УДК 004.052.42 DOI 10.18522/2311-3103-2024-5-271-282

И.А. Калмыков, И.Д. Ефременков, Д.В. Духовный

ПОМЕХОУСТОЙЧИВЫЙ ПРОТОКОЛ ОПОЗНАВАНИЯ НИЗКООРБИТАЛЬНОГО СПУТНИКА-РЕТРАНСЛЯТОРА

Освоение месторождений в районах Крайнего Севера относится к глобальным проектам, которые реализует Российская Федерация. Эффективный контроль и мониторинг состояния необслуживаемых объектов (НО), занимающихся промыслом углеводородов, достоверное доведение до них команд управления возможно только с помощью низкоорбитальных спутников (НС), объединенных в одну группировку. Однако по мере расширения числа стран, участвующих в разработке месторождений в районах Крайнего Севера, будет расти и количество группировок НС. В результате этого приемник, расположенный на НО, будет видеть сразу несколько спутников-ретрансляторов. При этом НС-злоумышленник (НСЗ) может попытаться навязать приемнику перехваченную ранее команду управления, что может привести к выходу из строя НО. Предотвратить возможность навязывания такой спуфинг-помехи можно с помощью системы опознавания низкоорбитального спутника (СОНС). Эффективность работы СОНС во многом зависит от протокола опознавания. Для повышения скорости проведения аутентификации НС в ряде работ предлагается использовать протокол с нулевым разглашением знаний, который выполняется в модулярных кодах (МК). Данный результат достигается за счет параллельного выполнения арифметических операций по основаниям кода. Однако это свойство МК можно использовать для повышения помехоустойчивости СОНС, которая должна функционировать в различной погодных условиях. Цель – разработка помехоустойчивого протокола опознавания НС-ретранслятора, выполняемого в модулярном коде и требующего меньшего времени на коррекцию ошибок.

Протокол опознавания с нулевым разглашением знаний; модулярные коды; поиск и коррекция ошибок; позиционные характеристики.

I.A. Kalmykov, I.D. Efremenkov, D.V. Dukhovnyj

NOISE-RESISTANT LOW-ORBIT REPEATER SATELLITE IDENTIFICATION PROTOCOL

The development of deposits in the Far North is one of the global projects implemented by the Russian Federation. Effective control and monitoring of the condition of unattended objects (UO) engaged in hydrocarbon fishing, reliable communication of control commands to them is possible only with the help of low-orbit satellites (LOS) combined into one grouping. However, as the number of countries involved in the development of deposits in the Far North expands, the number of LOS groupings will also grow. As a result, the receiver located on the UO will see several repeater satellites at once. In this case, a low-orbit intruder satellite (LOIS) may try to impose a previously intercepted control command on the receiver, which may lead to the failure of the UO. To prevent the possibility of imposing such spoofing interference, you can use the low-orbit satellite identification system (LSIS). The effectiveness of the LSIS depends largely on the identification protocol. In order to increase the speed of authentication of the NS, in a number of works it is proposed to use a zero-knowledge protocol, which is performed in modular codes (MC). This result is achieved by parallel execution of arithmetic operations on the basis of the code. However, this property of the MC can be used to increase the noise immunity of the LSIS, which must function in various weather conditions. The goal is to develop a noise-resistant protocol for recognizing an LOS-repeater, executed in modular code and requiring less time for error correction.

Zero-knowledge recognition protocol; modular codes; error detection and correction; positional characteristics.

Введение. Одним из перспективных глобальных проектов развития Крайнего Севера нашей Родины является разработка и освоение месторождений углеводородов, находящихся в данном регионе. Так как эти месторождения находятся в труднодоступной местности с суровой климатической обстановкой, то добыча и транспортировка углеводородов будет организована с помощью необслуживаемых объектов (НО). Благодаря своим достоинствам, позволяющим повысить эффективность мониторинга, контроля и управления такими необслуживаемыми объектами, снизить вероятности их

выхода из строя, а также уменьшить себестоимость продукции, технологии промышленного интернета вещей (IIoT) нашли широкое применение в нефтегазодобывающую отрасль (НГДО) [1, 2].

Обеспечить достоверное получение информации от НО и доведение до них соответствующих команд управления, возможно только с помощью низкоорбитальных спутников (НС), объединенных в группировку. Перспективность месторождений, находящихся на шельфе Северного Ледовитого океана, стала стимулом к расширению числа стран, участвующих в их разработке. При этом, очевидно, будет расти и количество группировок низкоорбитальных спутников. В результате этого приемники, расположенные на НО, будут видеть в зоне своего приема сразу несколько спутников-ретрансляторов. При этом НС-злоумышленник (НСЗ) может осуществить деструктивное воздействие на необслуживаемый объект. Для этого он сначала осуществляет перехват сигнала (команды), которая передается на НО. Затем он ее, задержав на некоторое время, пытается навязать приемнику. Так как параметры задержанного сигнала являются известными приемнику, то он передает навязанную команду в систему управления НО. В результате этого объект может выйти из строя, и даже вызвать экологическую катастрофу.

Предотвратить возможность навязывания такой спуфинг-помехи можно с помощью системы опознавания низкоорбитального спутника (СОНС). Данная система сначала проводит аутентификацию НС, а затем, если спутник «свой», ему выделяется канал связи. Очевидно, что эффективность работы такой СОНС во многом зависит от применяемого протокола опознавания. В работах [3, 4] представлен протокол опознавания с нулевым разглашением знаний, который обеспечивает аутентификацию НС за меньшее время по сравнению с другими протоколами. Для повышения скорости проведения аутентификации НС в ряде работ [5–7] предлагается выполнять данный протокол в модулярных кодах (МК). Данный результат достигается за счет параллельного выполнения арифметических операций по основаниям кода. При этом независимость остатков МК друг от друга можно использовать для выполнения поиска и коррекции ошибок, возникающих из-за пачек помех. Это свойство МК можно использовать для повышения помехоустойчивости СОНС, которая должна эффективно функционировать в различной погодных условиях. Цель статьи – разработка помехоустойчивого протокола опознавания НС-ретранслятора, выполняемого в модулярном коде и требующего меньшего времени на коррекцию ошибок.

Постановка задачи исследования. Кодовая комбинация МК представляет собой кортеж остатков, которые сравнимы с целым числом X по модулю оснований $m_1, m_2, ..., m_k$, где $\underset{i \neq j}{НОД}(m_i, m_j) = 1,\ i,\ j = 1, ..., k$,

$$X = (X_1, X_2, ..., X_k), \tag{1}$$

где $X_i \equiv X \bmod m_i,\ i = 1, ..., k$.

Согласно работам [8–10] в МК эффективно выполняются следующие модульные операции , т.е. сложение, вычитание и умножение

$$X + C = ((X_1 + C_1) \bmod m_1, ..., (X_k + C_k) \bmod m_k), \tag{2}$$

$$X - C = ((X_1 - C_1) \bmod m_1, ..., (X_k - C_k) \bmod m_k), \tag{3}$$

$$X \cdot C = ((X_1 \cdot C_1) \bmod m_1, ..., (X_k \cdot C_k) \bmod m_k), \tag{4}$$

где $C_i = C \bmod m_i;\ i = 1, ..., k$.

Для получения правильного ответа необходимо чтобы результаты выражений (2)–(4) не превышали рабочий диапазон, который равен

$$M_k = \prod_{i=1}^{k} m_i \cdot \tag{5}$$

Анализ выражений (2)–(4) показывает – в МК операции сложения, вычитания и умножения выполняются параллельно, а это способствует повышению скорости вычислений. Это свойство МК было использовано для обеспечения более высокой степени ими-

тостойкости СОНС. Известно [11, 12], что в протоколах аутентификации с нулевым разглашением их имитостойкость определяется не применением шифрования, а за счет выполнения вычислений по модулю большого простого числа *D*. Так как основной операцией в этих протоколах является возведение в степень по модулю *D*, то это негативно сказывается на скорости опознавания НС-ретранслятора. В результате НСЗ появляется дополнительно время на подбор сигнала ответчика, что приводит к снижению имитостойкости СОНС и увеличению вероятности пропуска данного спутника. Чтобы повысить скорость опознавания НС без снижения имитостойкости СОНС в работе [5] были разработаны протоколы аутентификации с нулевым разглашением, который выполнялись в МК. Реализация этих протоколов на ПЛИС Kintex UltraScale (xcku3p-ffva676-1-e) показала, что для выполнения одномодульного протокола Фиат-Шамира потребовалось 21,34 мкс, а при использовании МК – 4,957 мкс. Меньшее время на опознавание, которое составило 3,912 мкс, требует одномодульный бесключевой протокол [3]. Применение МК в данном протоколе позволило снизить временные затраты на опознавание до 1,6 мкс.

Основным недостатком бесключевого протокола в модулярном коде является его низкая помехоустойчивость. Применение МК имело целью за счет распараллеливания вычислений повысить скорость опознавания НС. Однако МК, благодаря тому, что вычисления выполняются независимо по основаниям, могут корректировать ошибочные остатки в кодовых комбинациях. Для этого необходимо ввести в набор оснований дополнительные избыточные модули. Известно [13–15], что расширение набора оснований на два контрольных основания m_{k+1}, m_{k+2} позволяет корректировать однократную ошибку в МК. В этом случае избыточный МК сможет исправлять один ошибочный остаток. Для этого к этим основания предъявляются следующее требование

$$m_{k+1}m_{k+2} > m_{k-1}m_k. \tag{6}$$

Чтобы обеспечить коррекцию пачки ошибок в принятой кодовой комбинации, кратность которой равна $\gamma_{ПО}$, необходимо ввести дополнительно $\rho = 2\gamma_{ПО}$ контрольных оснований. Это приведет к расширению диапазона возможных кодовых комбинаций

$$M_{k+\rho} = \prod_{i=1}^{k+\rho} m_i = M_k \prod_{i=k+1}^{k+\rho} m_i = M_k M_\rho^*. \tag{7}$$

Считается, комбинация МК является разрешенной (она не содержит ошибки), если имеет место неравенство

$$X = (X_1, ..., X_k, X_{k+1}, ..., X_{k+\rho}) < M_k. \tag{8}$$

При наличии в избыточной комбинации МК пачки ошибок кратности $\gamma_{ПО}$ и меньше условие (8) нарушается. Так как основой для классификации принятой комбинации на разрешенные и ошибочные является положение числа *X* относительно рабочего диапазона M_k, то для поиска и коррекции ошибок в МК используются позиционные характеристики (ПХ).

Характерной чертой МК является наличие множества алгоритмов вычисления ПХ, с помощью которых можно выполнить поиск и коррекцию ошибок в МК. Одним из первых алгоритмов, позволяющих корректировать ошибки в МК, был разработан алгоритм проекции [16, 17]. Проекция получается из исходной избыточной комбинации $X = (X_1, X_2, X_3, ..., X_{k+\rho})$ путем удаления одного остатка. Так при удалении первого остатка X_1 получается проекция $\hat{X}^1 = (X_2, X_3, ..., X_{k+\rho})$. Если удалить второй остаток X_2, то получаем вторую проекцию $\hat{X}^2 = (X_1, X_3, ..., X_{k+\rho})$. Процедура выполняется для всех оставшихся остатков. После получения j-ой проекции $\hat{X}^o = (X_1, ..., X_{j-1}, X_{j+1}, ..., X_{k+\rho})$ к ней применяется обратное преобразование из МК в позиционный код (ПК). Для выполнения преобразования МК-ПК часто применяют Китайскую терему об остатках (КТО) [16]

$$\hat{X}^j = \sum_{\substack{i=1 \\ i\neq j}}^{k+\rho} X_i B_i^j \bmod M_{k+\rho}^j = \left| X_1 B_1^j + \ldots + X_{j-1} B_{j-1}^j + X_{j+1} B_{j+1}^j + \ldots + X_{k+\rho} B_{k+\rho}^j \right|_{M_{k+\upsilon}^j}, \quad (9)$$

где $B_i^j = M_{k+\rho}^j w_i \big/ m_i$ – ортогональные базисы;

$M_{k+\rho}^j = M_{k+\rho} \big/ m_j$; $B_i^j = 1 \bmod m_i$; $w_i \left| B_i^j \right|_{m_i}^+ = 1 \bmod m_i$.

Если из-за ошибки исказился *j*-й остаток, то все проекции будут больше рабочего диапазона за исключением текущей проекции

$$\left\{ \hat{X}_1, \ldots, \hat{X}_{j-1}, \hat{X}_{j+1}, \ldots, \hat{X}_{k+\rho} \right\} > M_k, \left\{ \hat{X}_j \right\} < M_k. \quad (10)$$

Основным недостатком данного алгоритма являются большие временные затраты на определение данной позиционной характеристики.

В работах [18, 19] для коррекции ошибок предлагается использовать старшие коэффициенты полиадической системы счисления (ПСС). Известно, что целое число *X* можно представить в виде коэффициентов ПСС $(S_1, S_2, \ldots, S_{k+\rho})$, используя равенство

$$X = S_1 + S_2 m_1 + S_2 m_1 m_2 + \ldots + S_k \prod_{i=1}^{k-1} m_i + S_{k+1} M_k + \ldots + S_{k+\rho} M_k \prod_{j=k+1}^{k+\rho-1} m_j. \quad (11)$$

Анализ выражения (11) показывает, что если выполняется условие (8), т.е. комбинация МК не содержит ошибки, старшие коэффициенты ПСС должны иметь значение $S_{k+1} = 0, S_{k+2} = 0, \ldots, S_{k+\rho} = 0$. Если эти коэффициенты будут отличаться от нуля, то это означает, что комбинация МК является ошибочной. Для вычисления коэффициентов ПСС, используя модулярный код, в работе [18] был предложен итерационный алгоритм

$$\begin{aligned} S_1 &= X_1, \\ S_2 &= ((X_2 - S_1) u_{12}) \bmod m_2, \\ &\vdots \\ S_{k+\rho} &= ((S_{k+\rho} + S_1) u_{1k+\rho} + S_2) u_{2k+\rho} + \ldots + S_{k+\rho=1} u_{(k+\rho+1)(k+\rho)}) \bmod m_{k+\rho}, \end{aligned} \quad (12)$$

где $u_{ji} = \left(1 \big/ m_j\right) \bmod m_i = m_j^{-1} \bmod m_i$; $i = 1, \ldots, k+\rho$.

В качестве недостатка алгоритма (12) перевода МК-ПСС можно выделить значительные временные затраты из-за итерационного процесса выполнения.

Довольно часто в алгоритмах коррекции ошибок в МК применяется ПХ – интервал числа [19, 20]. Данная ПХ имеет простой физический смысл, определяемый выражением

$$L = \left[X / M_k \right], \quad (13)$$

где [*] – целая часть частного.

Если комбинация МК является разрешенной, то выполняется условие (8). Так как число *X* меньше рабочего диапазона, то *L* = 0. Если комбинация МК содержит ошибки, то по интервалу $L \neq 0$ можно провести их коррекцию. В работе [21] авторы предлагают вычислять *L* с помощью функции Эйлера

$$L = \left| \sum_{i=1}^{k+\rho} \left| S_{X_i} X_i \right|_{M_k}^+ \right|_{M_k}^+, \quad (14)$$

где $S_{X_i} = \left| M_i^{\varphi(m_i)} \left(M_{k+\rho} \right)^{-1} \right|_{M_k}^+$; $\varphi(m_i)$ – функция Эйлера числа m_i; $M_i = \dfrac{M_{k+\rho}}{m_i}$.

К основным недостаткам текущего алгоритма можно отнести большие временные затраты на вычисление ПХ. Уменьшить время необходимое на нахождение интервала числа позволяет разработанный алгоритм коррекции пачек ошибок. В основе алгоритма лежит изоморфизм КТО. Если в выражение (13) подставить (9), используемое для выполнения преобразования МК-ПК, то

$$L = \left[\sum_{i=1}^{k+\rho} X_i B_i - r_X M_{k+\rho} \Big/ M_k \right], \tag{15}$$

где r_x – ранг числа X, представленного по информационным основаниям МК.

Представим ортогональные базисы оснований $m_1, m_2, ..., m_k$ в виде

$$B_i = \left[B_i / M_k \right] \cdot M_k + \ddot{B}_i = K_i M_k + \ddot{B}_i, \tag{16}$$

где $\ddot{B}_i$ – ортогональные базисы МК с основаниями $m_1, ..., m_k$; $\ddot{B}_i \equiv B_i \bmod M_k$; $i = 1,2,...,k$.

Для контрольных оснований, где $i = k+1,...,k+\rho$, справедливо равенство

$$B_i = K_i M_k. \tag{17}$$

Для перехода от вычисления целой части частого в (15) к модульным операциям воспользуемся свойством полного диапазона избыточного МК. Из выражения (7) видно, что полный диапазон $M_{k+\rho}$ больше рабочего диапазона разрешенных комбинаций M_k в M_ρ^* раз. Другими словами в состав $M_{k+\rho}$ входит M_ρ^* рабочих диапазонов M_k. При этом каждый рабочий диапазон имеет свой номер от 0 до $M_\rho^* - 1$. Значит равенство (15) можно представить как

$$L = \left| \sum_{i=1}^{k+\rho} X_i B_i - r_X M_{k+\rho} \Big/ M_k \right|_{M_\rho^*}^{+}. \tag{18}$$

Подставим выражения (16) и (17) в последнее выражение. Тогда

$$L = \left| \sum_{i=1}^{k+\rho} X_i K_i + \left[\frac{\sum_{j=1}^{k} X_j \ddot{B}_j}{M_k} \right] \right|_{M_\rho^*}^{+} = \left| \sum_{i=1}^{k+\rho} X_i K_i + \ddot{r}_X \right|_{M_\rho^*}^{+}, \tag{19}$$

где $\ddot{r}_X$ – ранг числа X, представленного в МК с основаниями $m_1, m_2, ..., m_k$.

Алгоритм, описываемый выражением (19) имеет ряд недостатков. Во-первых, вычисление ПХ осуществляется по модулю, который представляет собой произведение контрольных оснований $M_\rho^* = \prod_{ш=k+1}^{k+\rho} m_i$. Это влечет за собой увеличение аппаратурных затрат. Во-вторых, чтобы вычислить ПХ необходимо выполнить $k+\rho$ операций умножения остатков кода на константы K_i, где $i = 1,2,...,k+\rho$ и столько же операций сложения по модулю M_ρ^*.

Для устранения отмеченных было предложено использовать изоморфизм Китайской теоремы об остатках. Данное свойство КТО позволяет свети вычисление выражения (19) к ρ параллельным вычислений ПХ по контрольным модулям. Получаем

$$L_{k+1} = |L|^{+}_{m_{k+1}} = \left| \sum_{i=1}^{k} X_i \left| K_i \right|^{+}_{m_{k+1}} + X_{k+1} \left| K_{k+1} \right|_{m_{k+1}} + \ddot{\ddot{r}}_X \right|^{+}_{m_{k+1}},$$
$$\vdots \qquad (20)$$
$$L_{k+\rho} = |L|^{+}_{m_{k+\rho}} = \left| \sum_{i=1}^{k} X_i \left| K_i \right|^{+}_{m_{k+\rho}} + X_{k+\rho} \left| K_{k+\rho} \right|_{m_{k+\rho}} + \ddot{\ddot{r}}_X \right|^{+}_{m_{k+\rho}}.$$

Следует отметить, что на передающей стороне СОНС для построения помехоустойчивого кода необходимо реализовать процесс вычисления контрольных остатков в МК. Для этого был разработан алгоритм вычисления контрольных остатков. Положим, что имеется набор оснований $m_1,...,m_k,m_{k+1}$. Если комбинация не содержит ошибки, то справедливо равенство

$$L_{k+1} = \left| \sum_{i=1}^{k} X_1 \left| K_1 \right|_{m_{k+1}} + X_{k+1} \left| K_{k+11} \right|_{m_{k+1}} + \ddot{\ddot{r}}_X \right|^{+}_{m_{k+1}} = 0. \qquad (21)$$

Выполнив преобразования, получаем алгоритм вычисления первого контрольного остатка

$$X_{k+1} = \left| m_{k+1} - \left(K_{m+1} \right)^{-1} \left| \sum_{i=1}^{k} X_i \left| K_i \right|_{m_{k+1}} + \ddot{\ddot{r}}_X \right|^{+}_{m_{k+1}} \right|^{+}_{m_{k+1}}. \qquad (22)$$

Остальные контрольные можно получить аналогично.

Алгоритмы вычисления контрольных оснований (22) и коррекции ошибок в МК (20) были использованы в разработанном помехоустойчивом протоколе опознавания с нулевым разглашением знаний, вычисления в котором выполняются в МК. Данный протокол состоит из нескольких частей.

Предварительная часть помехоустойчивого протокола:

1. Генерируется набор, состоящий из *k* оснований m_1, $m_2,...,m_k$ МК, для которого справедливо неравенство $M_k > D$, где D – большое простое число, по модулю которого выполняется протокол опознавания [3].

2. Представление секретных элементов протокола в модулярном коде: $U = (U_1, U_2,...,U_k)$ – секретный ключ спутника; $S(j) = (S_1(j),...,S_k(j))$ – сеансовый ключ; $T(j) = (T_1(j),...,T_k(j))$ – параметр, который необходим для проверки повторного использования *S*(*j*), где *j* – номер сеанса.

3. В зависимости от кратности пачек ошибок $\gamma_{ПО}$ происходит выбор контрольных оснований $m_{k+1},...,m_{k+\rho}$.

Основная часть помехоустойчивого протокола. Первый этап основной части протокола включает себя процедуры:

1. Ответчик СОНС, который располагается на спутнике, получает истинный статус НС, представленный в МК

$$C_i = \left| g^{U_1} g^{S_1(j)} g^{T_1(j)} \right|^{+}_{m_i}, \qquad (23)$$

где *g* – порождающий элемент по модулю m_i; $i = 1,2,\ldots, k$.

Используя алгоритм (22), вычисляет контрольные остатки для истинного статуса НС. Комбинация $(C_1,...,C_k,C_{k+1},...,C_{k+\rho})$ хранится в блоке памяти НС.

2. Ответчик выбирает случайные комбинации $\Delta U(j)=(\Delta U_1(j),..\Delta U_k(j))$, $\Delta S(j)=(\Delta S_1(j),..\Delta S_k(j))$, $\Delta T(j)=(\Delta T_1(j),..\Delta T_k(j))$, с помощью которых проводит «зашумление» секретных элементов помехоустойчивого протокола

$$U_i^*(j)=\left|U_i+\Delta U_i(j)\right|_{\varphi(m_i)}^{+};\ S_i^*(j)=\left|S_i(j)+\Delta S_i(j)\right|_{\varphi(m_i)}^{+};$$

$$T_i^*(j)=\left|T_i(j)+\Delta T_i(j)\right|_{\varphi(m_i)}^{+}. \quad (24)$$

3. Ответчик получает «зашумленный» статус НС в МК

$$C_i^*=\left|g^{U_i^*(j)}g^{S_i^*(j)}g^{T_i^*(j)}\right|_{m_i}^{+}. \quad (25)$$

Используя алгоритм (22), вычисляет контрольные остатки для зашумленного статуса НС. Комбинация $(C_1^*,...,C_k^*,C_{k+1}^*,...,C_{k+\rho}^*)$ хранится в блоке памяти НС.

На втором этапе протокола опознавания выполняются процедуры.

1. Запросчик СОНС, находящийся на НО, генерирует случайное число *d*. Это число представляет в виде $d=(d_1,...,d_{k+\rho})$, а затем передается ответчику.

2. Ответчик, используя алгоритм (20), сначала проверяет на наличие ошибок полученный «вопрос» $d=(d_1,d_2,...,d_{k+\rho})$. А затем готовит три ответа

$$r_i^1(j)=\left|U_i^*(j)-d_iU_i\right|_{\varphi(m_i)}^{+};\ r_i^2(j)=\left|S_i^*(j)-d_iS_i(j)\right|_{\varphi(m_i)}^{+};$$

$$r_i^3(j)=\left|T_i^*(j)-d_iT_i(j)\right|_{\varphi(m_i)}^{+}. \quad (26)$$

Используя алгоритм (22), ответчик вычисляет контрольные остатки для трех ответов. Затем формируется сигнал ответчика, который передается запросчику

$$\left\{(C_1,...,C_{k+\rho}),(C_1^*,...,C_{k+\rho}^*),(r_1^1(j),...,r_{k+\rho}^1(j)),(r_1^2(j),...,r_{k+\rho}^2(j)),(r_1^3(j),...,r_{k+\rho}^3(j))\right\}.$$

3. Запросчик с помощью алгоритма (20) осуществляет поиск и коррекцию пачек ошибок в принятом сигнале. Затем он приступает к проверке сигнала

$$Y_i=\left|(C_i)^{d_i}g^{r_i^1(j)}g^{r_i^2(j)}g^{r3_i(j)}\right|_{m_i}^{+}. \quad (27)$$

При выполнении условия

$$\{Y_1=C_1^*,Y_2=C_2^*,...,Y_k=C_k^*\}, \quad (28)$$

спутник получает статус «свой», и СОНС предоставляет ему сеанс связи.

Результаты экспериментальных исследований. Рассмотрим пример работы разработанного помехоустойчивого протокола, осуществляющего опознавание с использованием МК.

Предварительная часть помехоустойчивого протокола:

1. Пусть имеем простое число *D* = 2251. Выбираем информационные основания $m_1=7, m_2=17, m_3=19$, так как их рабочий диапазон $M_3=2261$ превышает число *D*. При этом они имеют одинаковый элемент *g* = 2.

2. Представим секретные элементы протокола в модулярном коде: секретный ключ НС $U=1000=(3,14,12)$; сеансовый ключ $S(j)=248=(3,10,1)$; параметр проверки $T(j)=452=(4,10,15)$.

3. Для более простых расчетов выберем кратность исправляемой ошибки $\gamma=1$. Тогда достаточно добавить два контрольных основания $m_4=29, m_5=37$.

Основная часть помехоустойчивого протокола. Первый этап основной части протокола включает себя процедуры:

1. Получение ответчиком СОНС истинного статуса НС согласно (23)

$$C_1 = \left| g^{U_1} g^{S_1(j)} g^{T_1(j)} \right|_{m_1}^{+} = \left| 2^3 \cdot 2^3 \cdot 2^4 \right|_7^{+} = \left| 2^4 \right|_7^{+} = 2.$$

$$C_2 = \left| g^{U_2} g^{S_2(j)} g^{T_2(j)} \right|_{m_2}^{+} = \left| 2^{14} \cdot 2^{10} \cdot 2^{10} \right|_{17}^{+} = \left| 2^2 \right|_{17}^{+} = 4.$$

$$C_3 = \left| g^{U_3} g^{S_3(j)} g^{T_3(j)} \right|_{m_3}^{+} = \left| 2^{12} \cdot 2^1 \cdot 2^{15} \right|_{19}^{+} = \left| 2^{10} \right|_{19}^{+} = 17.$$

Используя алгоритм (22), вычислим первый контрольный остаток. Для полной системы оснований вычислим ортогональные базисы

$$B_1 = 1386316 = K_1 \cdot M_3 + \ddot{B}_1 = 613 \cdot 2261 + 323 \cdot$$

$$B_2 = 1997926 = K_2 \cdot M_3 + \ddot{B}_2 = 883 \cdot 2261 + 1463 \cdot$$

$$B_3 = 1404557 = K_3 \cdot M_3 + \ddot{B}_3 = 621 \cdot 2261 + 476 \cdot$$

$$B_4 = 1505826 = K_4 \cdot M_3 = 666 \cdot 2261 \cdot$$

$$B_5 = 983535 = K_5 \cdot M_3 = 435 \cdot 2261 \cdot$$

Имеем безизбыточную комбинацию $C(j) = (2, 4, 17)$. Вычислим ранг числа

$$\ddot{r}_X = \left\lfloor \frac{\sum_{i=1}^{3} X_i \ddot{B}_i}{M_3} \right\rfloor = \left\lfloor \frac{2 \cdot 323 + 4 \cdot 1463 + 17 \cdot 476}{2261} \right\rfloor = 12 \cdot$$

Тогда первый контрольный остаток равен

$$X_4 = \left| m_4 - \frac{\left| \sum_{i=1}^{k} X_i \left| K_i \right|_{m_{k+1}} + \ddot{r}_U \right|_{m_4}}{K_4} \right|_{m_4}^{+} = \left| 29 - \frac{2 \cdot 4 + 4 \cdot 13 + 17 \cdot 12}{28} + 12 \right|_{29}^{+} = 0 \cdot$$

Аналогичным образом получили $X_5 = 16$. Тогда $C(j) = (2,4,17,0,16) \cdot$

2. Ответчик выбирает $\Delta U(j) = (5,13,5)$, $\Delta S(j) = (5,5,11)$, $\Delta T(j) = (1,13,7)$, с помощью которых проводит «зашумление» секретных элементов

$$U^*(j) = \left(\left| 3+5 \right|_6^{+}, \left| 14+13 \right|_{16}^{+}, \left| 12+5 \right|_{18}^{+} \right) = (2,11,17); \; S^*(j) = (2,15,12); \; T^*(j) = (5,7,4) \cdot$$

3. Ответчик получает «зашумленный» статус НС в МК согласно (25)

$$C_1^* = \left| g^{U_1^*(j)} g^{S_1^*(j)} g^{T_1^*(j)} \right|_{m_1}^{+} = \left| 2^2 \cdot 2^2 \cdot 2^5 \right|_7^{+} = \left| 2^3 \right|_7^{+} = 1.$$

$$C_2^* = \left| g^{U_2^*(j)} g^{S_2^*(j)} g^{T_2^*(j)} \right|_{m_2}^{+} = \left| 2^{11} \cdot 2^{15} \cdot 2^7 \right|_{17}^{+} = \left| 2^1 \right|_{17}^{+} = 2.$$

$$C_3^* = \left| g^{U_3^*(j)} g^{S_3^*(j)} g^{T_3^*(j)} \right|_{m_3}^{+} = \left| 2^{17} \cdot 2^{12} \cdot 2^4 \right|_{19}^{+} = \left| 2^{15} \right|_{19}^{+} = 12.$$

Используя алгоритм (22), получили $C^*(j) = (1,2,12,3,32) \cdot$

На втором этапе протокола опознавания выполняются процедуры.

1. Запросчик СОНС, находящийся на НО, генерирует случайное число $d = (3,16,6,14,27)$, которое затем передал ответчику

2. Ответчик сначала проверяет на наличие ошибок полученный «вопрос». Пусть при передаче помеха исказила первый остаток, и принятая ошибочная комбинация имеет вид $\widetilde{d} = (\widetilde{0},16,6,14,27)$. Воспользуемся алгоритмом (20). Вычислим ранг числа

$$\ddot{r}_d = \left[\frac{\sum_{i=1}^{3} d_i \ddot{B}_i}{M_3}\right] = \left[\frac{0\cdot 323 + 16\cdot 1463 + 6\cdot 476}{2261}\right] = 11.$$

Вычислим интервал числа *d*, представленного в модулярном коде

$$L_4 = \left|\sum_{i=1}^{3} d_i \left|K_i\right|_{m_4} + d_4\left|K_4\right|_{m_4} + \ddot{r}_d\right|_m^+ = \left|0\cdot 4 + 16\cdot 13 + 6\cdot 12 + 14\cdot 28 + 11\right|_{29}^+ = 16.$$

$$L_5 = \left|\sum_{i=1}^{3} d_i \left|K_i\right|_{m_5} + d_5\left|K_5\right|_{m_5} + \ddot{r}_d\right|_{m_5}^+ = \left|0\cdot 21 + 16\cdot 32 + 6\cdot 29 + 27\cdot 28 + 11\right|_{29}^+ = 10.$$

Так позиционная характеристика не равна нулю, то это означает, что комбинация содержит ошибку. Для значений $L_4 = 16, L_5 = 10$ вектор ошибки равен $\bar{e} = (3,0,0,0,0)$. Произведем исправление ошибки

$$d = \widetilde{d} + \bar{e} = \widetilde{d} = (\widetilde{0},16,6,14,27) + (3,0,0,0,0) = \widetilde{d} = (3,16,6,14,27).$$

Затем ответчик готовит три ответа согласно (26)

$$r_1^1(j) = \left|U_1^*(j) - d_1 U_1\right|_{\varphi(m_1)}^+ = \left|2 - 3\cdot 3\right|_6^+ = 5.\ r_1^2(j) = \left|2 - 3\cdot 3\right|_6^+ = 5.\ r_1^3(j) = \left|5 - 3\cdot 4\right|_6^+ = 5.$$

$$r_2^1(j) = \left|U_2^*(j) - d_2 U_2\right|_{\varphi(m_2)}^+ = \left|11 - 16\cdot 14\right|_{16}^+ = 11.\ r_2^2(j) = \left|15 - 16\cdot 10\right|_{16}^+ = 15.$$

$$r_2^3(j) = \left|7 - 16\cdot 10\right|_{16}^+ = 7.$$

$$r_3^1(j) = \left|U_3^*(j) - d_3 U_3\right|_{\varphi(m_3)}^+ = \left|17 - 6\cdot 12\right|_{18}^+ = 17.\ r_3^2(j) = \left|12 - 6\cdot 1\right|_{18}^+ = 6.$$

$$r_3^3(j) = \left|4 - 6\cdot 15\right|_{18}^+ = 4.$$

Используя алгоритм (22), ответчик вычисляет контрольные остатки для трех ответов. Затем формируется сигнал ответчика, который содержит: истинный статус $C(j) = (2,4,17,0,16)$, «зашумленный статус» $C^*(j) = (1,2,12,3,32)$, ответа $r^1(j) = (5,11,17,1,4)$, $r^2(j) = (5,15,6,8,28)$, $r^3(j) = (5,7,4,20,9)$. Сигнал передается запросчику.

3. Запросчик с помощью алгоритма (20) проверил принятый сигнал. Пусть в нем ошибок не было. Затем он приступает к проверке сигнала

$$Y_1 = \left|\left(C_1\right)^{d_1} g^{r_1^1(j)} g^{r_1^2(j)} g^{r_1^3(j)}\right|_{m_1}^+ = \left|2^3\cdot 2^5\cdot 2^5\cdot 2^5\right|_7^+ = \left|2^0\right|_7^+ = 1.$$

$$Y_2 = \left|\left(C_2\right)^{d_2} g^{r_2^1(j)} g^{r_2^2(j)} g^{r_2^3(j)}\right|_{m_2}^+ = \left|4^{16}\cdot 2^{11}\cdot 2^{15}\cdot 2^7\right|_{17}^+ = \left|2^1\right|_{17}^+ = 2.$$

$$Y_3 = \left|\left(C_3\right)^{d_3} g^{r_3^1(j)} g^{r_3^2(j)} g^{r_3^3(j)}\right|_{m_3}^+ = \left|17^6\cdot 2^{17}\cdot 2^6\cdot 2^4\right|_{17}^+ = \left|2^{15}\right|_{19}^+ = 12.$$

Так как условие(28) выполнилось

$$\left\{Y_1 = C_1^* = 1, Y_2 = C = 2_2^*, Y_3 = C_k^* = 12\right\}, \tag{28}$$

спутник получил статус «свой», и СОНС предоставила ему сеанс связи.

В ходе исследований был проведен анализ двух алгоритмов коррекции ошибок в МК с использованием FPGA Xilinx Artix-7 (xc7a12ticsg325-1L). Результаты моделирования показали, что при выполнении алгоритма (19) на поиск и исправление ошибок было потрачено 152 нс. Применение разработанного алгоритма (20) сократило это время до 123 нс. Поставленная цель достигнута.

Выводы. В статье представлен разработанный помехоустойчивый протокол опознавания низкоорбитальных спутников., который выполняется в МК. Применение модулярного кода позволяет не только уменьшить временные затраты на опознавание НС, но и способствует приданию СОНС свойства помехоустойчивости. Проведен анализ алгоритмов поиска и коррекции ошибок в МК. Показано, что данные алгоритмы имеют большие временные затраты. Для устранения этого недостатка был разработан алгоритм коррекции ошибок в МК, использующий изоморфизм КТО. Также этот алгоритм был использован для процедуры вычисления контрольных остатков, которая реализуется перед сигналов по каналу связи. Данные алгоритмы были использованы в разработанном помехоустойчивом протоколе опознавания низкоорбитального спутника-ретранслятора. В ходе исследований был проведен анализ двух алгоритмов коррекции ошибок в МК с использованием FPGA Xilinx Artix-7 (xc7a12ticsg325-1L). Результаты моделирования показали, что при выполнении алгоритма (19) на поиск и исправление ошибок было потрачено 152 нс. Применение разработанного алгоритма (20) сократило это время до 123 нс. Таким образом, разработанный алгоритм коррекции оказывает меньшее влияние на скорость опознавания НС. В результате этого СОНС, использующая разработанный помехоустойчивый алгоритм будет обладать более высокой имитостойкостью по сравнению с алгоритмом (19).

Исследование выполнено за счет гранта Российского научного фонда, grant number 23-21-00036, https://rscf.ru/en/project/23-21-00036/.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. *Прахова М.Ю., Хорошавина Е.А.* Системы автоматизации в нефтяной промышленности. – М. – Вологда: Инфра-Инженерия, 2019. – 304 с.
2. *Liao Y., Loures E. de F.R., Deschamps F.* Industrial internet of things: a systematic literature review and insights // IEEE Internet Things Journal. – 2018. – Vol. 5 (6). – P. 4515-4525. – DOI: 10.1109/JIOT.2018.2834151.
3. *Kalmykov I.A., Olenev A.A., Kalmykova N.I., Dukhovnyj D.V.* Using Adaptive Zero-Knowledge Authentication Protocol in VANET Automotive Network // Information. – 2023. – Vol. 14(1), 27. – DOI: 10.3390/info14010027.
4. *Chistousov N.K., Kalmykov I.A., Dukhovnyj D.V., Kalmykov M.I., Olenev A.A.* Adaptive Authentication Protocol Based on Zero-Knowledge Proof // Algorithms. – 2022. – Vol. 15 (2), 50. – DOI: 10.3390/a15020050.
5. *Olenev A.A., Kalmykov I.A., Pashintsev V.P.* Improved Spacecraft Authentication Method for Satellite Internet System Using Residue Codes // Information. – 2023. – Vol. 14 (7), 407. – DOI: 10.3390/info14070407.
6. *Kalmylov I.A., Kopytov V.V., Olenev A.A., Kalmykova N.I., Chistousov N.K.* Application of Modular Residue Classes Codes in an Authentication Protocol for Satellite Internet Systems // IEEE Access. – 2023. – Vol. 11:1-1. – P. 71624-71633. – DOI: 10.1109/ACCESS.2023.3290498.
7. *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.
8. *Tyncherov K.T., Mukhametshin V.Sh., Khuzina L.B.* Method to control and correct telemetry well information in the basis of residue number system // Journal of Fundamental and Applied Sciences. – 2017. – Vol. 9 (2). – P. 1370-1374.
9. *Mohan A*. Residue Number Systems. Theory and Applications. – Switzerland, Springer International Publishing, 2016. – 351 p.
10. *Mohan A*. RNS-Based arithmetic circuits and applications // Arithmetic Circuits for DSP Applications. Chapter 6. / Eds. P.K. Meher, T. Stouraitis. – John Wiley and Sons, Ltd, 2017. – P. 186-236.
11. *Черемушкин А.В.* Криптографические протоколы. Основные свойства и уязвимости. – М.: Академия, 2009. – 272 с.

12. *Запечников С.В.* Криптографические протоколы и их применение в финансовой и коммерческой деятельности. – М.: Горячая линия-Телеком, 2011. – 256 с.
13. *Omondi A., Premkumar B.* Residue Number Systems: Theory and Implementation. – United Kingdom, Imperial College Press, 2007. – 293 p.
14. *Червяков Н.И., Коляда А.А., Ляхов П.А.* Модулярная арифметика и ее приложения в инфокоммуникационных технологиях. – М.: Физматлит, 2017. – 400 с.
15. *Червяков Н.И., Нагорнов Н.Н.* Коррекция ошибок при передаче и обработке информации, представленной в СОК, методом синдромного декодирования // Наука. Инновации. Технологии. – 2015. – № 2. – С. 15-40.
16. *Акушский И.Я., Юдицкий Д.М.* Машинная арифметика в остаточных классах. – М.: Сов. радио, 1968. – 440 с.
17. *Сиора А.А., Краснобаев В.А., Харченко В.С.* Отказоустойчивые системы с версионно-информационной избыточностью. – Харьков: ХАИ, 2009. – 321 с.
18. *Sun J.-D., Krishna H.* A coding theory approach to error control in redundant residue number systems. II. Multiple error detection and correction // IEEE Transactions on Circuits and Systems II: Analog and Digital Signal Processing. – 1992. – Vol. 39 (1). – P. 18-34.
19. *Червяков Н.И., Сахнюк П.А., Макоха А.Н.* Нейрокомпьютеры в остаточных классах. Кн. 11. – М.: Радиотехника, 2003. – 272 с.
20. *Chervyakov N.I., Lyakhov P.A., Babenko M.G., Lavrinenko I.N., Lavrinenko A.V., Nazarov A.S.* The architecture of a fault-tolerant modular neurocomputer based on modular number projections // Neurocomputing. – 2018. – Vol. 10. – P. 96-107.
21. *Червяков Н.И., Сахнюк П.А., Шапошников А.В., Ряднов С.А.* Модулярные параллельные вычислительные структуры нейропроцессорных систем. – М.: Физматлит, 2003. – 288 с.

REFERENCES

1. *Prakhova M.Yu., Khoroshavina E.A.* Sistemy avtomatizatsii v neftyanoy promyshlennosti [Automation systems in the oil industry]. Moscow – Vologda: Infra-Inzheneriya, 2019, 304 p.
2. *Liao Y., Loures E. de F.R., Deschamps F.* Industrial internet of things: a systematic literature review and insights, *IEEE Internet Things Journal,* 2018, Vol. 5 (6), pp. 4515-4525. DOI: 10.1109/JIOT.2018.2834151.
3. *Kalmykov I.A., Olenev A.A., Kalmykova N.I., Dukhovnyj D.V.* Using Adaptive Zero-Knowledge Authentication Protocol in VANET Automotive Network, *Information,* 2023, Vol. 14(1), 27. DOI: 10.3390/info14010027.
4. *Chistousov N.K., Kalmykov I.A., Dukhovnyj D.V., Kalmykov M.I., Olenev A.A.* Adaptive Authentication Protocol Based on Zero-Knowledge Proof, *Algorithms,* 2022, Vol. 15 (2), 50. DOI: 10.3390/a15020050.
5. *Olenev A.A., Kalmykov I.A., Pashintsev V.P.* Improved Spacecraft Authentication Method for Satellite Internet System Using Residue Codes, *Information,* 2023, Vol. 14 (7), 407. DOI: 10.3390/info14070407.
6. *Kalmylov I.A., Kopytov V.V., Olenev A.A., Kalmykova N.I., Chistousov N.K.* Application of Modular Residue Classes Codes in an Authentication Protocol for Satellite Internet Systems, *IEEE Access,* 2023, Vol. 11:1-1, pp. 71624-71633. DOI: 10.1109/ACCESS.2023.3290498.
7. *Chistousov N.K., Kalmykov I.A., Chipiga A.F., Kalmykova N.I.* Razrabotka protokolov autentifikatsii nizkoorbital'nykh kosmicheskikh apparatov na osnove parallel'nykh kodov sistem ostatochnykh klassov [Development of authentication protocols for low-orbit spacecraft based on parallel codes of residual class systems], *Inzhenernyy vestnik Dona* [Engineering Bulletin of the Don], 2021, No. 4. Available at: ivdon.ru/ru/magazine/archive/n4y2021/6912.
8. *Tyncherov K.T., Mukhametshin V.Sh., Khuzina L.B.* Method to control and correct telemetry well information in the basis of residue number system, *Journal of Fundamental and Applied Sciences,* 2017, Vol. 9 (2), pp. 1370-1374.
9. *Mohan A*. Residue Number Systems. Theory and Applications. Switzerland, Springer International Publishing, 2016, 351 p.
10. *Mohan A*. RNS-Based arithmetic circuits and applications, *Arithmetic Circuits for DSP Applications. Chapter 6*, Eds. P.K. Meher, T. Stouraitis. John Wiley and Sons, Ltd, 2017, pp. 186-236.
11. *Cheremushkin A.V.* Kriptograficheskie protokoly. Osnovnye svoystva i uyazvimosti [Cryptographic protocols. Basic properties and vulnerabilities]. Moscow: Akademiya, 2009, 272 p.
12. *Zapechnikov S.V.* Kriptograficheskie protokoly i ikh primenenie v finansovoy i kommercheskoy deyatel'nosti [Cryptographic protocols and their application in financial and commercial activities]. Moscow: Goryachaya liniya-Telekom, 2011, 256 p.

13. *Omondi A., Premkumar B.* Residue Number Systems: Theory and Implementation. United Kingdom, Imperial College Press, 2007, 293 p.
14. *Chervyakov N.I., Kolyada A.A., Lyakhov P.A.* Modulyarnaya arifmetika i ee prilozheniya v infokommunikatsionnykh tekhnologiyakh [Modular arithmetic and its applications in infocommunication technologies]. Moscow: Fizmatlit, 2017, 400 p.
15. Chervyakov N.I., Nagornov N.N. Korrektsiya oshibok pri peredache i obrabotke informatsii, predstavlennoy v SOK, metodom sindromnogo dekodirovaniya [Error correction in transmission and processing of information presented in the SOC using the syndrome decoding method], *Nauka. Innovatsii. Tekhnologii* [Science. Innovations. Technologies], 2015, No. 2, pp. 15-40.
16. *Akushskiy I.Ya., Yuditskiy D.M.* Mashinnaya arifmetika v ostatochnykh klassakh [Machine arithmetic in residual classes]. Moscow: Sov. radio, 1968, 440 p.
17. *Siora A.A., Krasnobaev V.A., Kharchenko V.S.* Otkazoustoychivye sistemy s versionno-informatsionnoy izbytochnost'yu [Fault-tolerant systems with version-information redundancy]. Khar'kov: KhAI, 2009, 321 p.
18. *Sun J.-D., Krishna H.* A coding theory approach to error control in redundant residue number systems. II. Multiple error detection and correction, *IEEE Transactions on Circuits and Systems II: Analog and Digital Signal Processing,* 1992, Vol. 39 (1), pp. 18-34.
19. *Chervyakov N.I., Sakhnyuk P.A., Makokha A.N.* Neyrokomp'yutery v ostatochnykh klassakh [Neurocomputers in residual classes]. Book 11. Moscow: Radiotekhnika, 2003, 272 p.
20. *Chervyakov N.I., Lyakhov P.A., Babenko M.G., Lavrinenko I.N., Lavrinenko A.V., Nazarov A.S.* The architecture of a fault-tolerant modular neurocomputer based on modular number projections, *Neurocomputing,* 2018, Vol. 10, pp. 96-107.
21. *Chervyakov N.I., Sakhnyuk P.A., Shaposhnikov A.V., Ryadnov S.A.* Modulyarnye parallel'nye vychislitel'nye struktury neyroprotsessornykh system [Modular parallel computing structures of neuroprocessor systems]. Moscow: Fizmatlit, 2003, 288 p.

Статью рекомендовала к опубликованию д.т.н., профессор Л.К. Бабенко.

Калмыков Игорь Анатольевич – Северо-Кавказский федеральный университет; e-mail: kia762@yandex.ru; г. Ставрополь, Россия; тел.: 89034163533; кафедра вычислительной математики и кибернетики; д.т.н.; профессор.

Ефременков Иван Дмитриевич – e-mail: kia545@yandex.ru; тел.: 89283097648; кафедра вычислительной математики и кибернетики; старший преподаватель.

Духовный Даниил Вячеславович – e-mail: dduhovny26@gmail.com; тел.: 89620070023; кафедра вычислительной математики и кибернетики; аспирант.

Kalmykov Igor Anatolyevich – North Caucasus Federal University; e-mail: kia762@yandex.ru; Stavropol, Russia; phone: +79034163533; the Department of Computational Mathematics and Cybernetics; dr. of eng. sc.; professor.

Efremenkov Ivan Dmitrievich – e-mail: kia545@yandex.ru; phone: +79283097648; the Department of Computational Mathematics and Cybernetics; senior lecturer.

Dukhovnyj Daniil Vyacheslavovich – e-mail: dduhovny26@gmail.com; phone: +79620070023; the Department of Computational Mathematics and Cybernetics; postgraduate student.