Инженерный вестник Дона, №11 (2023)
ivdon.ru/ru/magazine/archive/n11y2023/8799

Разработка структурной схемы запросно-ответной системы «свой-чужой» для спутникового низкоорбитального интернета

И.А. Калмыков, Д.В. Духовный, М.И. Калмыков, Н.К. Чистоусов, Т.А. Пелешенко

Северо-Кавказский федеральный университет, Ставрополь

Аннотация: Перспективность построения спутникового интернета на основе низкоорбитальной группировки спутников (НОГС) обусловлена тем, что только она позволяет обеспечить устойчивую и достоверную связь в любой точке планеты. Поэтому технология спутникового промышленного интернета вещей IIoT получила широкое распространение в нефтегазовой индустрии, многие объекты которой располагаются в районах Крайнего Севера. Однако, при использовании спутникового низкоорбитального интернета (СНИ), возникают новые угрозы и атаки на него. Среди атак на НОГС особое место занимают попытки навязать абонентам СНИ неавторизованный контент. Предотвратить данную ситуацию можно с помощью системы опознавания спутника. Для эффективной работы запросно-ответной системы «свой-чужой», для НОГС был разработан имитостойкий протокол аутентификации с нулевым разглашением знаний. Данное свойство было достигнуто за счет сокращения времени аутентификации благодаря использованию модулярных кодов классов вычетов (МККВ). Применение параллельных кодов МККВ привело к изменению способа опознавания спутника, что влечет за собой пересмотр принципов построения запросно-ответной системы. В этом случае создание структурной схемы системы «свой-чужой», функционирующей в МККВ для спутникового низкоорбитального интернета – актуальная задача.

Ключевые слова: имитостойкость, протокол аутентификации с нулевым разглашением знаний, модулярные коды классов вычетов, структурная схема системы опознавания низкоорбитальных спутников.

Введение

В последние годы наблюдается резкое расширение областей применения спутникового интернета вещей IoT. Без данной технологии невозможно обеспечить научно-технические прорывы практически во всех областях современного общества. Наряду с потребительским сегментом интернета вещей бурно развивается сегмент промышленного IoT (IIoT) [1,2]. Увеличить область использования IIoT позволил созданный недавно спутниковый низкоорбитальный интернет (далее СНИ). Так как в спутниковом интернете используется низкоорбитальная группировка

спутников (далее НОГС), это позволяет применять технологию IIoT практически в любой точке Земли, включая районы побережья Северного Ледовитого океана [3,4]. Однако переход к СНИ приводит к резкому росту проблем, связанных с обеспечением кибербезопасности IIoT. Это вызвано тем, что канал передачи данных СНИ имеет достаточно большую протяженность, что влечет за собой увеличения числа угроз и атак, реализация которых может не только нарушить работу IIoT, но и даже вызвать экологическую катастрофу. Чтобы обеспечить эффективное решение выявленной проблемы в НОГС, было предложено использовать представленный в [5] протокол аутентификации космических аппаратов (далее КА). Для обеспечения более высокого уровня его имитостойкости предложили использовать модулярные коды классов вычетов (далее МККВ). При использовании данного протокола у спутника-нарушителя уменьшалось время на подбор правильного ответа на запрос проверяющего. В результате этого снижалась вероятность навязывания неавторизованного контента абонентам СНИ.

Однако использование новой алгебраической системы «кольцо» привело к модификации способа аутентификации, представленного в [5], что влечет за собой изменение структуры системы «свой-чужой». Поэтому целью статьи является разработка структурной схемы системы опознавания спутника, использующей протокол аутентификации с нулевым разглашением знаний, реализованный в МККВ. Применение в данной системе параллельных кодов класса вычетов позволит снизить вероятность навязывания неавторизованного контента абонентам СНИ за счет уменьшения времени для подбора правильного ответа на запрос, поступивший от проверяющего.

Материал и методы исследования

Использование протоколов с нулевым разглашением знаний в системах аутентификации обусловлено тем, что они имеют высокую криптографическую стойкость, которая достигается без применения шифрования [6]. Поэтому для аутентификации низкоорбитальных спутников был разработан метод, который позволял проводить опознавание космических аппаратов на основе протокола с нулевым разглашением знаний. Так как аутентификация осуществлялась без использования ключей, то в данный протокол были введены два секретных параметра. Это сеансовый ключ и число, которое позволяло определить повторное использование этого ключа при аутентификации. Кроме того, чтобы усложнить процедуру подбора правильного ответа на запрос проверяющего, все вычисления выполнялись по модулю большого числа Q.

Однако при этом возникала следующая проблема. Увеличение разрядности числа Q приводит к тому, что возрастают временные затраты необходимые на вычисление статуса КА. В результате этого, у спутника-злоумышленника расширяется временной интервал, в течение которого он может подбирать правильный ответ на полученный запрос. А это, в свою очередь, увеличивает вероятность пропуска спутника-злоумышленника системой «свой-чужой». Для устранения данного проблемы в работе [7] был разработан протокол аутентификации, который был реализован в МККВ. Применение параллельного кода позволило уменьшить время аутентификации, что способствовало снижению вероятности пропуска спутника-злоумышленника.

1. Реализация протокола аутентификации с нулевым разглашением знаний в МККВ

Принципы построения модулярных кодов классов вычетов определяются из самого названия кода. В МККВ используются модули, в

качестве которых могут быть выбраны или целые числа p_1, p_2, ..., p_n [8,9] или неприводимые многочлены $p_1(x)$, $p_2(x)$, ..., $p_n(x)$ [10,11]. Так как МККВ являются арифметическими кодами, то в них операции сложения, вычитания и умножения выполняются по модулям, которые являются основаниями кода. В статье будут использованы модулярные коды классов вычетов, у которых основаниями являются простые числа p_1, p_2, ..., p_n.

Рассмотрим принципы построения МККВ. Для их создания выбирают основания, для которых наибольший общий делитель (далее НОД) равен единице. После этого основания выставляются в следующем порядке:

$$p_1 < p_2 < ... < p_n, \tag{1}$$

где $\underset{i \neq j}{НОД}(p_i, p_j) = 1$.

Произведение выбранных оснований определяют рабочий диапазон кода МККВ:

$$P_n = \prod_{i=1}^{n} p_i \ . \tag{2}$$

Чтобы получить кодовую комбинацию МККВ надо выбрать целое число K, значение которого не превышает рабочий диапазон, а затем определить остатки от его деления на основания кода. В результате получаем кортеж остатков:

$$K = (K_1, K_2, ..., K_{n-1}, K_n), \tag{3}$$

где $K < P_n$; $K_i \equiv K \bmod p_i$; $i = 1, ..., n$.

Так как коды МККВ являются арифметическими, то с помощью их можно эффективно выполнять модульные операции, к которым относятся сложение, вычитание и умножение. В этом случае для двух чисел K и Z справедливо:

$$K + Z = \left|K_1 + Z_1\right|_{p_1}^{+}, \left|K_2 + Z_2\right|_{p_2}^{+}, ..., \left|K_n + Z_n\right|_{p_n}^{+}, \tag{4}$$

$$K - Z = \left|K_1 - Z_1\right|_{p_1}^{+}, \left|K_2 - Z_2\right|_{p_2}^{+}, \ldots, \left|K_n - Z_n\right|_{p_n}^{+}, \quad (5)$$

$$K \cdot Z = \left|K_1 \cdot Z_1\right|_{p_1}^{+}, \left|K_2 \cdot Z_2\right|_{p_2}^{+}, \ldots, \left|K_n \cdot Z_n\right|_{p_n}^{+}, \quad (6)$$

где $Z < P_n$; $Z_i \equiv Z \bmod p_i$; $i = 1, \ldots, n$.

Выражения (4) – (6) наглядно показывают достоинства МККВ. Во-первых, данные операции выполняются параллельно. Во-вторых, между основаниями МККВ при вычислениях отсутствуют переносы. В-третьих, операнды K_i, Z_i, где $i = 1, \ldots, n$, имеют меньшую разрядность, чем целые числа K и Z. Обобщая, можно сделать вывод о том, что коды МККВ поддерживают параллельные вычисления. При этом существует возможность заменить выполнение модульных операций на выборку результатов из LUT-таблицы благодаря малоразрядности операндов. Таким образом, используя МККВ, можно повысить скорость выполнения аддитивных и мультипликативных операций.

Кроме того МККВ позволят обеспечить криптографическую стойкость не ниже чем у одномодульных протоколов аутентификации. Для этого необходимо так подобрать основания, чтобы было справедливо:

$$Q < P_n \ . \quad (7)$$

Тогда, согласно изоморфизму Китайской теоремы об остатках вычисления, которые выполнялись по большому модулю Q, появляется возможность реализации в модулярных кодах.

Данные гипотезы были положены в основу разработанного протокола аутентификации, который представляет собой интеграцию теории аутентификации и теории построения МККВ.

На предварительном этапе протокола аутентификации с нулевым разглашением, реализованным в МККВ [7], доверенный центр (далее ДЦ) генерирует секретные параметры, который затем поступают в запросчик и ответчик системы опознавания спутника. Рассмотрим данный этап.

Предварительный этап протокола

1. Доверенный центр осуществляет выбор оснований модулярного кода классов вычетов, в качестве которых выступают простые числа. Выбор оснований определяется разрядностью сигнала ответчика. В протоколе [7] сигнал ответчика, имея длину L бит, состоит из пяти частей. Это истинный дайджест, искаженный дайджест спутника, а также три ответа на поставленный вопрос, вычисленных по модулю простого числа Q. Далее для каждого i-го основания МККВ определяется порождающий элемент u_i.

$$ДЦ: P_n = \prod_{i=1}^{n} p_i, \tag{8}$$

$$ДЦ: \log_2 P_n > \log_2 Q, \tag{9}$$

где $p_1 < p_2 < \ldots < p_n$; P_n – рабочий диапазон МККВ; $\log_2 Q = L/5$; L – разрядность сигнала ответчика.

2. Доверенный центр генерирует секретные параметры. Это G – секретный ключ спутника, случайные числа V и S, где:

$$ДЦ: \{G, V, S\} < P_n - 2. \tag{10}$$

С помощью этих чисел на борту КА будут генерироваться сеансовые ключи $V(k)$ спутника, а также $S(k)$ – числа, с помощью которых в центре принятия решения смогут установить факт повторного использования сеансового ключа. Секретные параметры $\{G, V, S\}$ записываются в память ответчика. Ответчик должен располагаться на борту КА.

Рабочий этап разработанного протокола в МККВ

Рабочую часть представленного в работе [7] протокола можно разделить на две части. Первая часть данного протокола состоит в следующем:

1. На первом этапе ответчик производит вычисление двух параметров протокола $V(k), S(k)$. Для решения данной задачи можно использовать псевдослучайную функцию [12]. Затем параметры представляются в МККВ

$$G = (G_1, G_2, ..., G_n), \quad (11)$$

$$V(k) = (V_1(k), V_2(k), ..., V_n(k)), \quad (12)$$

$$S(k) = (S_1(k), S_2(k), ..., S_n(k)), \quad (13)$$

где $G_i = G \bmod p_i$; $V_i(k) = V(k) \bmod p_i$; $S_i(k) = S(k) \bmod p_i$; $k = 1, 2, 3, ...,$ – порядковый номер сеанса аутентификации.

2. Ответчик, используя секретные параметры, осуществляет вычисление «истинного» дайджеста КА для *k*-ого сеанса аутентификации:

$$M_i(k) = (u_i^{G_i} u_i^{V_i(k)} u_i^{S_i(k))}) \bmod p_i, \quad (14)$$

где u_i – порождающий элемент мультипликативной группы p_i; $i = 1, ..., n$.

Так как вычисления в МККВ происходят параллельно по основаниям кода, то порождающие элементы могут не совпадать.

3. Ответчик, прежде чем вычислит «искаженный» статус КА, приступает к «искажению» секретных параметров. Для этого он находит три случайных числа $\Delta G(k), \Delta V(k), \Delta S(k)$, для которых справедливо:

$$\{\Delta G(k), \Delta V(k), \Delta S(k)\} < \prod_{i=1}^{n} \varphi(p_i) - 1, \quad (15)$$

где $\varphi(p_i)$ – функция Эйлера для числа p_i; $i = 1, ..., n$.

Затем он вычисляет «искаженные» секретные параметры:

$$\begin{aligned} G_i^*(k) &= G_i(k) + \Delta G_i(k) \bmod \varphi(p_i), \\ V_i^*(k) &= V_i(k) + \Delta V_i(k) \bmod \varphi(p_i), \\ S_i^*(k) &= S_i(k) + \Delta S_i(k) \bmod \varphi(p_i), \end{aligned} \quad (16)$$

где $\Delta G_i(k) \equiv \Delta G(k) \bmod p_i$; $\Delta V_i(k) \equiv \Delta V(k) \bmod p_i$; $\Delta S_i(k) \equiv \Delta S(k) \bmod p_i$; $i = 1, ..., n$.

4. Ответчик, используя «искаженные» секретные параметры, приступает к вычислению «искаженного» дайджеста КА:

$$M_i^*(k) = (u_i^{G_i^*} u_i^{V_i^*(k)} u_i^{S_i^*(k))}) \bmod p_i, \quad (17)$$

Рассмотрим вторую часть рабочего этапа протокола, на котором выполняется процедура аутентификации спутника.

5. После того, как спутник появится в зоне видимости запросчика, последний генерирует кодовую комбинацию МККВ:

$$B(k) = (B_1(k), B_2(k), \ldots, B_n(k)), \tag{18}$$

где $B_i(k) < p_i$; $i = 1, \ldots, n$.

Данная кодовая комбинация является вопросом, который задает запросчик. Вопрос передается ответчику.

8. Ответчик, получив вопрос $B(k) = (B_1(k), B_2(k), \ldots, B_n(k))$, приступает к вычислению трех ответов:

$$W_i^1(k) = (G_i^*(k) - B_i(k)G_i) \bmod \varphi(p_i), \tag{19}$$

$$W_i^2(k) = (V_i^*(k) - B_i(k)V_i(k)) \bmod \varphi(p_i), \tag{20}$$

$$W_i^3(k) = (E_i^*(k) - B_i(k)E_i(k)) \bmod \varphi(p_i), \tag{21}$$

где $i = 1, \ldots, n$.

Ответчик передает запросчику свой ответный сигнал:

$$\{(M_i(k)) \| (M_i^*(k)) \| (W_i^1(k)) \| (W_i^2(k)) \| (W_i^3(k))\}, \tag{22}$$

где $i = 1, \ldots, n$.

9. После получения сигнала ответчика запросчик приступает к его проверке:

$$\begin{aligned} X_1(k) &= (M_1(k))^{B_1(k)} u^{W_1^1(k)} u^{W_1^2(k)} u^{W_1^3(k)} \bmod p_1, \\ &\vdots \\ X_n(k) &= (M_n(k))^{B_n(k)} u^{W_n^1(k)} u^{W_n^2(k)} u^{W_n^3(k)} \bmod p_n. \end{aligned} \tag{23}$$

Результат выполнения (23) запросчик сравнивает с «искаженным» дайджестом КА. Если справедливо равенство:

$$(X_1(k), X_2(k), \ldots, X_n(k)) = (M_1^*(k), M_2^*(k), \ldots, M_n^*(k)), \tag{24}$$

то КА аутентифицируется как «свой», и ему предоставляется сеанс связи с абонентом СНИ.

Результаты исследования и их обсуждение

На основании представленного выше протокола аутентификации, выполняемого в МККВ, была создана структурная схема системы «свой-чужой», позволяющая провести аутентификацию космических аппаратов спутникового низкоорбитального интернета. На рисунке 1 показан блок ответчика, реализующий первую часть рабочего этапа протокола аутентификации. Структурная схема запросчика системы опознавания представлена на рисунке 2. На рисунке 3 показан блок ответчика, реализующий вторую часть рабочего этапа протокола аутентификации. Рассмотрим работу разработанной структурной схемы системы «свой-чужой» для спутникового низкоорбитального интернета. Пусть выбраны основания кода СОК $p_1 = 17$, $p_2 = 19$, $p_3 = 31$. В качестве порождающего элемента этих оснований выберем число:

$$u_1 = u_2 = u_3 = 3.$$

Диапазон МККВ $P_{раб} = 10013$. Перед запуском спутника в блок хранения и генерации секретных параметров (БХГ СП) будут записаны G – секретный ключ спутника, случайные числа V и S, удовлетворяющие условию (10). В данном блоке хранения и генерации секретных параметров с помощью чисел V и S будут получены сеансовые ключи $V(k)$ спутника, а также $S(k)$ – число, с помощью которого в центре принятия решения смогут установить факт повторного использования сеансового ключа.

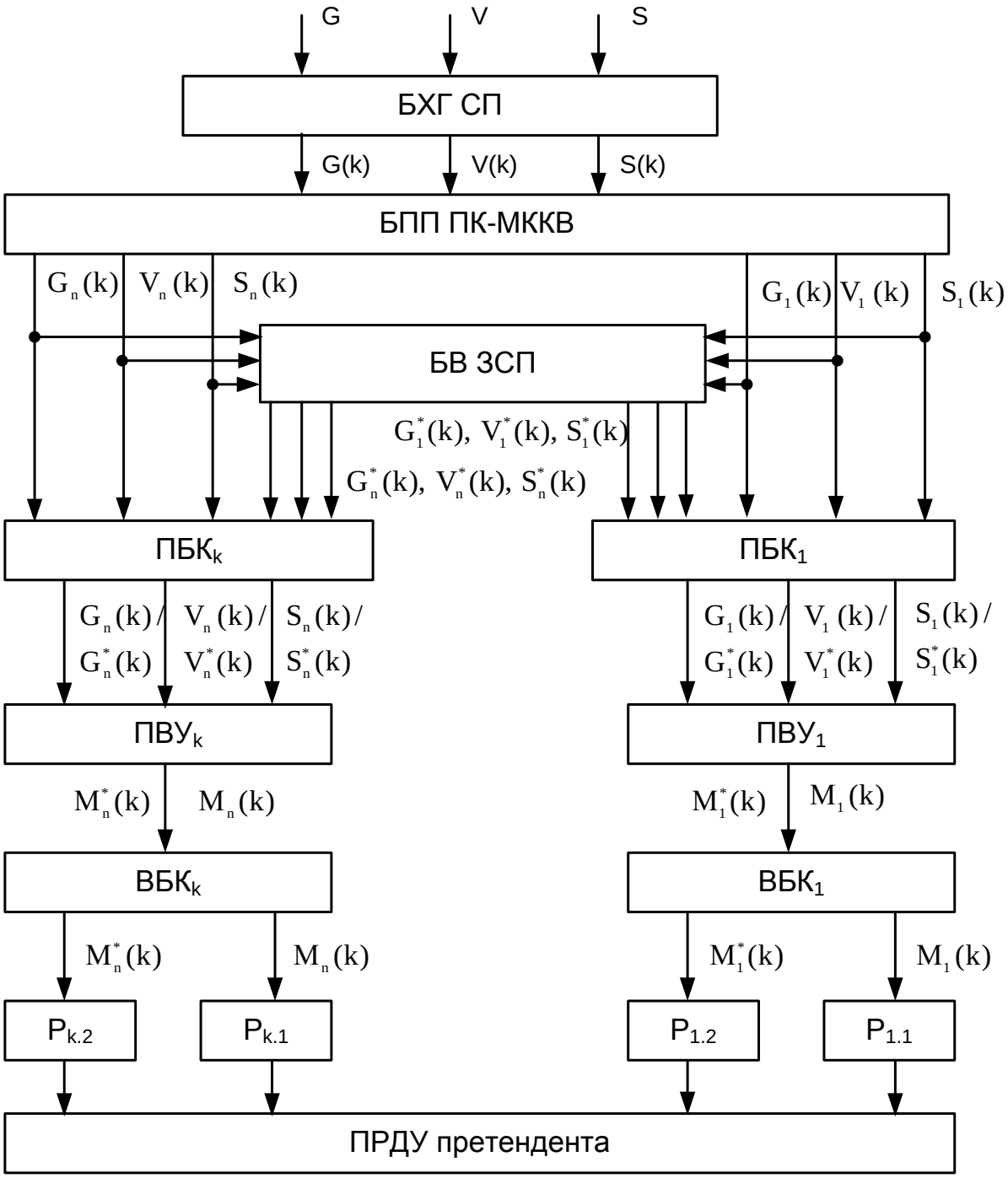

Рисунок 1. – Блок ответчика, реализующий первую часть рабочего этапа протокола аутентификации

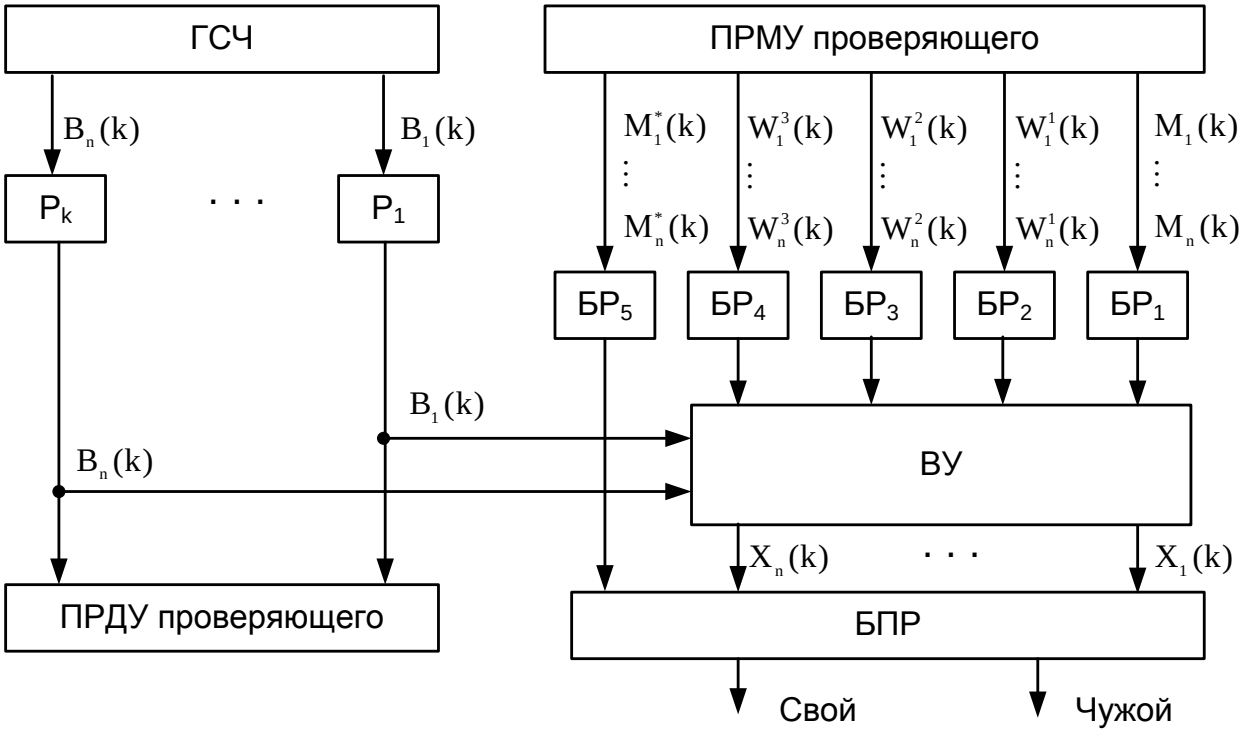

Рисунок 2. – Структурная схема запросчика системы опознавания

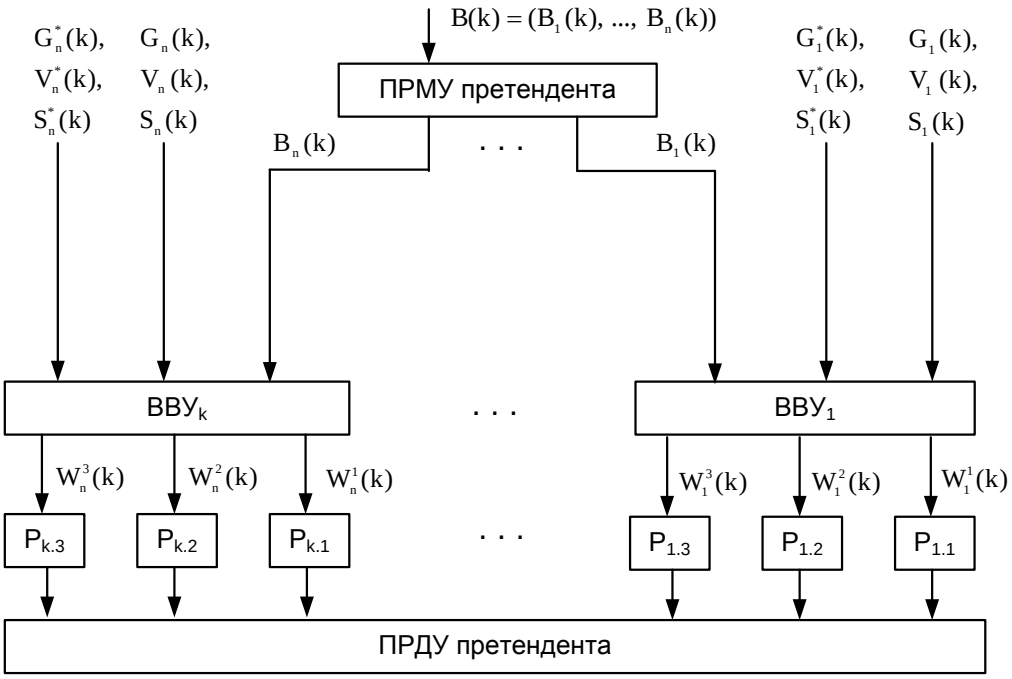

Рисунок 3. – Блок ответчика, реализующий вторую часть рабочего этапа протокола аутентификации

Пусть с входа БХГ СП снимаются секретные параметры $G(k)=2000,\ V(k)=1001,\ S(k)=561$, которые попадают на вход блока прямого преобразования (БПП), где из позиционного кода (ПК) преобразуются в МККВ. В результате получаются кодовые комбинации МККВ:

$$G(k)=(11,\ 5,\ 16),\ V(k)=(15,\ 13,\ 9),\ S(k)=(0,\ 10,\ 3).$$

Данные комбинации подаются на соответствующие первые блоки коммутации (ПБК$_1$ – ПБК$_n$). С выходов данных блоков комбинации МККВ поступают первые вычислительные устройства (ПВУ$_1$ – ПВУ$_n$). С помощью них производится вычисление истинного дайджеста спутника. Для этого используется выражения (14).

$$M_1(k)=(u_1^{G_1(k)}u_1^{V_1(k)}u_1^{S_1(k))})\bmod 17=\left|3^{11}\cdot 3^{15}\cdot 3^{0}\right|_{17}^{+}=\left|3^{10}\right|_{17}^{+}=8,$$

$$M_2(k)=(u_2^{G_2(k)}u_2^{V_2(k)}u_2^{S_2(k))})\bmod 19=\left|3^{5}\cdot 3^{13}\cdot 3^{10}\right|_{19}^{+}=\left|3^{10}\right|_{19}^{+}=16,$$

$$M_3(k)=(u_3^{G_3(k)}u_3^{V_3(k)}u_3^{S_3(k))})\bmod 31=\left|3^{16}\cdot 3^{9}\cdot 3^{3}\right|_{31}^{+}=\left|3^{28}\right|_{31}^{+}=7.$$

Полученные результаты $M_1(k)=8,\ M_2(k)=16, M_3(k)=7$ через вторые блоки коммутации (ВБК$_1$ – ВБК$_n$) поступают для хранения в регистры (Р$_{1.1}$ – Р$_{n.1}$). Для того, чтобы получить зашумленный дайджест, кодовые комбинации (25) подаются на входы блока вычисления зашумленных секретных параметров (БВЗСП). Пусть в данном блоке происходит выбор случайных чисел $\Delta G(k)=438,\ \Delta V(k)=529,\ \Delta S(k)=1494$, удовлетворяющих (15). Затем данные числа представляются в модулярном коде:

$$\Delta G(k)=\left(\left|438\right|_{16}^{+},\left|438\right|_{18}^{+},\left|438\right|_{30}^{+}\right)=(13,1,4),\ \Delta V(k)=\left(\left|529\right|_{16}^{+},\left|529\right|_{18}^{+},\left|429\right|_{30}^{+}\right)=(1,7,19),$$

$$\Delta S(k)=\left(\left|1494\right|_{16}^{+},\left|1494\right|_{18}^{+},\left|1494\right|_{30}^{+}\right)=(15,12,6).$$

А затем производится «зашумление» секретных параметров согласно (16). В результате получаются следующие кодовые комбинации МККВ:

$$G_1^{*}(k)=\left|11+13\right|_{16}^{+}=8, G_2^{*}(k)=\left|5+1\right|_{18}^{+}=6, G_3^{*}(k)=\left|16+4\right|_{30}^{+}=20.$$

$$V_1^*(k)=\left|15+1\right|_{16}^{+}=0, V_2^*(k)=\left|13+7\right|_{18}^{+}=2, V_3^*(k)=\left|9+19\right|_{30}^{+}=28.$$

$$S_1^*(k)=\left|0+15\right|_{16}^{+}=15, S_2^*(k)=\left|10+12\right|_{18}^{+}=4, S_3^*(k)=\left|3+1\right|_{30}^{+}=9.$$

Полученные комбинации МККВ через ПБК$_1$ – ПБК$_n$ подаются на входы ПВУ$_1$ – ПВУ$_n$, с помощью которых происходит вычисление зашумленного дайджеста КА, представленного в МККВ. Для этого используется равенство (17). Получаем:

$$M_1^*(k)=(u_1^{G_1^*(k)}u_1^{V_1^*(k)}u_1^{S_1^*(k))})\bmod 17=\left|3^8\cdot 3^0\cdot 3^{15}\right|_{17}^{+}=\left|3^7\right|_{17}^{+}=11.$$

$$M_2^*(k)=(u_2^{G_2^*(k)}u_2^{V_2^*(k)}u_2^{S_2^*(k))})\bmod 19=\left|3^6\cdot 3^2\cdot 3^4\right|_{19}^{+}=\left|3^{12}\right|_{19}^{+}=11.$$

$$M_3^*(k)=(u_3^{G_3^*(k)}u_3^{V_3^*(k)}u_3^{S_3^*(k))})\bmod 31=\left|3^{20}\cdot 3^{28}\cdot 3^9\right|_{31}^{+}=\left|3^{27}\right|_{31}^{+}=23.$$

Полученные результаты $M_1^*(k)=11, M_2^*(k)=11, M_3^*(k)=23$ через блоки коммутации ВБК$_1$ – ВБК$_n$ поступают для хранения в регистры (Р$_{1.2}$ – Р$_{n.2}$). При генерации сигнала претендента, кодовые комбинации МККВ $M_1(k)=8, M_2(k)=16, M_3(k)=7$ и $M_1^*(k)=11, M_2^*(k)=11, M_3^*(k)=23$ с выходов регистров будут переданы на входы передающего устройства (ПРДУ) претендента.

Рассмотрим работу запросной части системы опознавания, функционирующей в МККВ, которая представлена на рисунке 2. Для генерации запроса, представленного в коде МККВ, используется генератор случайных чисел (ГСП). Пусть было выбрано случайное число 257, которое в коде МККВ представляется $B(k)=257=(2,10,9)$. Полученная кодовая комбинация запросного числа поступает на вход передающего устройства (ПРДУ) проверяющего. Данный запрос поступает на вход приемного устройства (ПРМУ) претендента, которое показано на рисунке 3. С выхода ПРМУ кодовая комбинация поступает на третьи входы вторых вычислительных устройств ВВУ$_1$ – ВВУ$_n$. На первый и второй входы ВВУ$_1$ – ВВУ$_n$ поступают истинные и зашумленные параметры протокола. Вторые

вычислительные устройства генерируют ответы на запрос $B(k)=(2,10,9)$, используя выражения (19)-(21). Получаем

$$W_1^1(k)=\left|8-2\cdot 11\right|_{16}^{+}=2,\ W_2^1(k)=\left|6-10\cdot 5\right|_{18}^{+}=10,\ W_3^1(k)=\left|20-9\cdot 16\right|_{30}^{+}=26.$$

$$W_1^2(k)=\left|0-2\cdot 15\right|_{16}^{+}=2,\ W_2^2(k)=\left|2-10\cdot 13\right|_{18}^{+}=16,\ W_3^2(k)=\left|28-9\cdot 9\right|_{30}^{+}=7.$$

$$W_1^3(k)=\left|15-2\cdot 0\right|_{16}^{+}=15,\ W_2^3(k)=\left|4-10\cdot 10\right|_{18}^{+}=12,\ W_3^3(k)=\left|9-9\cdot 3\right|_{30}^{+}=12.$$

Затем формируется сигнал претендента согласно (22):

$$\{(8,16,7),\ (11,11,23),\ (2,10,26),\ (2,16,7),\ (15,12,12)\}.$$

Этот сигнал поступает на вход передающего устройства (ПРДУ) претендента и передается в эфир. Сигнал поступает на вход приемного устройства (ПРМУ) проверяющего (см. рисунок 2), а затем записывается в блоки регистров $БР_1$ – $БР_5$. С выходов данных блоков принятые значения поступают на вход вычислительного устройства (ВУ) проверяющего. На ВУ также подается запрос $B(k)=257=(2,10,9)$, представленный в МККВ. ВУ производит проверку принятого сигнала претендента, используя (23)

$$X_1(k)=\left(M_1(k)\right)^{B_1(k)}u^{W_1^1(k)}u^{W_1^2(k)}u^{W_1^3(k)}\bmod p_1=\left|8^2\cdot 3^2\cdot 3^2\cdot 3^{15}\right|_{17}^{+}=\left|3^7\right|_{17}^{+}=11.$$

$$X_2(k)=\left(M_2(k)\right)^{B_2(k)}u^{W_2^1(k)}u^{W_2^2(k)}u^{W_2^3(k)}\bmod p_2=\left|16^{10}\cdot 3^{10}\cdot 3^{16}\cdot 3^{12}\right|_{19}^{+}=\left|3^{12}\right|_{19}^{+}=11.$$

$$X_3(k)=\left(M_3(k)\right)^{B_3(k)}u^{W_3^1(k)}u^{W_3^2(k)}u^{W_3^3(k)}\bmod p_3=\left|7^9\cdot 3^{26}\cdot 3^7\cdot 3^{12}\right|_{31}^{+}=\left|3^{27}\right|_{31}^{+}=23.$$

Вычисленные значения подаются на блок принятия решения (БПР). Также на БПР подается зашумленный дайджест спутника. В БПР происходит сравнение вычисленных результатов с зашумленным статусом. Так как выполняется условие (24),

$$(X_1(k),X_2(k),.X_3(k))=(M_1^*(k),M_2^*(k),M_3^*(k))=(11,11,23),$$

то КА аутентифицировался как «свой», и ему предоставлен сеанс связи с абонентом СНИ

Чтоб провести оценку эффективности протокола, позволяющего провести аутентификацию с помощью МККВ [7], разработанная структурная схема системы «свой-чужой» была реализована на FPGA Kintex UltraScale (xcku025-ffva1156-1-c). Система «свой-чужой» при использовании одного модуля $Q = 20407339$ обеспечивает время выполнения протокола аутентификации спутника равное 4995 нс. Если модулярный код состоит из оснований $m_1 = 37, m_2 = 79, m_3 = 83, m_4 = 101$, то время аутентификации КА составит 1949 нс, что в 2,56 раза меньше по сравнению с [7]. Следовательно, использование разработанной структурной схемы системы «свой-чужой», функционирующей в МККВ, позволило сократить время на аутентификацию КА. Таким образом, уменьшается вероятность подбора правильного ответа на запрос проверяющего. В результате этого снижается вероятность навязывания неавторизованного контента абонентам СНИ.

Выводы

В статье представлен протокол аутентификации, обладающий минимальным временем опознавания за счет использования МККВ. На основе данного протокола с нулевым разглашением знаний была разработана структурная схема системы «свой-чужой», которая может быть использована для предотвращения навязывания неавторизованного контента абонентам СНИ. Описан состав и работа данной системы опознавания. Для оценки эффективности разработанной системы «свой-чужой» были созданы две схемотехнические модели на FPGA Kintex UltraScale (xcku025-ffva1156-1-c). Проведенные исследования показали, что использование разработанной структурной схемы системы «свой-чужой» позволяет провести аутентификацию претендента за 1949 нс, что в 2,56 раза меньше по сравнению с одномодульным протоколом, выполняемым по модулю $Q = 20407339$.

Исследование выполнено за счет гранта Российского научного фонда № 23-21-00036, rscf.ru/project/23-21-00036/.

Литература

1. What is the Internet of Things? What IoT means and how it works // Insider. – 2022 – URL: insiderintelligence.com/insights/internet-of-things-definition/ (дата обращения: 16.10.2023).

2. Khana W.Z., Rehmanb M.H. Industrial internet of things: Recent advances, enabling technologies and open challenges. Computers and Electrical Engineering, 2020, 81 106522. URL: doi.org/10.1016/j.compeleceng.2019.106522

3. Edward, J. A Techno-Economic Framework for Satellite Networks Applied to Low Earth Orbit Constellations. Assessing Starlink, OneWeb and Kuiper, IEEE Access, vol. 9, October 2021, pp 141611-141622.

4. Geng H. IoT Revolution in Oil and Gas Industry. Internet of Things and Data Analytics Handbook. New York, NY, USA: Wiley, 2017, pp. 513–520. DOI: 10.1002/9781119173601.ch31.

5. Пашинцев В.П., Ляхов А.В., Применение помехоустойчивого протокола аутентификации космического аппарата для низкоорбитальной системы спутниковой связи // Инфокоммуникационные технологии. 2015. № 2. С. 183-190.

6. Molahosseini A.S. Embedded Systems Design with Special Arithmetic and Number Systems. Springer International Publishing AG 2017 – 390 p.

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. ivdon.ru/ru/magazine/archive/n4y2021/6912. (дата обращения: 16.10.2023).

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

9. Калмыков И.А., Духовный Д.В., Калмыкова Н.И. Ортогональная обработка сигналов с использованием математических моделей целочисленных вейвлет-преобразований, реализованных в модулярных кодах классов вычетов// Инженерный вестник Дона, 2023, №3. ivdon.ru/ru/magazine/archive/n3y2023/8273 (дата обращения: 16.10.2023).

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

11. Kalmykov I.A., Pashintsev V.P., Tyncherov K T, Olenev A.A. Error-Correction Coding Using Polynomial Residue Number System. Applied Sciences. 2022. 12(7), 3365. URL: doi.org/10.3390/app12073365.

12. Naor M., Reingold O. Number-Theoretic Constructions of Efficient Pseudo-Random Functions . Journal of the ACM. – 2004. – Vol. 51, No. 2. – pp. 231-262.

References

1. What is the Internet of Things? What IoT means and how it works. Insider. 2022. URL: insiderintelligence.com/insights/internet-of-things-definition/.

2. Khana W.Z., Rehmanb M.H. Computers and Electrical Engineering, 2020, 81, 106522. URL: doi.org/10.1016/j.compeleceng.2019.106522.

3. Edward J. A Techno-Economic Framework for Satellite Networks Applied to Low Earth Orbit Constellations. Assessing Starlink, OneWeb and Kuiper, IEEE Access, vol. 9, October 2021, pp. 141611-141622.

4. Geng H. IoT Revolution in Oil and Gas Industry. Internet of Things and Data Analytics Handbook. New York, NY, USA: Wiley, 2017, pp. 513–520. DOI: 10.1002/9781119173601.ch31.

5. Pashintsev V.P., Lyakhov A.V. Infokommunikatsionnye tekhnologii. 2015. No. 2. pp. 183-190.

6. Molahosseini A.S. Embedded Systems Design with Special Arithmetic and Number Systems. Springer International Publishing AG 2017 – 390 p.

7. 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.

8. 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]. Moskva: FIZMATLIT, 2017. 400 p.

9. Kalmykov I.A., Dukhovny D.V. Kalmykova N.I. Inzhenernyj vestnik Dona, 2023, №3. URL: ivdon.ru/ru/magazine/archive/n3y2023/8273.

10. Emarlukova Ya.V., Gish T.A., Dunin 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.

11. Kalmykov I.A., Pashintsev V.P., Tyncherov K T, Olenev A.A. Applied Sciences. 2022. 12(7), 3365. URL: doi.org/10.3390/app12073365.

12. Naor M., Reingold O. Journal of the ACM. 2004. Vol. 51, No. 2. pp. 231-262.