УДК 004.052.2

СРАВНИТЕЛЬНЫЙ АНАЛИЗ МОДИФИКАЦИЙ ПРОТОКОЛОВ АУТЕНТИФИКАЦИИ ФИАТА – ШАМИРА И ГИЛЛОУ – КУИСКУОТЕРА, РЕАЛИЗОВАННЫХ В КОДАХ СИСТЕМЫ ОСТАТОЧНЫХ КЛАССОВ

Чистоусов Н.К., Калмыков И.А., Чипига А.Ф., Калмыкова Н.И., Павлюк Д.Н.
ФГАОУ ВО «Северо-Кавказский федеральный университет», Ставрополь, e-mail: kia762@yandex.ru

В настоящее время область применения низкоорбитальных систем спутниковой связи (ССС) постоянно расширяется. Одной из наиболее перспективных сфер применения низкоорбитальных группировок спутников являются дистанционные системы контроля и управления необслуживаемыми объектами, расположенными в районах Крайнего Севера. Так как время нахождения космического аппарата в зоне видимости приемной станции ССС составляет минуты, то группировка включает в свой состав до 70 спутников. При этом наблюдается тенденция к увеличению группировок таких спутников. Поэтому обеспечение информационной скрытности ССС становится важной задачей. Для предотвращения навязывания спутником-нарушителем ранее прихваченной и задержанной команды управления предлагается применять систему «свой – чужой» для спутников, которые используют методы аутентификации на основе протоколов с нулевым разглашением знаний. Чтобы снизить вероятность подбора ответного сигнала спутника, необходимо увеличить скорость процесса аутентификации космического аппарата. Достичь данной цели можно за счет использования модифицированных протоколов, реализованных в кодах системы остаточных классов (СОК). Данные коды, выполняя параллельно операции сложения, вычитания и умножения, позволяют повысить скорость работы системы «свой-чужой». Целью работы является снижение временных затрат на определение статуса спутника за счет применения кодов системы остаточных классов.

Ключевые слова: системы «свой – чужой» для космических аппаратов, методы аутентификации на основе доказательства с нулевым разглашением знаний, код системы остаточных классов

COMPARATIVE ANALYSIS OF MODIFICATIONS OF THE FIAT – SHAMIR AND GUILLOU – QUISQUATER AUTHENTICATION PROTOCOLS IMPLEMENTED IN THE CODES OF THE RESIDUE NUMBER SYSTEM

Chistousov N.K., Kalmykov I.A., Chipiga A.F., Kalmykova N.I., Pavlyuk D.N.
North-Caucasian Federal University, Stavropol, e-mail: kia762@yandex.ru

Currently, the scope of application of low-orbit satellite communication systems (SCS) is constantly expanding. One of the most promising areas of application of low-orbit satellite groupings is remote monitoring and control systems for unattended objects located in the Far North. Since the time spent by the spacecraft in the field of view of the SCS receiving station is minutes, the grouping includes up to 70 satellites. At the same time, there is a tendency to increase the groupings of such satellites. Therefore, ensuring the information secrecy of the SCS becomes an important task. To prevent the intruder satellite from imposing a previously intercepted and delayed control command, it is proposed to use the «friend-foe» system for satellites that use authentication methods based on zero-knowledge protocols. To reduce the probability of picking up a satellite response signal, it is necessary to increase the speed of the spacecraft authentication process. This goal can be achieved by using modified protocols implemented in the codes of the Residual number system (RNS). These codes, performing parallel operations of addition, subtraction and multiplication, allow you to increase the speed of the system «friend-foe». The aim of the work is to reduce the time spent on determining the satellite status by using the codes of the residual number system.

Keywords: «Friend-or-foe» systems for spacecraft, proof-based authentication methods with zero knowledge disclosure, residue number system

В последние годы наблюдается повышенный интерес к применению низкоорбитальных систем спутниковой связи (ССС). Такие системы нашли применение при освоении Северного морского пути, развертывании Вооруженных Сил в Арктике, а также в дистанционных системах контроля и управления необслуживаемыми объектами добычи углеводородного сырья в районах Крайнего Севера. Так как наблюдается тенденция к увеличению группировок как отечественных, так и зарубежных спутников, то для предотвращения навязывания спутником-нарушителем ранее прихваченной и задержанной команды управления в работах [1, 2] предлагается применять систему «свой – чужой» для спутников. Снижение времени, необходимого на аутентификацию спутника, позволит повысить информационную скрытность низкоорбитальных ССС. Решить проблему можно за счет использования в системах «свой – чужой» методов аутентификации, реализующих параллельные вычисления с использованием кодов системы остаточных классов (СОК).

Для обеспечения высокой имитостойкости к подбору сигнала ответчика без использования криптографических шифров применяются методы аутентификации на основе протоколов с нулевым разглашением знаний. При этом наибольший интерес представляют протоколы, имеющие один раунд аутентификации. Повысить информационную скрытность ССС возможно за счет

повышения скорости процесса аутентификации космического аппарата. Достичь данной цели можно за счет использования модифицированных протоколов, реализованных в модулярных кодах (МК). Данные коды, выполняя параллельно операции сложения, вычитания и умножения, позволяют повысить скорость работы системы «свой – чужой». Целью работы является снижение временных затрат на определение статуса спутника за счет применения кодов системы остаточных классов.

Материалы и методы исследования

Коды системы остаточных классов являются арифметическими непозиционными кодами [3, 4]. Для вычислений целое число X однозначно задается кортежем остатков

$$X = (x_1, x_2, ..., x_k), \quad (1)$$

где $x_i \equiv X \bmod m_i$, m_i – основания кода СОК; НОД $(m_i, m_j) = 1$; $i = 1,...,k$.

Так как основаниями СОК выступали попарно простые числа m_i, где $i = 1,...,k$, то их произведение задает размер рабочего диапазона

$$M_k = \prod_{i=1}^{k} m_i > X. \quad (2)$$

Так как коды выполняют параллельно операции сложения, вычитания и умножения

$$X \pm C = ((x_1 \pm c_1) \bmod m_1, (x_2 \pm c_2) \bmod m_2, ..., (x_k \pm c_k) \bmod m_k), \quad (3)$$

$$X \cdot C = ((x_1 \cdot c_1) \bmod m_1, (x_2 \cdot c_2) \bmod m_2, ..., (x_k \cdot c_k) \bmod m_k), \quad (4)$$

то их целесообразно использовать для повышения скорости выполняемых вычислений.

Анализ выражений (3) и (4) показал, что коды СОК можно использовать в протоколах аутентификации, в которых используются аддитивные и мультипликативные операции по модулю. Особое место среди последних занимают протоколы, основанные на доказательстве с нулевым разглашением знаний. В работе [5] представлен протокол аутентификации Фиата – Шамира. Рассмотрим модификацию данного протокола в МК.

1. Определяем два больших простых числа m_1 и m_2 в качестве оснований МК. Тогда согласно (2) их произведение дает диапазон M_2, который является частью открытого ключа.

2. Ответчик выбирает случайное число Q, которое является секретным ключом, из условия НОД $(M_2, Q) = 1$, $Q \in \{1, 2, .., M_2 - 1\}$. Число переводится в МК $Q = (Q_1, Q_2)$.

3. Ответчик вычисляет квадратичный вычет L по модулю M_2 в модулярном коде. Это вторая часть открытого ключа

$$L_i = Q_i^2 \bmod m_i. \quad (5)$$

При этом должно выполняться условие

$$L_i \cdot L_i^{-1} \equiv 1 \bmod m_i. \quad (6)$$

Процесс аутентификации включает в себя следующие этапы.

4. Ответчик выбирает случайное число R и представляет его в модулярном коде. Затем проводится вычисление числа W и его передача запросчику

$$W_i \equiv R_i^2 \bmod m_i. \quad (7)$$

5. Запросчик, получив $W = (W_1, W_2)$, выбирает случайное число $C \in \{0, 1\}$ и передает ответчику.

6. Ответчик вычисляет ответ на поставленный вопрос C:

$$У_i = R_i \cdot Q_i^C \bmod m_i. \quad (8)$$

Ответ передается запросчику.

7. Запросчик проверяет истинность ответа при условии:

– если вопрос $C = 0$, то получаем выражение

$$G_i = Y_i^2 \bmod m_i, \quad (9)$$

– если вопрос $C = 1$, то получаем выражение

$$G_i = (Y_i^2 L_i) \bmod m_i. \quad (10)$$

Проверяемый объект получит статус «свой» если будет справедливым условие

$$G_i \equiv W_i \bmod m_i. \quad (11)$$

При невыполнении условия (11) проверяемый объект получает статус «чужой».

В работах [6, 7] представлен протокол аутентификации Гиллоу – Куискуотера, который также относится к протоколам с нулевым разглашением знаний. Проведем его модификацию в модулярном коде СОК.

Для выполнения данного протокола претендент P должен обладать определенной идентификационной информацией I_P. В состав этих данных может входить тип спутника, его личный идентификатор, срок выхода на орбиту, и т.д. На этапе получения открытого и секретного выполняется алгоритм, который состоит из следующих шагов.

1. Выбираются два больших простых числа m_1 и m_2, которые являются основаниями МК. Затем находится их произведение $M_k = m_1 m_2$.

2. Ответчик вычисляет хеш-функцию строки идентификации I_P, используя выражение

$$J = f(I_P), \quad (12)$$

где f – функция, реализующая процедуры свертки.

3. Ответчик выбирает секретный ключ $B = (B_1, B_2)$ из условия

$$J_i \cdot B_i^X \equiv 1 \bmod m_i, \quad (13)$$

где $i = 1, 2$.

Открытым ключом данного протокола являются (M, X, J). Секретным ключом – B.

На этапе проведения аутентификации выполняются следующие этапы.

4. Ответчик выбирает случайное число C, из условия $C \le M_k - 1$, и преобразует его в модулярный код. После этого он вычисляет число в МК

$$T_i = C_i^X \bmod m_i, \quad (14)$$

где $i = 1, 2$.

Данное число $T = (T_1, T_2)$ передается на проверяющую сторону запросчику.

5. Запросчик, получив число D, выбирает случайное число из условия $1 \le D \le X - 1$. Выбранное число пересылается ответчику на борт спутника.

6. Ответчик, получив вопрос D, отвечает на поставленный вопрос

$$Y_i = C_i \cdot B_i^D \bmod m_i. \quad (15)$$

Вычисленный ответ $Y = (Y_1, Y_2)$ пересылается запросчику.

7. Запросчик, получив число $Y = (Y_1, Y_2)$, проверяет правильность ответа

$$T_i^* = Y_i^X J_i^D \bmod m_i. \quad (16)$$

Если вычисленное значение совпадет с числом T, то запросчик принимает решение, что спутник имеет статус «свой». В противном случае – спутник получает статус «чужой».

Результаты исследования и их обсуждение

Рассмотрим выполнение протокола аутентификации Фиата – Шамира. Рассмотрим модификацию данного протокола в МК.

1. Пусть выбраны основания кода $m_1 = 5$ и $m_2 = 7$. Тогда согласно (2) их произведение дает диапазон $M_2 = 35$, который является частью открытого ключа.

2. Ответчик вычисляет квадратичные вычеты L по модулю $M_2 = 35$, которые удовлетворяют условию (5). Тогда получаем числа $L = \{1, 4, 9, 11, 14, 15, 16, 21, 29, 30\}$. Из них условию (6) удовлетворяют $L = \{1, 4, 9, 11, 14, 16, 29\}$.

Например, если выбрать число $L = 16 = (1, 2)$, то мультипликативная инверсия по модулю 35 будет равна $L^{-1} = 11 = (1, 4)$, так как имеем $16 \cdot 11 \bmod 35 = 176 \bmod 35 = 1$.

3. Ответчик выбирает случайное число Q, которое является секретным ключом, из условия НОД $(M_2, Q) = 1$, $Q \in \{1, 2, .., M_2 - 1\}$. При этом число Q должно удовлетворять выражению (5). Пусть ответчик выбрал число $Q = 9 = (4, 2)$. Возведем его в квадрат

$$Q^2 \bmod M_2 = 9^2 \bmod 35 = 11.$$

В модулярном коде получаем

$$L = Q^2 \bmod M_2 = (4^2 \bmod 5, 2^2 \bmod 7) = (1, 4) = 11.$$

Тогда открытым ключом является кортеж $(M_2, L) = (35, (1, 4))$.

Процесс аутентификации включает в себя следующие этапы.

4. Ответчик выбирает случайное число R. Пусть $R = 8 = (3, 1)$. Затем проводится вычисление числа W на основе (6) и его передача запросчику

$$W_1 \equiv R_1^2 \bmod m_1 = 3^2 \bmod 5 = 4.$$

$$W_2 \equiv R_2^2 \bmod m_2 = 3^2 \bmod 7 = 1.$$

Вычисленное число в модулярном коде $W = (4, 1)$ передается запросчику.

Рассмотрим оба случая проверки статуса объекта, то есть при $C = 0$ и $C = 1$.

5.1. Запросчик, получив $W = (4, 1)$, выбирает число $C = 0$ и передает ответчику.

6.1. Ответчик вычисляет ответ на вопрос $C = 0$, используя выражение (8):

$$Y_1 = R_1 \cdot Q_1^C \bmod m_1 = 3 \cdot 4^0 \bmod 5 = 3.$$

$$Y_2 = R_2 \cdot Q_2^C \bmod m_2 = 1 \cdot 2^0 \bmod 7 = 1.$$

Ответ $Y = (Y_1, Y_2) = (3, 1)$ передается запросчику.

7.1. Так как запросчик передал $C = 0$, то для проверки используется (9). Тогда

$$G_1 = Y_1^2 \bmod m_1 = 3^2 \bmod 5 = 4,$$

$$G_2 = Y_2^2 \bmod m_2 = 1^2 \bmod 7 = 1.$$

Так как выполняется равенство (11), то объект имеет статус «свой».

5.2. Запросчик, получив $W = (4, 1)$, выбирает число $C = 1$ и передает ответчику.

6.2. Ответчик вычисляет ответ на вопрос $C = 1$, используя выражение (8)

$$Y_1 = R_1 \cdot Q_1^C \bmod m_1 = 3 \cdot 4^1 \bmod 5 = 2.$$

$$Y_2 = R_2 \cdot Q_2^C \bmod m_2 = 1 \cdot 2^1 \bmod 7 = 2.$$

Ответ $Y = (Y_1, Y_2) = (2, 2)$ передается запросчику.

7.1. Так как запросчик передал $C = 1$, то для проверки используется (10). Тогда

$$G_1 = (Y_1^2 L_1) \bmod m_1 = (2^2 \cdot 1) \bmod 5 = 4,$$

$$G_2 = (Y_2^2 L_2) \bmod m_1 = (2^2 \cdot 2) \bmod 7 = 1.$$

Так как выполняется равенство (11), то объект имеет статус «свой»

Рассмотрим модификацию протокола аутентификации Гиллоу – Куискуотера.

1. Пусть ответчиком выбираются два простых числа $m_1 = 5$ и $m_2 = 11$. Тогда диапазон модулярного кода $M_k = m_1 \cdot m_2 = 55$.

2. Положим, что идентификатор ответчика равен $I_P = 14367$. Затем он вычисляет хеш-функцию согласно (12) в модулярном коде

$$J_1 = h(I_P) = I_P \bmod m_1 = 2,$$

$$J_2 = h(I_P) = I_P \bmod m_2 = 1.$$

3. Ответчик выбирает секретный ключ B из условия (13), используя МК

$$J_1 \cdot B_1^X \equiv 1 \bmod m_1 = 2 \cdot B_1^X \equiv 1 \bmod m_1,$$

$$J_2 \cdot B_2^X \equiv 1 \bmod m_2 = 1 \cdot B_2^X \equiv 1 \bmod m_2.$$

Преобразуем данные равенства и получаем, что

$$B_1^X \equiv 3 \bmod 5,$$

$$B_2^X \equiv 1 \bmod 11.$$

Тогда в качестве секретного ключа B можно взять число $B = 3$ (3, 3), а показатель степени $X = 5$.

Открытым ключом данного протокола являются $(M, X, J) = ((5, 11), 5, (1, 2))$.

Рассмотрим аутентификацию ответчика. Для этого необходимо выполнить

4. Ответчик выбирает случайное число $C = 17 = (2, 6)$ из условия $1 \le C \le M_k - 1$, а затем вычисляет число

$$T_1 = C_1^X \bmod m_1 = 2^5 \bmod 5 = 2,$$

$$T_2 = C_2^X \bmod m_2 = 6^5 \bmod 11 = 10.$$

Данное число $T = (2, 10)$ передается запросчику.

5. Запросчик, получив число $T = (2, 10)$, выбирает случайное число $D = 4$, из условия $1 \le D \le X - 1$. Число $D = 4$ пересылается ответчику.

3. Ответчик, получив вопрос $D = 4$, отвечает на поставленный вопрос

$$Y_1 = C_1 \cdot B_1^D \bmod m_1 = \left|2 \cdot 3^4\right|_5^+ = 2,$$

$$Y_2 = C_2 \cdot B_2^D \bmod m_2 = \left|6 \cdot 3^4\right|_{11}^+ = 2.$$

Вычисленный в модулярном коде ответ пересылается запросчику.

4. Запросчик, получив число $Y = (2, 2)$, проверяет правильность ответа

$$T_1^* = Y_1^X J_1^D \bmod m_1 = \left|2^5 \cdot 2^4\right|_5^+ = 2,$$

$$T_2^* = Y_2^X J_2^D \bmod m_2 = \left|2^5 \cdot 1^4\right|_{11}^+ = 10.$$

Так как вычисленное значение совпадет с числом T, то есть $T^* = T = (2, 10)$, то запросчик принимает решение, что проверяемый спутник «свой».

Рассмотренные модификации протоколов аутентификации, построенные на основе доказательства с нулевым разглашением знаний, можно отнести к многошаговым. При этом для обеспечения высокого уровня криптостойкости протокола аутентификации Фиата – Шамира требуется выполнения от 20 до 40 раундов. Это связано с тем, что вероятность подбора правильного ответа на одном раунде составляет 0,5. Поэтому для снижения такой вероятности необходимо многократное повторение раундов аутентификации.

Для оценки реализации данных модификаций протоколов в модулярных кодах был разработан аппаратный дизайн структурной модели системы опознавания, реализованной на основе 32-разрядного модуля. Построение выполнено на основе ПЛИС FPGA Xilinx Virtex-7 с использованием инструментария Vivado HLS 2019.2. Максимальная тактовая частота устройства составила 250 МГц. Для выполнения мультипликативных и аддитивных операций использовались LUT-таблицы. Сравнительный анализ одного раунда аутентификации, реализованный в модулярных кодах, показал, что для реализации протокола Фиата – Шамира требуется 2,42 ms. При этом временные затраты на один раунд выполнения протокола Гиллоу – Куискуотера составят 3,7 ms. В результате получаем, что реализация одного раунда протокола Фиата – Шамира требует в 1,53 раза меньше временных затрат по сравнению с протоколом Гиллоу – Куискуотера. Однако для достижения требуемой криптографической стойкости к подбору сигнала ответчика для выполнения протокола аутентификации Фиата – Шамира требуется несколько раундов реализации. В этом случае при выполнении

20 раундов опознавания спутника временные затраты составят 48,4 ms. Поэтому модификацию протокола аутентификации Гиллоу – Куискуотера, реализованного в МК, можно считать более эффективной по сравнению с многораундовым проколом Фиата – Шамира.

Заключение

Для повышения эффективности систем аутентификации низкоорбитальных спутников необходимо уменьшать время на процедуру вычисления статуса спутника, так как это позволяет снизить вероятность подбора сигнала ответчика. Для достижения поставленной цели в статье рассмотрены модификации протоколов аутентификации Фиата – Шамира и Гиллоу – Куискуотера, реализованные в МК. Проведенный сравнительный анализ показал, что, несмотря на то, что временные затраты на выполнение одного раунда аутентификации протоколом Фиата – Шамира в 1,53 раза меньше временных затрат по сравнению с протоколом Гиллоу – Куискуотера, на полную аутентификацию спутника потребуется 48,4 ms. На основе полученных результатов исследования можно сделать вывод о том, что модификация протокола аутентификации Гиллоу – Куискуотера, реализованная в МК, можно быть использована для построения систем опознавания спутника.

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

Список литературы

1. 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.

2. Rezenkov R.N., Pashintsev V.P., Zhuk P.A. Application of spoof resistant authentication protocol of spacecraft in low earth orbit systems of satellite communication. International Journal of Mechanical Engineering and Technology (IJMET). 2018. Vol. 9. Issue 5. May, P. 958–965.

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

4. Ananda Mohan Residue Number Systems. Theory and Applications. Springer International Publishing Switzerland. 2016. 351 p.

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

6. Запечников С.В. Криптографические протоколы и их применение в финансовой и коммерческой деятельности: учебное пособие для вузов. М.: Горячая линия – Телеком, 2007. 320 с.

7. Kevin Kusnardi, Dennis Gunawan Guillou-quisquater protocol for user authentication based on zero knowledge proof. TELKOMNIKA. April 2019. Vol. 17. No. 2. P. 826–834. DOI: 10.12928/TELKOMNIKA.v17i2.11754.