Инженерный вестник Дона, №4 (2021)
ivdon.ru/ru/magazine/archive/n4y2021/6912

Разработка протоколов аутентификации низкоорбитальных космических аппаратов на основе параллельных кодов систем остаточных классов

И.А. Калмыков, Н.К. Чистоусов, Н.И. Калмыкова, А.Ф. Чипига

Северо-Кавказский федеральный университет, Ставрополь, Россия

Аннотация: Низкоорбитальные системы спутниковой связи (НССС) достаточно успешно применяются для организации устойчивой связи в Северных широтах. С помощью НССС обеспечивается эффективное управление и мониторинг процесса добычи и транспортировки углеводородного сырья. Такой подход позволяет обеспечить минимальные затраты на извлечение и доставку нефти и газа из месторождений, расположенных на шельфе Северного Ледовитого океана. По мере расширения числа стран, занимающихся освоением месторождений Северного Ледовитого океана, растет и число группировок НССС. Чтобы предотвратить возможность перехвата и навязывания задержанной команды управления спутником-нарушителем, необходимо повышать информационную скрытность НССС с помощью систем опознавания «свой-чужой» для космического аппарата. При этом для обеспечения высокой имитостойкости в таких системах предлагается использовать протоколы аутентификации с нулевым разглашением знаний. Чтобы повысить их эффективность, в статье предлагается использовать коды системы остаточных классов (СОК). Новизна данной идеи состоит в том, что использование параллельных кодов СОК позволит уменьшить временные затраты на выполнение арифметических операций, реализуемых в протоколах аутентификации, а это в свою очередь приведет к повышению информационной скрытности НССС, так уменьшается вероятность подбора правильного ответного сигнала спутником-нарушителем. Поэтому целью статьи является разработка протоколов аутентификации низкоорбитальных космических аппаратов на основе параллельных кодов систем остаточных классов, применение которых позволит сократить время на опознавание спутника.

Ключевые слова: система опознавания спутника, протоколы аутентификации с нулевым разглашением знаний, коды системы остаточных классов.

Введение

В настоящее время невозможно представить реализацию глобальных проектов освоения и защиты территорий нашей страны, расположенных на побережье Северного Ледовитого океана, без использования низкоорбитальных систем спутниковой связи (далее НССС) [1]. Только с помощью низкоорбитальной группировки космических аппаратов (далее КА) возможно организовать эффективное управление процессом добычи и транспортировки углеводородного сырья с использованием

необслуживаемых объектов. Однако увеличение числа стран, занимающихся освоением месторождений Северного Ледовитого океана, влечет за собой рост числа группировок НССС. Чтобы предотвратить возможность перехвата и навязывания задержанной команды управления спутником-нарушителем необходимо повышать информационную скрытность НССС. Поэтому разработка системы опознавания «свой-чужой» для КА является актуальной задачей.

Цель исследования

Известно, что повысить имитостойкость системы опознавания спутника без использования секретных ключей позволяют протоколы аутентификации с нулевым разглашением знаний [2,3]. Однако данные протоколы имеют итерационный характер выполнения. Чтобы уменьшить временные затраты на определение статуса космического аппарата, необходимо использовать параллельные вычисления. Одним из наиболее перспективных подходов, позволяющих решить данную задачу, является применение кодов системы остаточных классов (далее СОК). Новизна данной идеи состоит в том, что использование параллельных кодов СОК позволит уменьшить временные затраты на выполнение арифметических операций, реализуемых в протоколах аутентификации, а это в свою очередь приведет к повышению информационной скрытности НССС, так уменьшается вероятность подбора правильного ответного сигнала спутником-нарушителем. Поэтому целью статьи является разработка протоколов аутентификации низкоорбитальных космических аппаратов на основе параллельных кодов систем остаточных классов, применение которых позволит сократить время на опознавание спутника.

Материалы и методы

Коды системы остаточных классов относятся к арифметическим кодам,

которые используются при проведении вычислений с целыми числами [4,5]. Для этого выбирается кортеж оснований $m_1, m_2, \ldots, m_k$, в качестве которых выступают числа такие, что $НОД(m_i, m_j) = 1, i \neq j$ при $i \neq j$. Произведение таких оснований дает рабочий диапазон СОК:

$$M_k = \prod_{i=1}^{k} m_i \ . \quad (1)$$

Число А, если оно меньше рабочего диапазона, в коде СОК имеет вид:

$$A = (a_1, a_2, \ldots, a_k), \quad (2)$$

где $a_i \equiv A \bmod m_i$; $i = 1, \ldots, k$.

Так как коды СОК реализуются в кольце целых числе, то справедливы выражения:

$$A + C = ((a_1 + c_1) \bmod m_1, (a_2 + c_2) \bmod m_2, \ldots, (a_k + c_k) \bmod m_k), \quad (3)$$

$$A - C = ((a_1 - c_1) \bmod m_1, (a_2 - c_2) \bmod m_2, \ldots, (a_k - c_k) \bmod m_k), \quad (4)$$

$$A \cdot C = ((a_1 \cdot c_1) \bmod m_1, (a_2 \cdot c_2) \bmod m_2, \ldots, (a_k \cdot c_k) \bmod m_k), \quad (5)$$

где $c_i \equiv C \bmod m_i$; $i = 1, \ldots, k$.

На основе анализа равенств (3) -(5) можно сделать вывод о том, что применение кодов СОК позволяет уменьшать временные затраты на выполнение модульных операций сложения, вычитания и умножения. Это определяется малоразрядностью остатков СОК, а также параллельностью выполнения этих модульных операций по основаниям кода.

Так как базовыми операциями в большинстве протоколов аутентификации с нулевым разглашением знаний являются операции, которые можно отнести к модульным, то использование свойства изоморфизма, порожденного Китайской теоремой об остатках, позволит уменьшить время, необходимое на определение статуса претендента. Значит, разработка протоколов аутентификации с использованием параллельных кодов СОК и их сравнительный анализ позволит

обоснованно выбрать протокол, характеризующийся минимальными временными затратами на определение статуса космического аппарата.

Рассмотрим реализацию протокола аутентификации Fiat-Shamir, алгоритм которого приведен в [6], с использованием параллельных кодов СОК. В данном протоколе есть предварительный этап.

1. Претендент использует в качестве модулей кода СОК большие простые числа m_1 и m_2. В этом случае рабочий диапазон кода M_2 определяется выражением (1). Данный диапазон M_2 используется в качестве открытого ключа.

2. Претендент определяет свой секретный ключ – число S, которое меньше диапазона M_2 и взаимно простое с ним. Секретный ключ представляется в коде СОК $S = (S_1, S_2)$.

3. Претендент находит квадратичный вычет G по модулю M_2. Данное число представляется в коде СОК $G = (G_1, G_2)$. При этом должны быть справедливыми условия:

$$G_i = S_i^2 \bmod m_i . \quad (6)$$

$$G_i G_i^{-1} \equiv 1 \bmod m_i . \quad (7)$$

Рассмотрим второй этап протокола – аутентификацию претендента.

1. Претендент выбирает случайное число H, а затем преобразует его в код СОК $H = (H_1, H_2)$. Используя данные числа, выполняется:

$$Q_i \equiv H_i^2 \bmod m_i . \quad (8)$$

Полученный в СОК результат $Q = (Q_1, Q_2)$ передается запросчику.

2. Запросчик, после получения кодограммы СОК $Q = (Q_1, Q_2)$, выбирает случайное число $L \in \{0,1\}$, которое передается претенденту.

3. Претендент, получив вопрос $L \in \{0,1\}$, определяет «ответ» в СОК:

$$V_i = H_i S_i^L \bmod m_i . \quad (9)$$

Ответ в виде кода поступает запросчику.

4. Получив ответ $V=(V_1,V_2)$, запросчик приступает к его проверке. При этом используются два выражения:

$$B_i = V_i^2 \bmod m_i . \quad (10)$$

$$B_i = (V_i^2 G_i) \bmod m_i . \quad (11)$$

Выражение (10) используется, если был задан вопрос $L=0$, а выражение (11) – если был задан вопрос $L=1$. Претенденту будет присвоен статус «свой» только при выполнении сравнения:

$$B_i \equiv Q_i \bmod m_i . \quad (12)$$

В качестве недостатка протокола аутентификации Fiat-Shamir можно выделить значительные временные затраты на опознавание претендента. Это связано с тем, что для обеспечения требуемой имитостойкости протокола необходимо выполнить от 30 до 40 раундов. Поэтому данный протокол нецелесообразно применять в системах аутентификации космического аппарата. Рассмотрим протоколы, которые позволяют определить статус спутника за один раунд.

В работах [7,8] рассмотрен протокол аутентификации Guillou-Quisquater. Данный протокол базируется на доказательстве с нулевым разглашением. Проведем его модификацию с использованием параллельного кода системы остаточных классов.

Перед началом функционирования каждый из претендентов получает личный идентификатор I_P. Можно предположить, что значение данного идентификатора будет определяться номером космического аппарата. Кроме того, в состав I_P можно включить и другие сведения, например, тип космического аппарата, дату начала работы на орбите. На предварительном этапе претендент реализует процедуру вычисления открытого и секретного ключей.

1. В качестве оснований кода СОК претенденту необходимо выбрать большие простых числа m_1 и m_2. Их произведение дает диапазон кода СОК $M_k = m_1 m_2$.

2. Претендент определяет значение хеш-функции F, где в качестве аргумента используется идентификатор I_P:

$$H = F(I_P). \quad (13)$$

Вычисленное значение представляется в СОК $H = (H_1, H_2)$.

3. Претендент вычисляет значение секретного ключа $L = (L_1, L_2)$, представленного в СОК. Для этого используется сравнение:

$$H_i L_i^Y \equiv 1 mod\, m_i \ . \quad (14)$$

Наряду с секретным ключом в протоколе используется открытый ключ $(m_1 \| m_2 \| Y_1 \| Y_2 \| H_1 \| H_2)$.

Процедура аутентификации претендента состоит из этапов.

1. Претендент осуществляет выбор случайного числа P, где $P < M_k - 1$. Это число представляется в коде СОК $P = (P_1, P_2)$. Затем претендент производит вычисление:

$$K_i = P_i^Y \, mod\, m_i \, . \quad (15)$$

Вычисленное значение параметра $K = (K_1 \| K_2)$ пересылается проверяющему.

2. Проверяющий после получения $K = (K_1 \| K_2)$ производит выбор случайного числа B, где $B \le Y - 1$. Данное число выступает в качестве запроса. Оно передается претенденту.

3. Претендент после получения запроса B приступает к вычислению ответа:

$$D_i = P_i \, L_i^B \, mod\, m_i \, . \quad (16)$$

Ответы, представленные в коде СОК $(D_1 \| D_2)$, передаются проверяющему.

4. Проверяющий после получения ответов $(D_1 \| D_2)$ выполняет проверку претендента. Для этого вычисляется:

$$K_i^* = D_i^Y H_i^B \, mod \, m_i \, . \quad (17)$$

Если выполняется равенство $K_i^* = K_i$, то претенденту присваивается статус «свой». В противном случае – у претендента получается статус «чужой».

Характерной чертой рассмотренного протокола аутентификации Guillou-Quisquater являются меньшие временные затраты по сравнению с протоколом Fiat-Shamir. Следовательно, данный протокол обладает большим потенциалом для реализации в системах опознавания «свой-чужой» для низкоорбитальных систем спутниковой связи.

Проведем модификацию протокола аутентификации с нулевым разглашением знаний Schnorr [8,9]. Данный протокол также состоит из предварительного этапа и этапа аутентификации претендента.

1. Претендент производит выбор простых чисел $m_1, m_2, \ldots, m_k$, которые станут основаниями кода СОК. Затем для каждого основания вычисляется функция Эйлера $\varphi(m_1), \varphi(m_2), \ldots, \varphi(m_k)$ и определяется ее делитель P_i, где $i = 1, \ldots, k$.

2. Претендент для каждого основания кода СОК вычисляет число A_i, которое справедливо:

$$A_i^{P_i} \equiv 1 mod \, m_i \, . \quad (18)$$

3. Претендент определяет диапазон секретного ключа:

$$P = \prod_{i=1}^{k} P_i \, . \quad (19)$$

Тогда секретный ключ D должен удовлетворять условию:

$$D < P. \quad (20)$$

Затем секретный ключ представляется в виде $D = (D_1, D_2, ..., D_k)$.

3. Претендент вычисляет открытый ключ $S = (S_1, S_2, ..., S_k)$, используя выражение:

$$S_i = A_i^{-D_i} \bmod m_i. \quad (21)$$

Этап аутентификации претендента включает в себя следующие операции.

1. Претендент производит выбор чисел $(X_1, X_2, ..., X_k)$, из условия $X_i < m_i - 1$, где $i = 1, ..., k$. Это число используется для вычисления:

$$W_i = A_i^{X_i} \bmod m_i. \quad (22)$$

Полученный результат $W = (W_1, W_2, ..., W_k)$ передается проверяющему.

2. Проверяющий производит выбор «вопроса», в качестве которого выступает случайное число:

$$R = (R_1, R_2, ..., R_k) \in \{1, 2, .., 2^H\}, \quad (23)$$

где H – заданный ранее параметр.

Выбранное значение передается претенденту.

3. Претендент, получив $R = (R_1, R_2, ..., R_k)$, определяет ответ по поставленный вопрос:

$$V_i = (X_i + R_i D_i) \bmod P_i. \quad (24)$$

Ответы $V = (V_1, V_2, ..., V_k)$ передаются проверяющему.

4. Проверяющий, получив ответы $V = (V_1, V_2, ..., V_k)$ на поставленный вопрос $R = (R_1, R_2, ..., R_k)$, осуществляет их проверку:

$$C_i = A_i^{V_i} S^{R_i} \bmod m_i. \quad (25)$$

Если будет выполнено равенство:

$$(C_1, C_2, ..., C_k) = (W_1, W_2, ..., W_k), \quad (26)$$

то претенденту присвоят статус «свой». Если условие (26) не выполняется, то претендент считается «чужим».

Анализ модифицированных протоколов Schnorr и Guillou-Quisquater показал, что этап аутентификации включает в себя четыре шага, необходимые для определения статуса претендента. Сократить число таких шагов позволяет протокол аутентификации, приведенный в работах [10,11]. В данном протоколе процедура опознавания сокращена до трех шагов – вопрос проверяющего, вычисление ответа претендентом и проверка правильности ответа. Однако данный протокол для выполнения аутентификации использует большое простое число, по модулю которого и выполняются все вычисления. Произведем разработку данного протокола в коде СОК.

Предварительный этап протокола.

1. Претендент имеет секретный ключ W, начальный параметр C для вычисления n-го сеансового ключа $C(n)$, где $n = 1, 2, \ldots$, число B, с помощью которого итерационно вычисляют аргумент $B(n)$, позволяющий определить факт двойного использования сеансового ключа. Данные параметры представляются в коде СОК $(W_1(n), W_2(n), \ldots, W_k(n))$, $(C_1(n), C_2(n), \ldots, C_k(n))$, $(B_1(n), B_2(n), \ldots, B_k(n))$. При этом основания кода СОК выбираются такими, чтобы они имели одинаковый порождающий элемент $a_1 = a_2 = \ldots, = a_k$.

2. Претендент перед началом n-го сеанса обмена данными вычисляет исходный статус КА:

$$\begin{aligned} U_1(n) &= (a_1^{W_1(n)} a_1^{C_1(n)} a_1^{B_1(n)}) \bmod m_1, \\ &\vdots \\ U_k(n) &= (a_k^{W_k(n)} a_k^{C_k(n)} a_k^{B_k(n)}) \bmod m_k. \end{aligned} \qquad (27)$$

3. Претендент выбирает случайные числа $\Delta W(n), \Delta C(n), \Delta B(n)$, где $1 < \Delta W(n), \Delta C(n), \Delta B(n) < \prod_{i=1}^{k} \varphi(m_i) - 1$. Представляет их в параллельном коде СОК, а затем изменяет параметры $W, C(n), B(n)$ с помощью выражения:

$$\begin{aligned} W_i^*(n) &= (W_i + \Delta W_i(n)) \bmod \varphi(m_i), \\ C_i^*(n) &= (C_i(n) + \Delta C_i(n)) \bmod \varphi(m_i), \\ B_i^*(n) &= (B_i(n) + \Delta B_i(n)) \bmod \varphi(m_i). \end{aligned} \quad (28)$$

4. Претендент вычисляет измененный статус космического аппарата

$$\begin{aligned} U_1^*(n) &= (a_1^{W_1^*(n)} a_1^{C_1^*(n)} a_1^{B_1^*(n)}) \bmod m_1, \\ &\vdots \\ U_k^*(n) &= (a_k^{W_k^*(n)} a_k^{C_k^*(n)} a_k^{B_k^*(n)}) \bmod m_k. \end{aligned} \quad (29)$$

Этап аутентификации претендента

1. Проверяющая сторона выбирает «вопрос» в виде случайного числа, удовлетворяющего условию $H(n) < \prod_{i=1}^{k} \varphi(m_i) - 1$, и представляет его в коде СОК $H = (H_1(n), H_2(n), \ldots, H_k(n))$. Данный «вопрос» передается претенденту.

2. Претендент, получив вопрос, осуществляет вычисление ответов:

$$\begin{cases} Q_1^1(n) = (W_1^*(n) - H_1 W_1(n)) \bmod \varphi(m_1), \\ \vdots \\ Q_k^1(n) = (W_k^*(n) - H_k W_k(n)) \bmod \varphi(m_k). \end{cases} \quad (30)$$

$$\begin{cases} Q_1^2(n) = (C_1^*(n) - H_1 C_1(n)) \bmod \varphi(m_1), \\ \vdots \\ Q_k^2(n) = (C_k^*(n) - H_k C_k(n)) \bmod \varphi(m_k). \end{cases} \quad (31)$$

$$\begin{cases} Q_1^3(n) = (B_1^*(n) - H_1 B_1(n)) \bmod \varphi(m_1), \\ \vdots \\ Q_k^3(n) = (B_k^*(n) - H_k B_k(n)) \bmod \varphi(m_k). \end{cases} \quad (32)$$

Претендент пересылает проверяющему представленные в коде СОК $U(n), U^*(n), Q^1(n), Q^2(n), Q^3(n)$.

3. Проверяющий осуществляет проверку ответов:

$$\begin{aligned} R_1(n) &= (U_1^{H_1(n)} a_1^{Q_1^1(n)} a_1^{Q_1^2(n)} a_1^{Q_1^3(n)}) \bmod m_1, \\ &\vdots \\ R_k(n) &= (U_k^{H_k(n)} a_k^{Q_k^1(n)} a_k^{Q_k^2(n)} a_k^{Q_k^3(n)}) \bmod m_k. \end{aligned} \quad (33)$$

Если после проверки получается:

$$(R_1(n), R_2(n), \ldots, R_k(n)) = (U_1^*(n), U_2^*(n), \ldots, U_k^*(n)), \quad (34)$$

то проверяющий присваивает претенденту статус «свой».

Проведем сравнительный анализ рассмотренных протоколов аутентификации, реализованных в коде СОК.

Результаты исследования и их обсуждение

Рассмотрим выполнение разработанного протокола аутентификации Guillou-Quisquater, реализованного в параллельном коде СОК.

1. В качестве оснований кода СОК претендент выбрал простые числа $m_1 = 7, m_2 = 13$. Их произведение дает диапазон $M_k = 91$.

2. Пусть хеш-функция, идентификатора претендента I_P равна $H = 5$. Вычисленное значение представляем в СОК $H = (5, 5)$.

3. Претендент вычисляет значение секретного ключа, представленного в СОК. Для этого используется сравнение (14).

$$\begin{aligned} 5 \cdot L_1^{Y_1} &\equiv 1 \bmod m_1 \\ 5 \cdot L_2^{Y_2} &\equiv 1 \bmod m_2 \end{aligned}.$$

Получили, что $(L_1^{Y_1}, L_2^{Y_2}) = (3, 8)$. Получаем, что секретный ключ равен $L = (L_1, L_2) = (3, 5)$. При этом показатели степени $Y = (Y_1, Y_2) = (0, 7)$.

Тогда открытый ключ $(m_1 \| m_2 \| Y_1 \| Y_2 \| H_1 \| H_2) = (7 \| 13 \| 0 \| 7 \| 5 \| 5)$.

Процедура аутентификации претендента.

1. Претендент выбирает случайного числа P = 8, и представляет в коде СОК $P = (1, 8)$. Затем претендент производит вычисление согласно (15):

$$\begin{aligned} K_1 &= P_1^{Y_1} \bmod m_1 = 1^0 \bmod 7 = 1 \\ K_2 &= P_2^{Y_2} \bmod m_2 = 8^7 \bmod 13 = 5 \end{aligned}$$

Это значение $K=(K_1 \| K_2)=(1\|5)$ пересылается проверяющему.

2. Проверяющий производит выбор случайного числа $B=5=(5\|5)$, которое передается претенденту.

3. Претендент, получив $B=5=(5\|5)$, вычисляет ответ согласно (16) :

$$D_1 = P_1 L_1^{B_1} \bmod m_1 = (1\cdot 3^5) \bmod 7 = 5,$$
$$D_2 = P_2 L_2^{B_2} \bmod m_2 = (8\cdot 5^5) \bmod 13 = 1.$$

Ответы $(D_1 \| D_2)=(5\|1)$ передаются проверяющему.

4. Проверяющий после получения ответов выполняет проверку претендента согласно (17):

$$K_1^* = D_1^{Y_1} H_1^{B_1} \bmod m_1 = (5^0 \cdot 5^5) \bmod 7 = 1,$$
$$K_2^* = D_2^{Y_2} H_2^{B_2} \bmod m_2 = (1^7 \cdot 5^1) \bmod 13 = 5.$$

Так как выполнялось равенство $K_i^* = K_i = (1\|5)$, то претенденту присваивается статус «свой».

Рассмотрим выполнение разработанного протокола аутентификации Schnorr, реализованного в коде СОК. Предварительный этап протокола.

1. Претендент выбирает основаниями СОК $m_1=23, m_2=47, m_3=83$. Вычислены функции Эйлера $\varphi(m_1)=22, \varphi(m_2)=46, \varphi(m_3)=82$, делителями которых являются $P_1=11, P_2=23, P_3=41$.

2. Претендент для каждого основания кода СОК вычисляет число A_i, которое справедливо (18). Были получены $A_1=3, A_2=3, A_3=3$

3. Претендент определяет диапазон секретного ключа согласно (19). Получаем $P=\prod_{i=1}^{k} P_i = 10373$. Выберем секретный ключ из условия (20). Пусть он имеет вид $D=(D_1, D_2, D_3)=(7,2,35)$.

3. Претендент вычисляет открытый ключ, используя выражение (21).

$$S_1 = A_1^{-D_1} \; mod \; m_1 = 3^{-7} \; mod \; 23 = 3^{11-7} \; mod \; 23 = 3^4 \; mod \; 23 = 12.$$

$$S_2 = A_2^{-D_2} \bmod m_2 = 3^{-2} \bmod 47 = 3^{23-2} \bmod 47 = 3^{21} \bmod 47 = 21.$$

$$S_3 = A_3^{-D_3} \bmod m_3 = 3^{-35} \bmod 83 = 3^{41-35} \bmod 83 = 3^{6} \bmod 83 = 65.$$

Этап аутентификации претендента включает в себя.

1. Претендент выбирает $X = (X_1, X_2, X_3) = (7,3,11)$ и вычисляет:

$$W_1 = \left|A_1^{X_1}\right|_{m_i}^{+} = \left|3^7\right|_{23}^{+} = 2,\ W_2 = \left|A_2^{X_2}\right|_{m_2}^{+} = \left|3^3\right|_{47}^{+} = 27,\ W_3 = \left|A_3^{X_3}\right|_{m_3}^{+} = \left|3^{11}\right|_{83}^{+} = 25.$$

Полученный результат передается проверяющему.

2. Проверяющий производит выбор «вопроса» $R = (8,4,4)$, который передается претенденту.

3. Претендент определяет ответ на вопрос согласно (24):

$$V_1 = \left|X_1 + R_1 D_1\right|_{P_1}^{+} = \left|7 + 8 \cdot 7\right|_{11}^{+} = 8. V_2 = \left|3 + 4 \cdot 2\right|_{23}^{+} = 11,\ V_3 = \left|11 + 4 \cdot 35\right|_{41}^{+} = 28.$$

Ответы $V = (8,11,28)$ передаются проверяющему.

4. Проверяющий осуществляет их проверку согласно (25):

$$C_1 = \left|A_1^{V_1} S_1^{R_1}\right|_{m_1}^{+} = \left|3^8 \cdot 12^8\right|_{23}^{+} = 2,\ C_2 = \left|A_2^{V_2} S_2^{R_2}\right|_{m_2}^{+} = \left|3^{11} \cdot 21^4\right|_{47}^{+} = 27,$$

$$C_3 = \left|A_3^{V_3} S_3^{R_3}\right|_{m_3}^{+} = \left|3^{28} \cdot 65^4\right|_{83}^{+} = 25.$$

Так как $(C_1, C_2, C_3) = (W_1, W_2, W_3) = (2,27,25)$ то претендент «свой».

Рассмотрим выполнение разработанного протокола аутентификации в модулярном коде.

Предварительный этап протокола

1. Претендент выбирает основания СОК $m_1 = 19, m_2 = 29, m_3 = 39$, так как они имеют порождающий элемент $a_1 = a_2 = a_3 = 2$. Учитывая диапазон кода $M_3 = \prod_{i=1}^{3} m_i = 21489$, выбираем секретный ключ $W = 10102 = (13,10,1)$, сеансовый ключ $C(1) = 365 = (2,17,32)$ и число $B(1) = 452 = (15,17,8)$.

2. Претендент перед началом первого сеанса обмена данными вычисляет исходный статус КА согласно (27):

$$U_1(1)=(a_1^{W_1(n)}a_1^{C_1(n)}a_1^{B_1(n)})\bmod m_1=\left|2^{13}\cdot 2^{2}\cdot 2^{15}\right|_{19}^{+}=\left|2^{12}\right|_{19}^{+}=11,$$
$$U_2(1)=(a_2^{W_2(n)}a_2^{C_2(n)}a_2^{B_2(n)})\bmod m_2=\left|2^{10}\cdot 2^{17}\cdot 2^{17}\right|_{29}^{+}=\left|2^{16}\right|_{29}^{+}=25,$$
$$U_3(1)=(a_3^{W_3(n)}a_3^{C_3(n)}a_3^{B_3(n)})\bmod m_3=\left|2^{1}\cdot 2^{32}\cdot 2^{8}\right|_{37}^{+}=\left|2^{5}\right|_{37}^{+}=32.$$

3. Претендент выбирает случайные числа $\Delta W(n)=221=(5,25,5)$, $\Delta C(n)=101=(11,17,29)$, $\Delta B(n)=58=(4,2,22)$. Изменяем параметры $W, C(n), B(n)$ согласно (28):

$$W^*(n)=(\left|13+5\right|_{18}^{+},\left|10+25\right|_{28}^{+},\left|1+5\right|_{36}^{+})=(0,7,6),$$
$$C^*(n)=(\left|4+11\right|_{18}^{+},\left|17+17\right|_{28}^{+},\left|32+29\right|_{36}^{+})=(15,6,25),$$
$$B^*(n)=((\left|15+4\right|_{18}^{+},\left|17+2\right|_{28}^{+},\left|8+22\right|_{36}^{+})=(1,19,30).$$

4. Претендент вычисляет измененный статус КА согласно (29):

$$U_1^*(1)=(a_1^{W_1^*(n)}a_1^{C_1^*(n)}a_1^{B_1^*(n)})\bmod m_1=\left|2^{0}\cdot 2^{15}\cdot 2^{1}\right|_{19}^{+}=\left|2^{16}\right|_{19}^{+}=5,$$
$$U_2^*(1)=(a_2^{W_2^*(n)}a_2^{C_2^*(n)}a_2^{B_2^*(n)})\bmod m_2=\left|2^{7}\cdot 2^{6}\cdot 2^{19}\right|_{29}^{+}=\left|2^{4}\right|_{29}^{+}=16,$$
$$U_3^*(1)=(a_3^{W_3^*(n)}a_3^{C_3^+(n)}a_3^{B_3^*(n)})\bmod m_3=\left|2^{6}\cdot 2^{25}\cdot 2^{30}\right|_{37}^{+}=\left|2^{25}\right|_{37}^{+}=20.$$

Этап аутентификации претендента.

1. Проверяющий выбирает «вопрос» $H=367=(6,19,34)$, который передает претенденту.

2. Претендент, получив вопрос, вычисляет ответы согласно (30) -(32):

$$\begin{cases}Q_1^1(1)=\left|W_1^*(1)-H_1W_1(1)\right|_{\varphi(m_1)}^{+}=\left|0-6\cdot 13\right|_{18}^{+}=12,\\ Q_2^1(1)=\left|W_2^*(1)-H_2W_2(1)\right|_{\varphi(m_2)}^{+}=\left|7-19\cdot 10\right|_{28}^{+}=13,\\ Q_3^1(1)=\left|W_3^*(1)-H_3W_3(1)\right|_{\varphi(m_3)}^{+}=\left|6-34\cdot 1\right|_{36}^{+}=8.\end{cases}$$

$$\begin{cases}Q_1^2(1)=\left|C_1^*(1)-H_1C_1(1)\right|_{\varphi(m_1)}^{+}=\left|15-6\cdot 4\right|_{18}^{+}=9,\\ Q_2^2(1)=\left|C_2^*(1)-H_2C_2(1)\right|_{\varphi(m_2)}^{+}=\left|6-19\cdot 17\right|_{28}^{+}=19,\\ Q_3^1(1)=\left|C_3^*(1)-H_3C_3(1)\right|_{\varphi(m_3)}^{+}=\left|25-34\cdot 32\right|_{36}^{+}=17.\end{cases}$$

$$\begin{cases} Q_1^3(1) = \left|B_1^*(1) - H_1 B_1(1)\right|_{\varphi(m_1)}^+ = \left|1 - 6 \cdot 15\right|_{18}^+ = 1, \\ Q_2^3(1) = \left|B_2^*(1) - H_2 B_2(1)\right|_{\varphi(m_2)}^+ = \left|19 - 19 \cdot 17\right|_{28}^+ = 4, \\ Q_3^3(1) = \left|B_3^*(1) - H_3 B_3(1)\right|_{\varphi(m_3)}^+ = \left|30 - 34 \cdot 8\right|_{36}^+ = 10. \end{cases}$$

Претендент пересылает проверяющему представленные в коде СОК $U(1), U^*(1), Q^1(1), Q^2(1), Q^3(1)$.

3. Проверяющий осуществляет проверку ответов согласно (33):

$$R_1(1) = \left|U_1^{H_1(n)} a_1^{Q_1^1(n)} a_1^{Q_1^2(n)} a_1^{Q_1^3(n)}\right|_{m_1}^+ = \left|11^6 \cdot 2^{12} \cdot 2^9 \cdot 2^1\right|_{19}^+ = 5,$$

$$R_2(1) = \left|U_2^{H_2(n)} a_2^{Q_2^1(n)} a_2^{Q_2^2(n)} a_2^{Q_2^3(n)}\right|_{m_2}^+ = \left|25^{19} \cdot 2^{12} \cdot 2^{19} \cdot 2^4\right|_{29}^+ = 16,$$

$$R_3(1) = \left|U_3^{H_3(n)} a_3^{Q_3^1(n)} a_3^{Q_3^2(n)} a_3^{Q_3^3(n)}\right|_{m_3}^+ = \left|32^{34} \cdot 2^8 \cdot 2^{17} \cdot 2^{10}\right|_{37}^+ = 20.$$

Так как в результате проверки получено равенство:

$$(R_1(1), R_2(1), R_3(1)) = (U_1^*(1), U_2^*(1), U_3^*(1)) = (5, 16, 20),$$

то проверяющий присваивает претенденту статус «свой».

С целью проведения сравнительного анализа разработанных протоколов аутентификации, реализованных в кодах СОК, был создан с использованием ПЛИС FPGA Xilinx Virtex-7 аппаратный дизайн структурной модели системы аутентификации. Разрядность основания кода СОК была выбрана равной 32. При реализации аппаратного дизайна системы применялась среда разработки Vivado HLS 2019.2. Тактовая частота ПЛИС равнялась 250 МГц. Сравнительный анализ показал, что для выполнения одного раунда этапа аутентификации при использовании протокола Guillou-Quisquater требуется 3,7 ms, для протокола Schnorr – 3,1 ms, для разработанного протокола – 1,2 ms. Наибольшие временные затраты для протокола Guillou-Quisquater связаны с тем, что на этапе аутентификации в нем необходимо выполнить две операции возведения в степень по модулю. В протоколе аутентификации Schnorr на данном этапе выполняется одна операция возведения в степень по модулю, а в разработанном протоколе –

такая операция отсутствует. На основе полученных данных можно сделать вывод, что применение разработанного протокола аутентификации, реализованного в кодах СОК, позволяет повысить информационную скрытность НССС в 2,58 раза по сравнению с протоколом Schnorr и в 3,08 раза по сравнению протоколом Guillou-Quisquater.

Выводы

Для обеспечения информационной скрытности НССС и предотвращения возможности навязывания перехваченной и задержанной команды управления в работе предлагается использовать систему опознавания «свой-чужой» для спутников. Для уменьшения вероятности подбора правильного ответного сигнала спутником-нарушителем, то есть дальнейшего повышения информационной скрытности, в работе предлагается реализовать протоколы аутентификации в кодах СОК. Новизна данной идеи состоит в том, что использование параллельных кодов СОК позволит уменьшить временные затраты на выполнение арифметических операций, реализуемых в протоколах аутентификации. С целью проведения сравнительного анализа разработанных протоколов аутентификации, реализованных в кодах СОК, был разработан аппаратный дизайн структурной модели системы аутентификации с разрядностью основания равной 32 бит. Полученные результаты показали, что применение разработанного протокола аутентификации, реализованного в кодах СОК, позволяет повысить информационную скрытность НССС в 2,58 раза по сравнению с протоколом Schnorr и в 3,08 раза по сравнению протоколом Guillou-Quisquater.

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

Литература

1. Комаров Н.И. РКС провел презентацию новой системы глобальной спутниковой связи.URL: rlocman.ru/news/new.html?di=503441

2. Шнайер Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си. – М.: Издательство ТРИУМФ, 2003. – 816 с.

3. Запечников С.В. Криптографические протоколы и их применение в финансовой и коммерческой деятельности: Учебное пособие для вузов. – М.: Горячая линия-Телеком, 2011. – 256 с.

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

5. Ananda Mohan Residue Number Systems. Theory and Applications. Springer International Publishing Switzerland. pp.2016 – 351

6. Dagdelen, Ö., Fischlin, M., Gagliardoni, T.: The Fiat–Shamir transformation in a quantum world. In: Sako, K., Sarkar, P. (eds.) ASIACRYPT 2013. LNCS, vol. 8270, pp. 62–81. Springer, Heidelberg .

7. Kusnardi Kevin, Gunawan Dennis Guillou-quisquater protocol for user authentication based on zero knowledge proof // Telkomnika, Vol.17, No.2, April 2019, pp.826-834. DOI: 10.12928/ Telkomnika v17i2.1175

8. Bellare, M., & Palacio, A. (2002, August). GQ and Schnorr identification schemes: Proofs of security against impersonation under active and concurrent attacks. In Annual International Cryptology Conference (pp. 162-177). Springer, Berlin, Heidelberg.

9. Черемушкин, А.В. Криптографические протоколы. Основные свойства и уязвимости. – М. : Издательский центр «Академия», 2009. – 272 с.

10. Пашинцев В.П., Калмыков М.И., Ляхов А.В. Применение помехоустойчивого протокола аутентификации космического аппарата для

низкоорбитальной системы спутниковой связи// Инфокоммуникационные технологии. 2015. − № 2. − С. 183-190

11. Калмыков И.А., Чистоусов Н.К., Чипига А.Ф., Калмыков М.И., 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

References

1. Komarov N.I. RKS provel prezentaciyu novoj sistemy global'noj sputnikovoj svyazi [Russian space systems held a presentation of a new global satellite communication system] URL:rlocman.ru/news/new.html?di=503441

2. Shnayyer, B. Prikladnaya kriptografiya. Protokoly, algoritmy, iskhodnyye teksty na yazyke Si [Applied cryptography. Protocols, algorithms, and source texts in C], M.: Izdatelstvo TRIUMF, 2003, 816 p.

3. Zapechnikov S.V. Kriptograficheskiye protokoly i ikh primeneniye v finansovoy i kommercheskoy deyatelnosti [Cryptographic protocols and their application in financial and commercial activities], M.: Goryachaya liniya-Telekom, 2011, 256 p.

4. 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

5. Ananda Mohan Residue Number Systems. Residue Number Systems. Theory and Applications, 2016, 353 p.

6. Dagdelen, Ö, Fischlin, M., Gagliardoni, T.: The Fiat–Shamir transformation in a quantum world. In: Sako, K., Sarkar, P. (eds.) ASIACRYPT 2013. LNCS, vol. 8270, Springer, Heidelberg, pp. 62–81.

7. Kusnardi Kevin, Gunawan Dennis Telkomnika, Vol.17, No.2, April 2019, pp.826-834. DOI: 10.12928/ Telkomnika.v17i2.1175

8. Bellare, M., & Palacio, A. (2002, August). GQ and Schnorr identification schemes: Proofs of security against impersonation under active and concurrent attacks. In Annual International Cryptology Conference. Springer, Berlin, Heidelberg, pp. 162-177.

9. Cheremushkin, A.V. Kriptograficheskiye protokoly. Osnovnyye svoystva i uyazvimosti [Cryptographic protocol. Key features and vulnerabilities]. M.: Izdatelskiy tsentr «Akademiya», 2009, 272 p.

10. Pashintsev V. P., Kalmykov M. I., Lyakhov A.V. Infokommunikacionnye tekhnologii, 2015, № 2, pp. 183-190.

11. Kalmykov I.A., Chistousov N.K., Chipiga A.F., Kalmykov M.I., Pavlyuk D.N. Inzhenernyj vestnik Dona, 2020, №4. URL: ivdon.ru/ru/magazine/archive/n4y2020/6416