:629.78

**АНАЛИЗ МАТЕМАТИЧЕСКИХ МОДЕЛЕЙ КОДОПРЕОБРАЗОВАНИЯ ДЛЯ СИСТЕМ
АУТЕНТИФИКАЦИИ, ФУНКЦИОНИРУЮЩИХ В МОДУЛЯРНЫХ КОДАХ****Чистоусов Никита Константинович**

аспирант 3 года обучения

Чипига Александр Федорович

кандидат технических наук, профессор

Калмыкова Наталья Игоревна

студентка 3 курса

ФГАОУ ВО «Северо-Кавказский федеральный университет»

ИМИТ имени профессора Н.И. Червякова

кафедра информационной безопасности автоматизированных систем, г. Ставрополь

Аннотация. Модулярные коды широко применяются в протоколах аутентификации с высокой имитостойкостью, которые функционируют в низкоорбитальных системах спутниковой связи. Вычисления, требуемые при аутентификации, подразумевают преобразование из модулярного кода в позиционный код. Цель - рассмотреть существующие модели преобразователей и выбрать алгоритм, выполняющий расчеты максимально быстро.

Ключевые слова: низкоорбитальная система спутниковой связи, система аутентификации космического аппарата, модулярный код, алгоритмы преобразования из модулярного кода в позиционный код, система остаточных классов

Введение

Приемлемые показатели имитостойкости достигаются в низкоорбитальных системах спутниковой связи за счет использования протокола аутентификации. Значительно ускорить вычисления в данных протоколах помогает применение модулярных кодов (МК), которые распараллеливают вычисления на уровне арифметических операций. Однако расчеты требуют обязательной операции обратного преобразования из МК в позиционную систему счисления (ПСС). Поэтому цель выбрать алгоритм, выполняющий преобразование из МК в ПСС максимально быстро.

Основная часть

Определение одномодульного алгоритма в системе остаточных классов (СОК) в работе [1] повысил скорость протокола в 4 раза. В СОК число A , принадлежащее ПСС, однозначно представляется в виде набора остатков при делении на основания системы СОК p_i , $i = 1, \dots, n$;



$$A = (\alpha_1, \alpha_2, \dots, \alpha_n), \quad (1)$$

где $\alpha_i \equiv A \bmod p_i$; $i = 1, 2, \dots, n$; $\text{НОД}(p_i, p_j) = 1$; $i \neq j$.

По математической структуре СОК является кольцом, причем:

$$A \pm B = ((\alpha_1 \pm \beta_1) \bmod p_1, (\alpha_2 \pm \beta_2) \bmod p_2, \dots, (\alpha_n \pm \beta_n) \bmod p_n), \quad (2)$$

$$A \cdot B = ((\alpha_1 \cdot \beta_1) \bmod p_1, (\alpha_2 \cdot \beta_2) \bmod p_2, \dots, (\alpha_n \cdot \beta_n) \bmod p_n), \quad (3)$$

где $\alpha_i \equiv A \bmod p_i$; $\beta_i \equiv B \bmod p_i$; $i = 1, 2, \dots, n$.

Однозначное отображение между числом в ПСС и кортежем в СОК существует, если число определено в рабочем диапазоне системы СОК:

$$P_{\text{раб}} = \prod_{i=1}^n p_i, \quad (4)$$

Преобразование из МК в ПСС (МК-ПСС) является немодульной операцией по причине непозиционности МК. Китайская теорема об остатках (КТО) основа данного преобразования [3]:

$$A = \left| \alpha_1 B_1 + \alpha_2 B_2 + \dots + \alpha_n B_n \right|_{P_{\text{раб}}}^+ = \left| \alpha_1 m_1 \right|_{p_1}^+ P_1^* + \left| \alpha_2 m_2 \right|_{p_2}^+ P_2^* + \dots + \left| \alpha_n m_n \right|_{p_n}^+ P_n^* \Big|_{P_{\text{раб}}}^+, \quad (5)$$

где $B_i = P_i^* \cdot m_i$ и $B_i \equiv 1 \bmod p_i$ – ортогональный базис i -го основания; m_i – вес

ортогонального базиса, $P_i^* = \frac{P_{\text{раб}}}{p_i}$.

Стоит отметить, что значения m_i и P_i^* являются константами, зависящими от оснований СОК, поэтому ускорить вычисления (МК-ПСС) можно за счет определения отображения $\alpha_i \rightarrow \left| \alpha_i m_i \right|_{p_i}^+ P_i^*$ с помощью LUT таблиц.

При расчете МК-ПСС число A в ПСС может оказаться вне рабочего диапазона, что противоречит определению выше. Позиционная характеристика ранг r числа разрешает данную вычислительную проблему:

$$A = \sum_{i=1}^n \alpha_i B_i - r P_{\text{раб}} \quad (6)$$



Деление числа A на $P_{pa\bar{b}}$ является одним из методов нахождения ранга r числа A .
Время алгоритма целочисленного деления без восстановления остатка, определенного в работе [2], имеет вид:

$$T_R = r_{\max}(t_{SUM} + t_{SH}) \quad (7)$$

где $r_{\max}$ – максимальный ранг в МК, t_{SUM} – время выполнения суммирования, t_{SH} – время выполнения операции сдвига.

Полное время работы МК-ПСС определяется следующим образом:

$$T_{МК-ПСС}^{DIV} = T_{SUM} + T_R + T_{MUL} + T_{SUB}, \quad (8)$$

где T_{SUM} – время суммирования произведений остатков МК на ортогональные базисы, T_R – время вычисления ранга числа, T_{MUL} – время умножения ранга числа на $P_{pa\bar{b}}$, T_{SUB} – время выполнения операции вычитания.

Введем другое решение для нахождения ранга числа. Обозначим дополнительное основание P_g по условию:

$$НОД(P_{pa\bar{b}}, p_g) = 1, p_g > r_{\max}, \quad (9)$$

Следовательно, имеем следующее:

$$\alpha_g \equiv \left(\sum_{i=1}^n \alpha_i B_i - r P_{pa\bar{b}} \right) \bmod p_g \quad (10)$$

Преобразуем

$$r P_{pa\bar{b}} = \left(\sum_{i=1}^n \alpha_i B_i - \alpha_g \right) \bmod p_g \quad (11)$$

Поделим обе части на $P_{pa\bar{b}}$, тогда

$$r = \left(\sum_{i=1}^n \frac{\alpha_i B_i}{P_{pa\bar{b}}} - \frac{\alpha_g}{P_{pa\bar{b}}} \right) \bmod p_g = \left(\sum_{i=1}^n \alpha_i B_i P_{pa\bar{b}}^{-1} - \alpha_g P_{pa\bar{b}}^{-1} \right) \bmod p_g \quad (12)$$

Введем две переменные

$$v_i = \frac{P_i^*}{P_{pa\bar{b}}} = \frac{1}{p_i}, v_g = P_{pa\bar{b}}^{-1} \bmod p_g \quad (13)$$

Поэтому получим

$$r = \left(\sum_{i=1}^n |\alpha_i m_i|_{p_i}^+ v_i + \alpha_g (p_g - v_g) \right) \bmod p_g \quad (14)$$

На рисунке 1 представлена схема обратного преобразователя МК-ПСС для трех рабочих оснований МК и одного дополнительного основания системы. Левая часть схемы вычисляет подмодульное выражение формулы (5), а правая часть определяет ранг числа согласно формуле (14).

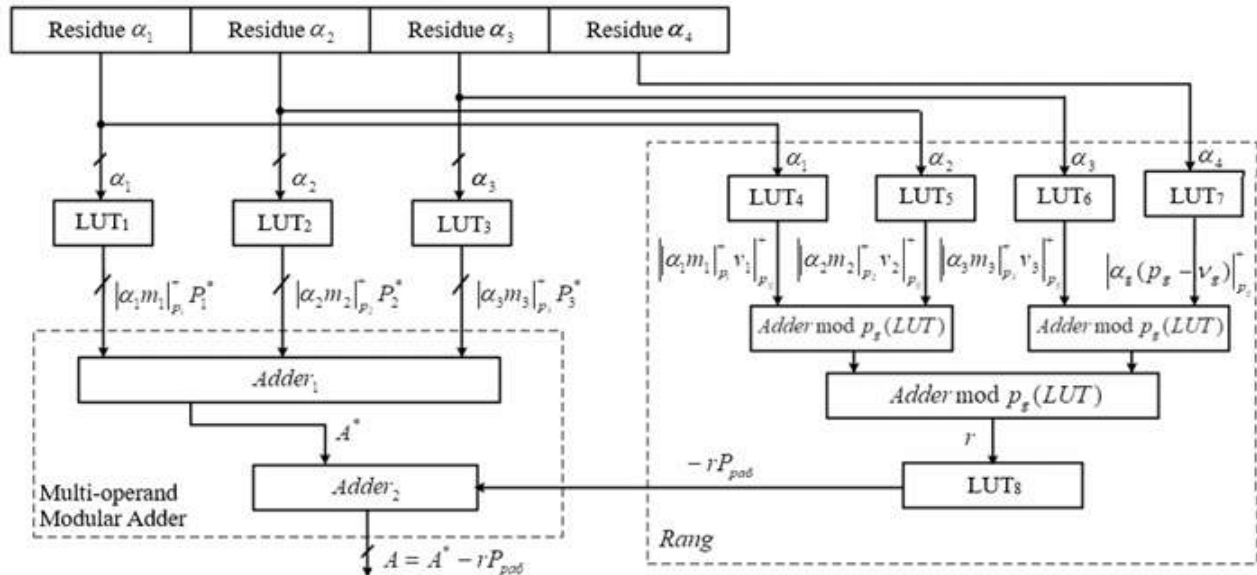


Рисунок 1 – Схема обратного преобразователя МК-ПСС

Пример

Пусть основания МК следующие: $p_1=41$, $p_2=43$ и $p_3=47$, тогда рабочий диапазон МК равен $P_{раб}=82861$. Найдем ортогональные базисы для оснований по следующим шагам [3]:

1. Определим $P_i^* = P_{раб} / p_i$;
2. Рассчитаем остаток $\delta_i = P_i^* \bmod p_i$;
3. Найдем вес ортогонального базиса m_i из условия $m_i \cdot \delta_i \equiv 1 \bmod p_i$;
4. Наконец, вычислим ортогональный базис основания $B_i = m_i \cdot P_i^*$.

По алгоритму найдены следующие значения для МК:

- $P_1^* = 2021$, $P_2^* = 1927$, $P_3^* = 1763$;
- веса ортогональных базисов $m_1=24$, $m_2=16$, $m_3=2$;
- ортогональные базисы $B_1=48504$, $B_2=30832$, $B_3=3526$.

Максимальный ранг равен $r_{max}=26$, значит, в качестве дополнительного основания

выберем

$p_g=53$.

Значения

констант

v_i :



$$v_1 = |p_1^{-1}|_{p_g}^+ = |41^{-1}|_{53}^+ = 22, v_2 = |p_2^{-1}|_{p_g}^+ = |43^{-1}|_{53}^+ = 37, v_3 = |p_3^{-1}|_{p_g}^+ = |47^{-1}|_{53}^+ = 44,$$

$$v_g = |P_{паб}^{-1}|_{p_g}^+ = |82861^{-1}|_{53}^+ = 41.$$

Пусть дано число $A = 19548 = (32, 26, 43, 44)$ в МК и необходимо перевести его в ПСС.

Вычислим значение выходного сигнала $Adder_1$:

$$LUT_1: A_1 = |\alpha_1 m_1|_{p_1}^+ P_1^* = |32 \cdot 24|_{41}^+ \cdot 2021 = 60630$$

$$LUT_2: A_2 = |\alpha_2 m_2|_{p_2}^+ P_2^* = |26 \cdot 16|_{43}^+ \cdot 1927 = 55883$$

$$LUT_3: A_3 = |\alpha_3 m_3|_{p_3}^+ P_3^* = |43 \cdot 2|_{47}^+ \cdot 1763 = 68757$$

$$Adder_1: A^* = A_1 + A_2 + A_3 = 185270$$

Теперь вычислим выходное значение LUT_8 :

$$LUT_4: |\alpha_1 m_1|_{p_1}^+ v_1|_{p_g}^+ = |32 \cdot 24|_{41}^+ \cdot 22|_{53}^+ = 24$$

$$LUT_5: |\alpha_2 m_2|_{p_2}^+ v_2|_{p_g}^+ = |26 \cdot 16|_{43}^+ \cdot 37|_{53}^+ = 13$$

$$LUT_6: |\alpha_3 m_3|_{p_3}^+ v_3|_{p_g}^+ = |43 \cdot 2|_{47}^+ \cdot 44|_{53}^+ = 20$$

$$LUT_7: |\alpha_g (p_g - v_g)|_{p_g}^+ = |44(53 - 41)|_{53}^+ = 51$$

$$\text{Входное значение } LUT_8: r = \left(\sum_{i=1}^n |\alpha_i m_i|_{p_i}^+ v_i + \alpha_g (p_g - v_g) \right) \bmod p_g = 2$$

$$\text{Выходное значение } LUT_8: -rP_{паб} = -165722$$

$$\text{В итоге получаем число } A = A^* - rP_{паб} = 185270 - 165722 = 19548$$

Найдем число A , используя КТО:

$$A = |\alpha_1 B_1 + \alpha_2 B_2 + \alpha_3 B_3|_{P_{паб}}^+ = |32 \cdot 48504 + 26 \cdot 30832 + 43 \cdot 3526|_{82861}^+ = 19548$$

Время работы разработанного алгоритма определяется

$$T_{МК-ПСС}^{МК} = T_{СУМ}^{МК} + T_{СУБ} = (T_{LUT} + T_{Adder_1}) + T_{СУБ} = 19\tau$$

где τ – время срабатывания логических схем совпадения.

Наконец вычислим временные затраты на обратное преобразование с помощью алгоритма деления без восстановления остатка:



$$T_{МК-ПСС}^{DIV} = T_{SUM} + T_R + T_{MUL} + T_{SUB} = 13\tau + 2(3\tau + 2\tau) + \tau + 6\tau = 30\tau$$

Проанализировав результаты можно сделать следующий вывод: применение КТО в обратном преобразовании МК-ПСС ускоряет вычисления алгоритма в 1,54 раза по сравнению с классическим методом деления.

Вывод

Имитостойкость и быстродействие главные характеристики функционирования низкоорбитальных систем спутниковой связи. Первая характеристика достигается за счет применения протокола аутентификации, а вторая за счет определения данного протокола в МК. Использование МК требует вычислять обратное преобразование МК-ПСС. Проведенный анализ показал, что применение КТО в обратном преобразовании МК-ПСС ускоряет вычисления алгоритма в 1,54 раза по сравнению с классическим методом деления.

Исследование выполнено при финансовой поддержке РФФИ в рамках научного проекта № 20-37-90009

Список литературы:

1. Чистоусов Н.К., Чипига А.Ф., Калмыкова Н.И. Разработка метода аутентификации, реализованного в модулярных кодах системы остаточных классов [Текст] // Сборник научных трудов по материалам XXVII Международной научно-практической конференции «Современные научные исследования» (г.-к. Анапа, 16 декабря 2020 г.). – Анапа: Изд-во «НИЦ ЭСП» в ЮФО, 2020 – с. 123-129
2. Червяков Н.И., Евдокимов А.А., Галушкин А.И., Лавриненко И.Н., Лавриненко А.В. Применение искусственных нейронных сетей и системы остаточных классов в криптографии. М.: Физматлит, 2012. 280 с.
3. Червяков Н.И., Коляда А.А., Ляхов П.А. Модулярная арифметика и ее приложения в инфокоммуникационных технологиях. М.: ФИЗМАТЛИТ, 2017. 400 с