Инженерный вестник Дона, №5 (2022)
ivdon.ru/ru/magazine/archive/n5y2022/7606

Модификация алгоритма коррекции ошибок, возникающих в процессе работы системы аутентификации спутника

Н.К. Чистоусов, И.А. Калмыков, Д.В. Духовный,

Н.И. Калмыкова

Северо-Кавказский федеральный университет, Ставрополь, Россия

Аннотация: По мере увеличения числа низкоорбитальных группировок спутников (НГС), будет возрастать вероятность деструктивного воздействия со стороны чужих космических аппаратов (КА). Одним из наиболее эффективных воздействий на НГС является постановка ретрансляционной помехи, которая представляет собой перехваченный и задержанный сигнал. Устранить данную проблему можно за счет использования системы опознавания «свой-чужой» для КА. При этом, для снижения вероятности подбора правильного сигнала ответчика, чужим КА предлагается снизить временные затраты на вычисления статуса спутника за счет применения параллельных вычисления с использованием кодов полиномиальной системы классов вычетов (ПСКВ). Характерной особенностью данных кодов является независимое и параллельное выполнение вычислений по основаниям ПСКВ. Однако, данное свойство кода ПСКВ можно также использовать для коррекции ошибок, которые возникают в процессе работы системы опознавания. При этом алгоритм должен выполнить данную процедуру при меньших временных затратах. Поэтому модификация алгоритма коррекции ошибок, позволяющая обеспечивать более высокую скорость поиска и исправления ошибок, является актуальной задачей. Цель работы – обеспечить снижение временных затрат на выполнение процедуры обнаружения и исправления ошибок в процессе работы системы опознавания, за счет модификации алгоритма коррекции на основе Китайской теоремы об остатках.

Ключевые слова: система опознавания спутника, коды полиномиальной системы классов вычетов, позиционная характеристика, алгоритмы обнаружения и коррекции ошибок.

Введение

Современный этап развития районов Крайнего Севера стал триггером повышенного интереса к низкоорбитальным группировкам спутников (далее НГС). Это вызвано, прежде всего, основным достоинством низкоорбитальных спутников – возможностью обеспечения связи в высоких широтах [1]. Однако, по мере увеличения числа таких группировок будет возрастать вероятность деструктивного воздействия на космическую связь со стороны чужих космических аппаратов (далее КА). Проведенный анализ показал, что одним из эффективных деструктивных воздействий является

постановка ретрансляционной помехи. В этом случае «спутник-нарушитель» перехватывает сигнал, задерживает его для последующего его навязывания приемному устройству системы спутниковой связи. При этом параметры ретрансляционной помехи полностью совпадают с сигналами, используемыми НГС. Чтобы устранить данную уязвимость в работе [2], предлагают перед началом сеанса связи провести аутентификацию спутника. Чтобы сократить время на вычисление статуса КА, то есть уменьшить вероятность подбора правильного сигнала ответчика, в работах [3, 4] были рассмотрены реализации протоколов аутентификации с нулевым разглашением знаний, реализованных в кодах системы остаточных классов. Для дальнейшего повышения имитостойкости НГС в работе [5] была произведена модификация метода аутентификации спутника. Авторы предложили применить в протоколе аутентификации коды полиномиальной системы классов вычетов (далее ПСКВ). Поставленная цель была достигнута за счет того, что все вычисления в данном коде выполняются параллельно по основаниям ПСКВ. При этом в процессе вычислений обмен промежуточными результатами между основаниями не происходит. Именно данное свойство положено в основу построения кодов ПСКВ, исправляющих ошибки вычислений [6]. Однако, учитывая тот факт, что процедура поиска и коррекции ошибок увеличивает время на определение статуса спутника, то необходимо получить такой алгоритм поиска и коррекции ошибок, который бы имел меньшие временные затраты. Поэтому модификация алгоритма коррекции ошибок, позволяющая выполнить данную процедуру при меньших временных затратах, является актуальной задачей.

Цель исследования

Известно, что модулярные коды (далее МК), а к ним относится и ПСКВ, обладают свойством диверсности при обнаружении и исправлении ошибок. Это вызвано тем, что при выполнении данных операций

используется целый ряд позиционных характеристик (далее ПХ) [7-9]. Все они показывают расположение кодовой комбинации, которая представляет собой набор остатков целого числа по основаниям МК, относительно рабочего диапазона. Большинство алгоритмов вычисления ПХ использует Китайскую теорему об остатках (далее КТО). Поэтому целью работы является модификация алгоритма коррекции на основе КТО для полиномов, применение которого позволит снизить временные затраты на исправление ошибок, возникающих в процессе функционирования системы опознавания.

Материалы и методы

В МК целые числа кодируются в виде набора остатков, которые вычисляются по основаниям кода. Для кодов ПСКВ основаниями являются неприводимые полиномы $m_i(x)$, где $i=1,...,n$. При этом двоичный код целого числа A представляется в виде многочлена $A(x)$, для которого справедливо:

$$A(x)=(A_1(x),\ A_2(x),\ A_3(x),...,\ A_n(x)), \quad (1)$$

где $A_i(x)\equiv A(x)\bmod m_i(x);\ i=1,...,n$.

При этом кортеж оснований кода ПСКВ определяет диапазон разрешенных комбинаций:

$$M_n(x)=\prod_{i=1}^{n} m_i(x). \quad (2)$$

В коде ПСКВ эффективно выполняются модульные операции, которые можно записать в виде равенств:

$$S(x)+A(x)=((S_1(x)+A_1(x))\bmod m_1(x),...,(S_n(x)+A_n(x))\bmod m_n(x)), \quad (3)$$

$$S(x)\cdot A(x)=((S_1(x)\cdot A_1(x))\bmod m_1(x),...,(S_n(x)\cdot A_n(x))\bmod m_n(x)), \quad (4)$$

где $\{\deg S(x),\deg A(x)\}<\deg M_n(x);\ S_i(x)\equiv S(x)\bmod m_i(x);\ i=1,...,n$.

Эффективность кодов ПСКВ определяется тем, что модульные операции выполняются параллельно по основаниям кода. При этом

используются остатки $A_i(x), S_i(x)$, разрядность которых значительно меньше исходных операндов $A(x), S(x)$. Это позволяет увеличить скорость проводимых вычислений.

Используя данное свойство кода ПСКВ, была выполнена модификация метода аутентификации, предназначенного для вычисления статусов космических аппаратов [5]. Перед началом работы системы опознавания КА осуществляется выбор оснований кода ПСКВ, для которых имеет место:

$$\log_2\{W, Q, E\} < \deg M_n(x). \quad (4)$$

где W – секретный ключ КА; Q и E – случайные числа, которые будет использованы для получения временного ключа $Q(j)$ для j-го сеанса проверки и аргумента $E(j)$ необходимого для проверки повторного применения $Q(j)$.

Для получения $Q(j), E(j)$ в работе [10] предлагается на ответчике использовать генератор псевдослучайной функцией, обладающей высокой криптостойкостью. Затем ответчик (O:) разбивает числа $W(j), Q(j), E(j)$ на части согласно условия $\log_2\{W_i(j), Q_i(j), E_i(j)\} = \deg m_i(x)$. Тогда:

$$\begin{aligned} &O: W(j) = (W_1(j) \| W_2(j) \| \ldots \| W_n(j)), \\ &O: Q(j) = (Q_1(j) \| Q_2(j) \| \ldots \| Q_n(j)), \\ &O: E(j) = (E_1(j) \| E_2(j) \| \ldots \| E_n(j)). \end{aligned} \quad (5)$$

Перед j-ым сеансом проверки ответчик для вычисления «истинного» статуса спутника использует выражение:

$$O: \begin{cases} A_1^j(x) = x^{W_1(j)} x^{Q_1(j)} x^{E_1(j)} \bmod m_1(x), \\ \vdots \\ A_n^j(x) = x^{W_n(j)} x^{Q_n(j)} x^{E_n(j)} \bmod m_n(x). \end{cases} \quad (6)$$

Чтобы вычислить «искаженный» статус КА для выполнения j-го сеанса проверки ответчик генерирует случайные числа:

$$\{\Delta W_i(j), \Delta Q_i(j), \Delta E_i(j)\} < V_i = 2^{\deg m_i(x)} - 1. \quad (7)$$

С помощью этих чисел ответчик производит замену параметров:

$$\begin{aligned} O:\widetilde{W}_i\ (j) &= W_i\ (j) + \Delta W_i\ (j) \bmod V_i\ , \\ O:\widetilde{Q}_i\ (j) &= Q_i\ (j) + \Delta Q_i\ (j) \bmod V_i\ , \\ O:\widetilde{E}_i\ (j) &= E_i\ (j) + \Delta E_i\ (j) \bmod V_i\ . \end{aligned} \tag{8}$$

Полученные искаженные параметры ответчик использует для вычисления «искаженного» статуса спутника:

$$O: \begin{cases} \widetilde{A}_1^{\,j}(x) = x^{\widetilde{W}_1(j)} x^{\widetilde{Q}_1(j)} x^{\widetilde{E}_1(j)} \bmod m_1(x), \\ \vdots \\ \widetilde{A}_n^{\,j}(x) = x^{\widetilde{W}_n(j)} x^{\widetilde{Q}_n(j)} x^{\widetilde{E}_n(j)} \bmod m_n(x). \end{cases} \tag{9}$$

На этом предварительная часть модифицированного метода аутентификации заканчивается и начинается процесс опознавания спутника.

Сначала запросчик производит вычисление случайного числа $C(j)$, используя генератор псевдослучайной функции, представленный в работе [10]. Затем разбивает это число на части и передает ответчику:

$$З \to O: C(j) = (C_1(j) \,\|\, C_2(j) \,\|\, ... \,\|\, C_n(j)), \tag{10}$$

где $\log_2\{C_i\ (j)\} = \deg m_i\ (x);\ i = 1, ..., n$.

Ответчик принимает сигнал, поступивший от запросчика, и вычисляет:

$$\begin{aligned} O: H_i^1(j) &= \widetilde{W}_i\ (j) - C_i\ (j) W_i\ (j) \bmod V_i\ , \\ O: H_i^2(j) &= \widetilde{Q}_i\ (j) - C_i\ (j) Q_i\ (j) \bmod V_i\ , \\ O: H_i^3(j) &= \widetilde{E}_i\ (j) - C_i\ (j) E_i\ (j) \bmod V_i\ . \end{aligned} \tag{11}$$

После этого ответчик собирает сигнал, который предается запросчику:

$$O \to З: \left\{A_i^j(x),\ \widetilde{A}_i^{\,j}(x),\ H_i^1(j),\ H_i^2(j),\ H_i^3(j)\right\} \quad . \tag{12}$$

Получив этот сигнал, запросчик должен выполнить его проверку:

$$З: \begin{cases} P_1^j(x) = \left(\left(A_1^j(x)\right)^{B_1(j)} x^{H_1^1(j)} x^{H_1^2(j)} x^{H_1^3(j)}\right) \bmod m_1(x), \\ \vdots \\ P_n^j(x) = \left(\left(A_n^j(x)\right)^{B_n(j)} x^{H_n^1(j)} x^{H_n^2(j)} x^{H_n^3(j)}\right) \bmod m_n(x). \end{cases} \tag{13}$$

После проверки сигнала ответчика запросчик выдает статус «свой» спутнику, если выполняется равенство:

$$\left\{P_1^j(x) = \tilde{A}_1^j(x), ..., P_n^j(x) = \tilde{A}_n^j(x)\right\}. \quad (14)$$

Используя данный модифицированный метод аутентификации, была разработана структурная модель системы опознавания, работающая в МК. Проведенные исследования показали, что при использовании 5 шестиразрядных неприводимых полиномов и за счет параллельных вычислений в кодах ПСКВ временные затраты сократились с $T_o = 5936$ нс для одномодульного протокола [2] до $T_{ПСКВ} = 3238$ нс.

Однако свойство кодов ПСКВ на параллельные и независимые вычисления по основаниям можно использовать для исправления ошибок, которые возникают из-за сбоев при работе системы опознавания. Для этого необходимо построить избыточные коды ПСКВ. В работе [6] доказано, что для исправления однократной ошибки в код ПСКВ надо добавить два контрольных основания. Они выбираются из условия:

$$\deg m_{n+1}(x) + \deg m_{n+2}(x) \geq \deg m_n(x) + \deg m_{n-1}(x). \quad (15)$$

Из-за введения этих оснований происходит увеличение диапазона кода ПСКВ до величины:

$$M_{n+2}(x) = \prod_{i=1}^{n+2} m_i(x). \quad (16)$$

При этом также увеличивается набор остатков:

$$A(x) = (A_1(x), A_2(x),..., A_n(x), A_{n+1}(x), A_{n+2}(x)). \quad (17)$$

Комбинация избыточного кода ПСКВ является разрешенной, если для нее справедливо:

$$\deg A(x) < \deg M_n(x). \quad (18)$$

Нарушение условия (18), свидетельствует о том, что комбинация, определяемая равенством (17), является запрещенной.

Учитывая, что наличие ошибки в кодовой комбинации определяется местоположением относительно рабочего диапазона, то для определения и

коррекции ошибки в модулярных кодах применяются различные позиционные характеристики [11]. При этом большинство алгоритмов вычисления ПХ использует Китайскую теорему об остатках. Так в работе [12] для кода предлагается на основе КТО реализовать вычисление позиционный характеристики – следа кода. Алгоритм вычисления данной ПХ является итерационным и содержит n этапов. На первом этапе из модулярного кода вычитают первую константу нулевизации. В результате получается:

$$A^1(x) = (A_1(x), A_2(x), ..., A_{n+2}(x)) - (A_{11}(x), A_{12}(x), ..., A_{1(n+2)}(x)) = \\ = (0, A_2^1(x), A_3^1(x), ..., A_{n+2}^1(x)), \quad (19)$$

где $A_1(x) = A_{11}(x)$; $A_i^1(x) = A_i(x) + A_{1i}(x) \bmod m_i$; $i = 2, ..., n+2$.

На втором этапе из полученного результата вычитают вторую константу нулевизации. В результате получается:

$$A^2(x) = (0, A_2^1(x), A_3^1(x), ..., A_{n+2}^1(x)) - (0, A_{22}(x), A_{23}(x), ..., A_{2n+2}(x)) = \\ = (0, 0, A_3^2(x), ..., A_{n+2}^2(x)), \quad (20)$$

где $A_2^1(x) = A_{22}(x)$; $A_i^2(x) = A_i^1(x) + A_{2i}(x) \bmod m_i(x)$; $i = 3, ..., n+2$.

Алгоритм повторяется n раз. На последнем этапе из полученного промежуточного результата вычитается n-ая константа нулевизации. В результате получается след кода:

$$A^n(x) = (0, ..., A_n^{n-1}(x), A_{n+1}^{n-1}(x), A_{n+2}^{n-1}(x)) - (0, ..., A_{nn}(x), A_{n(n+1)}(x), A_{n(n+2)}(x)) = \\ = (0, 0, , ,., A_{n+1}^n(x), A_{n+2}^n(x)) = (0, 0, , ,., \theta_{n+1}(x), \theta_{n+2}(x)). \quad (21)$$

где $A_n^{n-1}(x) = A_{nn}(x)$.

Если след кода $\theta_1(x) = 0$, $\theta_2(x) = 0$, то код ПСКВ не содержит ошибки. Если это условие не выполняется, то по величине данной ПХ определяется вектор ошибки, с помощью которого корректируется кодовая комбинация.

Анализ выражений (19) - (21) показывает, что данный алгоритм требует последовательного выполнения n итераций, так как выбор текущей константы нулевизации зависит от значения старшего остатка кода,

полученного на предыдущем этапе вычислений.

Устранить данный недостаток можно за счет модификации данного алгоритма. Так как разрешенная комбинация должна удовлетворять условию (18), то получаем равенство:

$$(A_1(x),\ A_2(x),...,\ A_n(x)) = (A_1(x),\ A_2(x),...,\ A_n(x),\ A_{n+1}(x),\ A_{n+2}(x)). \quad (22)$$

Используя КТО, выполним обратное преобразование из кода ПСКВ в позиционный код:

$$A(x) = \sum_{i=1}^{n} A_i(x) B_i(x) \bmod M_n(x), \quad (23)$$

где $B_i(x)$ – ортогональный базис по i-ому основанию кода ПСКВ; $i = 1,...,n$.

Ортогональные базисы содержат n остатков, среди которых все нули и только один остаток равен единице. То есть, они имеют вид:

$$\begin{aligned} B_1(x) &= (1,\ 0,\ 0,...,\ 0), \\ B_2(x) &= (0,\ 1,\ 0,...,\ 0), \\ B_3(x) &= (0,\ 0,\ 1,...,\ 0), \\ &\vdots \\ B_n(x) &= (0,\ 0,\ 0,...,\ 1). \end{aligned} \quad (24)$$

Расширим данные ортогональные базисы на два контрольных остатка. В результате получаем:

$$\begin{aligned} \ddot{B}_1(x) &= (1,\ 0,\ 0,...,\ 0,\ \mu_{n+1}^1(x),\ \mu_{n+2}^1(x)), \\ \ddot{B}_2(x) &= (0,\ 1,\ 0,...,\ 0,\ \mu_{n+1}^2(x),\ \mu_{n+2}^2(x)), \\ \ddot{B}_3(x) &= (0,\ 0,\ 1,...,\ 0,\ \mu_{n+1}^3(x),\ \mu_{n+2}^3(x)), \\ &\vdots \\ \ddot{B}_n(x) &= (0,\ 0,\ 0,...,\ 1,\ \mu_{n+1}^n(x),\ \mu_{n+2}^n(x)), \end{aligned} \quad (25)$$

где $\mu_{n+1}^i(x) = B_i(x) \bmod m_{n+1}(x)$; $\mu_{n+2}^i(x) = B_i(x) \bmod m_{n+2}(x)$; $i = 1,...,n$.

Это модифицированные константы нулевизации для остатков, равных единице, т.е. $A_i(x) = 1$, $i = 1,...,n$. В общем виде значения модифицированных констант нулевизации будут иметь вид:

$$\begin{aligned}
\hat{A}_1(x) &= \left|A_1(x)\vec{\vec{B}}_1(x)\right|^{+}_{M_n(x)} = (A_1(x),0,0,...,0,p^1_{n+1}(x),p^1_{n+2}(x)),\\
\hat{A}_2(x) &= \left|A_2(x)\vec{\vec{B}}_2(x)\right|^{+}_{M_n(x)} = (0,A_2(x),0,...,0,p^2_{n+1}(x),p^2_{n+2}(x)),\\
\hat{A}_3(x) &= \left|A_3(x)\vec{\vec{B}}_3(x)\right|^{+}_{M_n(x)} = (0,0,A_3(x),...,0,p^3_{n+1}(x),p^3_{n+2}(x)),\\
&\vdots\\
\hat{A}_n(x) &= \left|A_n(x)\vec{\vec{B}}_n(x)\right|^{+}_{M_n(x)} = (0,0,0,...,A_n(x),p^n_{n+1}(x),p^n_{n+2}(x)),
\end{aligned} \tag{26}$$

где $p^i_{n+1}(x) = \left\|A_i(x)\vec{\vec{B}}_i(x)\right|^{+}_{M_n(x)}\Big|^{+}_{m_{n+1}(x)}$; $p^i_{n+2}(x) = \left\|A_i(x)\vec{\vec{B}}_i(x)\right|^{+}_{M_n(x)}\Big|^{+}_{m_{n+2}(x)}$; ; $i = 1,...,n$.

На основе равенства (22), имеем равенство:

$$\begin{aligned}
&(A_1(x),A_2(x),...,A_n(x),A_{n+1}(x),A_{n+2}(x)) =\\
&= (A_1(x),A_2(x),...,A_n(x),\sum_{i=1}^{n}p^i_{n+1}(x),\sum_{i=1}^{n}p^i_{n+2}(x)).
\end{aligned} \tag{27}$$

Тогда справедливо:

$$\begin{aligned}
A_{n+1}(x) &= \sum_{i=1}^{n}p^i_{n+1}(x),\\
A_{n+2}(x) &= \sum_{i=1}^{n}p^i_{n+2}(x).
\end{aligned} \tag{28}$$

Значит, позиционная характеристика следа кода определяется:

$$\begin{aligned}
\theta_{n+1}(x) &= A_{n+1}(x) - \sum_{i=1}^{n}p^i_{n+1}(x),\\
\theta_{n+2}(x) &= A_{n+2}(x) - \sum_{i=1}^{n}p^i_{n+2}(x).
\end{aligned} \tag{29}$$

Если кодовая комбинация ПСКВ не содержит ошибки, то след кода $\theta_1(x) = 0$, $\theta_2(x) = 0$. Если данное условие не выполняется, то по величине данной ПХ определяется вектор ошибки, с помощью которого корректируется кодовая комбинация.

Анализ выражений (25) -(29) показывает, что модифицированный алгоритм вычисления следа кода позволяет осуществлять поиск и коррекцию ошибок за одну итерацию, используя многовходовые сумматоры по модулю два. Значит, использование модифицированного алгоритма вычисления следа кода ПСКВ позволяет сократить временные затраты на коррекцию ошибок,

которые возникают в процессе работы системы опознавания спутников.

Результаты исследования и их обсуждение

Выберем разрядность $\{W, Q, E\}$ равную 15 бит. Тогда, на основе (4), получим информационные основания кода ПСКВ $p_1(x) = x^5 + x^4 + x^3 + x^2 + 1$, $p_2(x) = x^5 + x^3 + x^2 + x + 1$, $p_3(x) = x^5 + x^4 + x^3 + x + 1$. В этом случае рабочий диапазон равный $M_3(x) = x^{15} + x^{11} + x^{10} + x^2 + 1$. В качестве избыточных оснований выбираем $p_4(x) = x^5 + x^2 + 1$ и $p_5(x) = x^5 + x^3 + 1$. В качестве секретных параметров имеем:

$$W(j) = W_1(j) \| W_2(j) \| W_3(j) \| W_4(j) \| W_5(j) = \\ = 00111 \| 00011 \| 00101 \| 01010 \| 01110 = 7_{10} \| 3_{10} \| 5_{10} \| 10_{10} \| 14_{10}.$$

$$Q(j) = Q_1(j) \| Q_2(j) \| Q_3(j) \| Q_4(j) \| Q_5(j) = \\ = 01010 \| 00100 \| 00011 \| 00101 \| 01010 = 10_{10} \| 4_{10} \| 3_{10} \| 5_{10} \| 10_{10}.$$

$$E(j) = E_1(j) \| E_2(j) \| E_3(j) \| E_4(j) \| E_5(j) = \\ = 00100 \| 00011 \| 00011 \| 01011 \| 00101 = 4_{10} \| 3_{10} \| 3_{10} \| 11_{10} \| 5_{10}.$$

Перед выполнением j-го сеанса связи ответчик системы опознавания получает «истинный» статус КА с помощью выражения (6):

$$O: \begin{cases} A_1^j(x) = \left| x^7 \cdot x^{10} \cdot x^4 \right|^+_{x^5+x^4+x^3+x^2+1} = \left| x^{21} \right|^+_{x^5+x^4+x^3+x^2+1} = x^2 + x = 6_{10} \\ A_2^j(x) = \left| x^3 \cdot x^4 \cdot x^3 \right|^+_{x^5+x^3+x^2+x+1} = \left| x^{10} \right|^+_{x^5+x^3+x^2+x+1} = x^3 + x + 1 = 11_{10} \\ A_3^j(x) = \left| x^5 \cdot x^3 \cdot x^3 \right|^+_{x^5+x^4+x^3+x+1} = \left| x^{11} \right|^+_{x^5+x^4+x^3+x+1} = x^3 + x^2 + x = 14_{10} \\ A_4^j(x) = \left| x^{10} \cdot x^5 \cdot x^{11} \right|^+_{x^5+x^2+1} = \left| x^{26} \right|^+_{x^5+x^2+1} = x^4 + x^2 + x + 1 = 23_{10} \\ A_5^j(x) = \left| x^{14} \cdot x^{10} \cdot x^5 \right|^+_{x^5+x^3+1} = \left| x^{29} \right|^+_{x^5+x^4+x^3+x+1} = x^3 + x = 10_{10} \end{cases}$$

Ответчик выбирает случайные числа, чтобы внести зашумление в секретные параметры. Пусть он выбрал:

$$\Delta W(j) = (3,5,9,13,6),\ \Delta Q(j) = (2,4,12,18,17)\ \Delta E_i(j) = (2,6,7,2,5).$$

В результате применения выражения (8) получили:

$$O:\tilde{W}_1(j)=\left|7+3\right|_{31}^{+}=10,\ \tilde{W}_2(j)=\left|3+5\right|_{31}^{+}=8,\ \tilde{W}_3(j)=\left|5+9\right|_{31}^{+}==14,$$
$$\tilde{W}_4(j)=\left|10+13\right|_{31}^{+}=23,\ \tilde{W}_5(j)=\left|14+6\right|_{31}^{+}=20.$$
$$O:\tilde{Q}_1(j)=\left|10+2\right|_{31}^{+}=12,\ \tilde{Q}_2(j)=\left|4+4\right|_{31}^{+}=8,\tilde{Q}_3(j)=\left|3+12\right|_{31}^{+}=15,$$
$$\tilde{Q}_4(j)=\left|5+18\right|_{31}^{+}=23,\tilde{Q}_5(j)=\left|10+17\right|_{31}^{+}=27.$$
$$O:\tilde{E}_1(j)=\left|4+2\right|_{31}^{+}=6,\tilde{E}_2(j)=\left|3+6\right|_{31}^{+}=9,\tilde{E}_3(j)=\left|3+7\right|_{31}^{+}=10,$$
$$\tilde{E}_4(j)=\left|11+2\right|_{31}^{+}=13,\tilde{E}_5(j)=\left|5+5\right|_{31}^{+}=10.$$

Полученные искаженные параметры ответчик использует для вычисления «искаженного» статуса спутника:

$$O:\begin{cases}\tilde{A}_1^j(x)=\left|x^{10}\cdot x^{12}\cdot x^{6}\right|_{x^5+x^4+x^3+x^2+1}^{+}=\left|x^{28}\right|_{x^5+x^4+x^3+x^2+1}^{+}=x^4+x^3+1=25_{10}\\ \tilde{A}_2^j(x)=\left|x^{8}\cdot x^{8}\cdot x^{9}\right|_{x^5+x^3+x^2+x+1}^{+}=\left|x^{25}\right|_{x^5+x^3+x^2+x+1}^{+}=x^3+x=10_{10}\\ \tilde{A}_3^j(x)=\left|x^{14}\cdot x^{15}\cdot x^{10}\right|_{x^5+x^4+x^3+x+1}^{+}=\left|x^{8}\right|_{x^5+x^4+x^3+x+1}^{+}=x^3+x^2+x+1=15_{10}\\ \tilde{A}_4^j(x)=\left|x^{23}\cdot x^{23}\cdot x^{13}\right|_{x^5+x^2+1}^{+}=\left|x^{28}\right|_{x^5+x^2+1}^{+}=x^4+x^2+x=22_{10}\\ \tilde{A}_5^j(x)=\left|x^{20}\cdot x^{27}\cdot x^{10}\right|_{x^5+x^3+1}^{+}=\left|x^{26}\right|_{x^5+x^3+1}^{+}=x^3+x+1=11_{10}\end{cases}$$

Пусть «вопросом», поступившим от запросчика, является число:

$$C(j)=C_1(j)\|C_2(j)\|C_3(j)\|C_4(j)\|C_5(j)=$$
$$=00010\|00111\|01111\|01001\|10001=2_{10}\|7_{10}\|15_{10}\|9_{10}\|17_{10}.$$

Ответчик принимает сигнал, поступивший от запросчика, и вычисляет:

$$O:H_1^1(j)=\left|10-2\cdot7\right|_{31}^{+}=27,\ H_2^1(j)=\left|8-7\cdot3\right|_{31}^{+}=18,\ H_3^1(j)=\left|14-15\cdot5\right|_{31}^{+}=1,$$
$$H_4^1(j)=\left|23-9\cdot10\right|_{31}^{+}=26,\ H_5^1(j)=\left|20-17\cdot14\right|_{31}^{+}=30.$$
$$O:H_1^2(j)=\left|12-2\cdot10\right|_{31}^{+}=23,\ H_2^2(j)=\left|8-7\cdot4\right|_{31}^{+}=11,\ H_3^2(j)=\left|15-15\cdot3\right|_{31}^{+}=1,$$
$$H_4^2(j)=\left|23-9\cdot5\right|_{31}^{+}=9,\ H_5^2(j)=\left|27-17\cdot10\right|_{31}^{+}=12.$$
$$O:H_1^3(j)=\left|6-2\cdot4\right|_{31}^{+}=29,\ H_2^3(j)=\left|9-7\cdot3\right|_{31}^{+}=19,\ H_3^3(j)=\left|10-15\cdot3\right|_{31}^{+}=27,$$
$$H_4^3(j)=\left|20-9\cdot14\right|_{31}^{+}=7,\ H_5^3(j)=\left|10-17\cdot5\right|_{31}^{+}=18.$$

Процесс вычисления ответов на вопрос закончен. Ответчик формирует свой сигнал, который будет передан запросчику:

$$O:\{(6,11,14,23,10)(25,10,15,22,11)(27,18,1,26,30)(23,11,1,9,12)(29,19,27,7,18)\}.$$

Получив сигнал ответчика, запросчик должен его проверить. Получаем:

$$3:\begin{cases} P_1^j(x)=\left|\left(x^2+x\right)^2 x^{27}\cdot x^{23}\cdot x^{29}\right|^{+}_{x^5+x^4+x^3+x^2+1}=x^4+x^3+1=\tilde{A}_1^j(x) \\ P_2^j(x)=\left|\left(x^3+x+1\right)^7 x^{18}\cdot x^{11}\cdot x^{19}\right|^{+}_{x^5+x^3+x^2+x+1}=x^3+x=\tilde{A}_2^j(x) \\ P_3^j(x)=\left|\left(x^3+x^2+x\right)^{15} x\cdot x\cdot x^{27}\right|^{+}_{x^5+x^4+x^3+x+1}=x^3+x^2+x+1=\tilde{A}_3^j(x) \\ P_4^j(x)=\left|\left(x^4+x^2+x+1\right)^9 x^{26}\cdot x^9\cdot x^7\right|^{+}_{x^5+x^2+1}=x^4+x^2+x=\tilde{A}_4^j(x) \\ P_5^j(x)=\left|\left(x^3+x^2\right)^{17} x^{30}\cdot x^{18}\cdot x^{20}\right|^{+}_{x^5+x^3+1}=x^3+x+1=\tilde{A}_5^j(x) \end{cases}$$

Так как условие (14) выполняется, то запросчик генерирует сигнал «свой». После этого КА получает возможность организовать сеанс связи.

Использование модифицированного алгоритма позволяет корректировать ошибки, возникающие при вычислении статусов спутника и проверки правильности полученных ответов.

Для данной системы оснований вычислим ортогональные базисы информационных оснований, удовлетворяющие условию (24). Тогда имеем:

$$B_1(x)=x^{14}+x^{13}+x^{11}+x^9+x^8+x^7+x^5+x^3+x+1,$$
$$B_2(x)=x^{12}+x^{11}+x^8+x^4+x^3+x^2+1,$$
$$B_3(x)=x^{14}+x^{13}+x^{12}+x^9+x^7+x^5+x^2+x+1.$$

Воспользуемся выражением (26) и вычислим модифицированные константы нулевизации для истинного статуса спутника:

$$A^j(x)=(x^2+x, x^3+x+1, x^3+x^2+x, x^4+x^2+x+1, x^3+x).$$

Получаем следующие значения:

$$\hat{A}_1(x)=(x^2+x,\ 0,\ 0,\ x^3,\ x^4+1);$$
$$\hat{A}_2(x)=(0,\ x^3+x+1,\ 0, x^3+x+1, x+1);$$
$$\hat{A}_3(x)=(0,\ 0,\ x^3+x^2+x, 0, 0, x^4+x^2, x^4+x^3).$$

Тогда след кода имеет вид:

$$\theta_4(x) = A_4(x) - \sum_{i=1}^{3} p_4^i(x) = (x^4 + x^2 + x + 1) - (x^3 + (x^3 + x + 1) + (x^4 + x^2)) = 0,$$
$$\theta_5(x) = A_5(x) - \sum_{i=1}^{3} p_5^i(x) = (x^3 + x) - ((x^4 + 1) + (x + 1) + (x^4 + x^3)) = 0.$$

Так как след кода равен нулю, то комбинация не имеет ошибки. Пусть при вычислении истинного статуса произошла ошибка по первому остатку глубиной $\Delta A_1(x) = 1$, то есть $\widehat{A}_1(x) = A_1(x) + \Delta A_1(z) = (x^2 + x) + 1 = x^2 + x + 1$. Тогда истинный статус КА имеет вид:

$$\widehat{A}^j(x) = (x^2 + x + 1, x^3 + x + 1, x^3 + x^2 + x, x^4 + x^2 + x + 1, x^3 + x).$$

Модифицированные коэффициенты нулевизации имеют вид:

$$\hat{A}_1(x) = (x^2 + x + 1,\ 0,\ 0,\ x^4 + x + 1,\ x^4);$$
$$\hat{A}_2(x) = (0,\ x^3 + x + 1,\ 0, x^3 + x + 1, x + 1);$$
$$\hat{A}_3(x) = (0,\ 0,\ x^3 + x^2 + x, 0, 0, x^4 + x^2, x^4 + x^3).$$

Тогда след кода имеет вид:

$$\theta_4(x) = A_4(x) - \sum_{i=1}^{3} p_4^i(x) = (x^4 + x^2 + x + 1) - ((x^4 + x + 1) + (x^3 + x + 1) + x^4) =$$
$$= x^4 + x^3 + x + 1,$$
$$\theta_5(x) = A_5(x) - \sum_{i=1}^{3} p_5^i(x) = (x^3 + x) - (x^4 + (x + 1) + (x^4 + x^3)) = 1.$$

Так как след кода не равен нулю, то истинный статус, представленный в коде ПСКВ, содержит ошибку. По значению ПХ величины следа можно построить вектор ошибки, который имеет вид:

$$e(x) = (1,\ 0,\ 0,\ 0,\ 0).$$

Корректировка ошибочного истинного статуса КА реализуется:

$$A^j(x) = \widehat{A}^j(x) - \bar{e}(x) = (x^2 + x + 1 - 1, x^3 + x + 1, x^3 + x^2 + x, x^4 + x^2 + x + 1, x^3 + x) =$$
$$= (x^2 + x, x^3 + x + 1, x^3 + x^2 + x, x^4 + x^2 + x + 1, x^3 + x).$$

В результате ошибка исправлена.

В ходе исследований были определена связь между значением следа кода и местоположением ошибки в кодовой комбинации. Полученные

результаты показали, что использование двух контрольных оснований позволяет исправить все однократные ошибки в коде ПСКВ.

Для оценки эффективности предложенного модифицированного алгоритма вычисления ПХ кода ПСКВ, была разработана структурная модель блока коррекции ошибки в модулярном коде. При этом была использована FPGA Xilinx Artix-7 и новая САПР Vivado HLS 2019.1. Сравнительный анализ проводился с методом нулевизации. При проведении сравнительного анализа были выбраны восемь неприводимых полиномов $GF(2^6)$. При этом полиномы 6D и 73 использовались в качестве контрольных оснований кода ПСКВ. Время, необходимое на выполнение метода нулевизации, составило 62 нс. При использовании модифицированного алгоритма время вычисления позиционной характеристики 34 нс. То есть, временные затраты были сокращены в 1,83 раза. Дальнейшее сокращение возможно, если блок вычисления ПХ след кода реализовать с использованием многовходовых сумматоров по модулю два.

Выводы

В статье показан метод аутентификации космического аппарата, построенный с использованием доказательства с нулевым разглашением и реализованный в модулярном коде. Показано, что использование кодов полиномиальной системы классов вычетов ПСКВ позволяет не только уменьшать время, необходимое на определение статуса спутника, но и обнаруживать и корректировать ошибки, возникающие в процессе работы системы опознавания. Чтобы снизить временные затраты на выполнение данных процедур, была выполнена модификация метода нулевизации кода ПСКВ. Изменение констант нулевизации позволило заменить итерационный алгоритм вычисления позиционный характеристики след кода на параллельный, в котором участвуют остатки контрольных оснований. Для оценки эффективности модифицированного кода была разработана

структурная модель блока коррекции с использованием FPGA Xilinx Artix-7. Проведенные исследования показали, что время, необходимое на выполнение метода нулевизации при использовании восьми шестиразрядных оснований кода ПСКВ, составило 62 нс. При использовании модифицированного алгоритма время вычисления позиционной характеристики 34 нс. То есть, временные затраты на обнаружение и коррекцию ошибки в коде ПСКВ были сокращены в 1,83 раза.

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

Литература

1. Андреева Е. В., Исаулова К.Я. Перспективы развития СМП // Деловой журнал «Neftegaz.RU», 2021, №6. С. 30-37.

2. Чипига А.Ф., Павлюк Д.Н. Разработка метода аутентификации для обеспечения информационной скрытности низкоорбитальной группировки космических аппаратов // Инженерный вестник Дона, 2020, №4. URL: ivdon.ru/ru/magazine/archive/n4y2020/6416.

3. Чистоусов Н.К. Калмыков И.А., Чипига А.Ф., Калмыкова Н.И. Разработка протоколов аутентификации низкоорбитальных космических аппаратов на основе параллельных кодов систем остаточных классов // Инженерный вестник Дона, 2021, №4. URL: ivdon.ru/ru/magazine/archive/n4y2021/6912

4. Olenev A., Kalmykova N. Development of Algorithms for Increasing the Information Secrecy of the Satellite Communication System Based on the Use of Authentication Technology // Advanced in Information Security Management and Applications, 2021, Volume 3094. pp. 59-64.

5. Чистоусов Н.К., Калмыков И.А., Духовный Д.В., Емельянов Е.А. Модификация метода аутентификации низкоорбитальных спутников на

основе кодов полиномиальной системы классов вычетов // Современные наукоемкие технологии, 2022, № 2. С. 164-169.

6. Емарлукова Я.В., Гиш Т.А., Дунин А.В., Макарова А.В., Гостев Д.В. Математические модели и схемные решения отказоустойчивых непозиционных вычислительных систем: коллективная монография. Ставрополь: Изд-во СКФУ, 2016. 216 с.

7. Mohan A. Residue Number Systems. Theory and Applications. Springer International Publishing Switzerland, 2016. 351 p.

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

9. Chu J., Benaissa M. Error Detecting AES Using Polynomial Residue Number System // Microprocessors and Microsystems, 2013, no 37. pp. 228-234.

10. Петрова Е.В., Степанова Е.П., Калмыков, М.И. Схемная реализация генератора псевдослучайной функции повышенной эффективности // Инфокоммуникационные технологии в науке, производстве и образовании (Инфоком-6): сборник научных трудов шестой международной научно-технической конференции. Ставрополь. 2014. С. 240-243.

11. Pashintsev V., Tyncherov K., Olenev A. Error-Correction Coding Using Polynomial Residue Number System. Applied Sciences. 2022. 12(7). URL: doi.org/10.3390/app12073365

12. Мартыненко С.О., Краснобаев В. А. Метод обнаружения ошибок в спецпроцессоре обработки криптографической информации // Радиоэлектроника и информатика, 2010, № 1. с. 74-78.

References

1. Andreyeva Ye. V., Isaulova K.YA. Delovoy zhurnal «Neftegaz.RU», 2021, №6. pp. 30-37

2. Chipiga A.F., Pavlyuk D.N. Inzhenernyj vestnik Dona, 2020, №4. URL: ivdon.ru/ru/magazine/archive/n4y2020/6416

3. Chistousov N.K. Kalmykov I.A., Chipiga A.F., Kalmykova N.I. Inzhenernyj vestnik Dona, 2021, № 4. URL: ivdon.ru/ru/magazine/archive/n4y2021/6912

4. Olenev A., Kalmykova N. Advanced in Information Security Management and Applications, 2021, Volume 3094. pp. 59-64.

5. Chistousov N.K., Kalmykov I.A., Dukhovnyy D.V., Yemel'yanov Ye.A. Sovremennyye naukoyemkiye tekhnologii. 2022, № 2. pp. 164-169.

6. Yemarlukova YA.V., Gish T.A., Dunin A.V., Makarova A.V., Gostev D.V. Matematicheskiye modeli i skhemnyye resheniya otkazoustoychivykh nepozitsionnykh vychislitelnykh sistem: kollektivnaya monografiya [Mathematical models and circuit solutions of fault-tolerant non-positional computing systems: collective monograph]. Stavropol: Izd-vo SKFU, 2016. 216 p.

7. Mohan A. Residue Number Systems. Theory and Applications. Springer International Publishing Switzerland, 2016. 351 p.

8. Chervyakov N. I., Kolyada A. A., Lyakhov P. A. Modulyarnaya arifmetika i ee prilozheniya v infokommunikacionnyh tekhnologiyah [Modular arithmetic and its applications in infocommunication technologies]. M.: FIZMATLIT, 2017. 400 p.

9. Chu J., Benaissa M. Microprocessors and Microsystems, 2013, no 37. pp. 228-234.

10. Petrova Ye. V., Stepanova Ye. P., Kalmykov, M. I. Infokommunikatsionnyye tekhnologii v nauke, proizvodstve i obrazovanii (Infokom-6): sbornik nauchnykh trudov shestoy mezhdunarodnoy nauchno-tekhnicheskoy konferentsii. Stavropol, 2014. pp. 240-243.

11. Pashintsev V., Tyncherov K., Olenev A. Applied Sciences. 2022, 12(7). URL: doi.org/10.3390/app12073365.

12. Martynenko S.O., Krasnobayev V. A. Radioelektronika i informatika, 2010, № 1. pp. 74-78