УДК 004.052.2:629.78

РЕАЛИЗАЦИЯ МАТЕМАТИЧЕСКОЙ И СТРУКТУРНОЙ МОДЕЛЕЙ КОДОПРЕОБРАЗОВАНИЯ ДЛЯ СИСТЕМЫ АУТЕНТИФИКАЦИИ КОСМИЧЕСКОГО АППАРАТА

[1]Степанова Е.П., [1]Калмыков М.И., [1]Ефременков И.Д., [1]Ефимович А.В., [1]Калмыков И.А., [2]Тынчеров К.Т.

[1]ФГАОУ ВО «Северо-Кавказский федеральный университет», Ставрополь, e-mail: kia762@yandex.ru;
[2]Филиал ФГАОУ ВО «Уфимский государственный нефтяной технический университет», Октябрьский

Для эффективного контроля, мониторинга и управления объектами, расположенными на шельфе Северого Ледовитого океана, широко используют автоматизированные системы дистанционного контроля и управления. Так как необслуживаемые объекты располагаются за полярным кругом, организация информационного обмена данными с центром управления возлагается на низкоорбитальные системы спутниковой связи (НССС). По мере увеличения числа стран и компаний, осваивающих недра арктического побережья, будет расширяться количество НССС. При этом может возникнуть ситуация, когда спутник-нарушитель попытается навязать ложную команду управления необслуживаемому объекту добычи и транспортировки, что может привести к экологической катастрофе. Для предотвращения данной ситуации и повышения информационной скрытности НССС предлагается использовать систему аутентификации космического аппарата, которая функционирует в модулярных кодах. Использование данных кодов позволяет повысить скорость аутентификации спутника. Это связано с тем, что в данных кодах операции сложения, вычитания и умножения выполняются над малоразрядными остатками параллельно по основаниям кода. Однако после вычислений, определяемых протоколом аутентификации, необходимо выполнить преобразование из модулярного кода в позиционный код. Очевидно, что сокращение времени выполнения такого обратного преобразования позволит повысить скорость аутентификации космического аппарата. Поэтому целью исследований является разработка математической и структурной моделей кодопреобразования моделей для систем аутентификации космического аппарата, обладающих минимальными временными затратами.

Ключевые слова: система аутентификации космического аппарата, модулярные коды, математическая и структурная модели преобразования из модулярного кода в позиционный код

IMPLEMENTATION OF MATHEMATICAL AND STRUCTURAL MODELS OF KETOPROPANE TO THE AUTHENTICATION SYSTEM OF THE SPACECRAFT

[1]Stepanova E.P., [1]Kalmykov M.I., [1]Efremenkov I.D., [1]Efimovich A.V., [1]Kalmykov I.A., [2]Tyncherov K.T.

[1]Federal State Autonomous Educational Institution Higher Professional Education «North-Caucasian Federal University, Stavropol, e-mail: kia762@yandex.ru;
[2]Branch of Federal State Autonomous Educational Institution of Higher Education «Ufa State Petroleum Technological University», Oktyabrskiy

For effective control, monitoring and management of hydrocarbon production and transportation facilities located on the shelf of the Arctic ocean, automated remote control and management systems are widely used. Since maintenance-free objects are located above the Arctic Circle, the organization of information exchange with the control center is assigned to the low-orbit satellite communication system (NSSs). As the number of countries and companies developing the bowels of the Arctic coast increases, the number of NASS will increase. In this case, a situation may arise when the intruder satellite tries to impose a false command to control an unattended object of production and transportation, which can lead to an environmental disaster. To prevent this situation and increase the information secrecy of the NSSs, it is proposed to use the spacecraft authentication system, which operates in modular codes. The use of these codes allows to increase the speed of satellite authentication. This is due to the fact that in these codes the operations of addition, subtraction and multiplication are performed on low-digit residues in parallel on the bases of the code. However, after the calculations defined by the authentication Protocol, you must convert from modular code to positional code. It is obvious that the reduction of the time for performing such a reverse conversion will increase the speed of authentication of the spacecraft. Therefore, the aim of the research is to develop mathematical and structural code transformation models for spacecraft authentication systems with minimal time costs.

Keywords: the authentication system of the spacecraft, modular codes, mathematical and structural models of the transformation of modular code in the position code

Современные низкоорбитальные системы спутниковой связи (НССС) достаточно успешно применяются для организации связи с объектами, расположенными за полярным кругом. Поэтому они используются в автоматизированных системах дистанционного контроля и управления. При этом количество таких группировок будет постоянно возрастать. В результате в зоне видимости приемника, расположенного на объекте управления добычи и транспортировки углеводородов, может появиться

спутник-нарушитель, который попытается навязать ложную команду управления. Чтобы предотвратить такое навязывание и повысить информационную скрытность НССС в работе [1], предлагается использовать систему аутентификации космического аппарата (КА). Повысить скорость определения статуса КА возможно за счет использования протокола аутентификации, реализованного в модулярных кодах (МК), так как в данных кодах обеспечивается максимальная скорость выполнения модульных операций [2]. Однако после проведенных в МК вычислений необходимо выполнить преобразование к коду позиционной системы счисления (ПСС). Поэтому разработка математической и структурной моделей кодопреобразования МК-ПСС для системы аутентификации космического аппарата, характеризующихся минимальными временными затратами, является актуальной задачей.

Чтобы обеспечить высокую информационную скрытность НССС, в [1] показана система опознавания с криптостойким протоколом аутентификации. Так как данный протокол построен на доказательстве с нулевым разглашением знаний, то в нем применяются большие простые числа, что характеризуется значительными временными и схемными затратами. Реализация такого протокола в МК позволит снизить временные затраты на аутентификацию КА, так, модульные операции выполняются над малоразрядными остатками и параллельно. Однако после выполнения соответствующих вычислений необходимо результат представить в ПСС. Для этого выполняется обратное преобразование. Так как скорость выполнения данной процедуры будет зависеть от алгоритма и его схемной реализации, то целью исследований является разработка математической и структурной моделей кодопреобразования моделей для систем аутентификации космического аппарата, обладающих минимальными временными затратами.

Материалы и методы исследования

Так как большинство протоколов аутентификации на основе доказательства с нулевым разглашением знаний реализуются по большому модулю, то для сокращения времени выполнения вычислений можно использовать МК. В непозиционных модулярных кодах используются взаимнопростые основания p_1, p_2, ..., p_k, где НОД(p_i, p_j) = 1 при $i \neq j$, с помощью которых получают остатки целого числа A. Тогда МК представляется как

$$A = (\alpha_1, \alpha_2, ..., \alpha_k), \quad (1)$$

где $\alpha_i \equiv A \bmod p_i$; $i = 1, \ldots, k$.

Так как остатки МК значительно меньше исходного числа A, то модульные операции над $A = (\alpha_1, \alpha_2, ..., \alpha_k)$ и $B = (\beta_1, \beta_2, ..., \beta_k)$ будут выполняться быстрее, так как справедливо

$$|A * B|_{p_i}^{+} = (|\alpha_1 * \beta_1|_{p_1}^{+}, |\alpha_2 * \beta_2|_{p_2}^{+}, ..., |\alpha_k * \beta_k|_{p_k}^{+}), \quad (2)$$

где $\alpha_i \equiv A \bmod p_i$; $\beta_i \equiv B \bmod p_i$.

Произведение оснований МК определяет его рабочий диапазон $P_{\text{раб}} = \prod_{i=1}^{k} p_i$.

Рассмотрим модификацию протокола аутентификации спутника, реализованной МК. В качестве секретных параметров применяются сеансовый ключ $S(j) = (S_1(j), ..., S_k(j))$ и параметр $T(j) = (T_1(j), ..., T_k(j))$, используемый для проверки нарушений использования сеансового ключа, где $S(j) \equiv S_i(j) \bmod p_i$; $T(j) \equiv T_i(j) \bmod p_i$. Протокол включает этапы:

1. На борту спутника сначала вычисляют истинный статус КА с помощью МК

$$Z_i(j) = \left| g^{S_i(j)} g^{T_i(j)} \right|_{p_i}^{+}, \quad (3)$$

где g – первообразный элемент мультипликативной группы по модулю p_i; $i = 1, 2, \ldots, k$.

2. На борту КА производится «зашумление» секретных параметров

$$S_i^*(j) = \left| S_i(j) + \Delta S_i(j) \right|_{p_i}^{+}; \; T_i^*(j) = \left| T_i(j) + \Delta T_i(j) \right|_{p_i}^{+}. \quad (4)$$

где $\Delta S(j), \Delta T(j)$ – параметры зашумления; $\Delta S(j) \equiv \Delta S_i(j) \bmod p_i$; $\Delta T(j) \equiv \Delta T_i(j) \bmod p_i$.

3. Затем на спутнике вычисляют зашумленный статус КА, представленного в МК

$$Z_i^*(j) = \left| g^{S_i^*(j)} g^{T_i^*(j)} \right|_{p_i}^{+}. \quad (5)$$

4. Для аутентификации спутника запросчик передает «вопрос» $d = (d_1,\ldots, d_k)$.

5. Ответчик, получив $d = (d_1,\ldots, d_k)$, осуществляет вычисление ответов на него

$$L_i(1) = \left|S_i^*(j) - d_i\, S_i\,(j)\right|^{+}_{\varphi(p_i)};$$

$$L_i(2) = \left|T_i^*(j) - d_i\, T_i\,(j)\right|^{+}_{\varphi(p_i)}. \qquad (6)$$

6. Ответчик выполняет обратное преобразование МК-ПСС истинного и зашумленного статусов, а также двух ответов на «вопрос» d, а затем передает их запросчику.

7. Получив ответ, запросчик осуществляет аутентификацию спутника, согласно

$$M = Z(j)^d\, g^{L(1)} g^{L(2)} \bmod P_{\text{раб}}, \qquad (7)$$

где

$$Z(j) = (Z_1(j), Z_2(j),..., Z_k(j));$$

$$L(1) = (L_1(1), L_2(1),..., L_k(1));$$

$$L(2) = (L_1(2), L_2(2),..., L_k(2)).$$

Если $M = Z^*(j)$, где $Z^*(j) = (Z_1^*(j),..., Z_k^*(j))$, то спутник является «своим».

Так как модулярные коды относятся к непозиционным кодам, то обязательной немодульной операцией выступает обратное преобразование МК-ПСС. Для преобразования МК в позиционный код используют китайскую теорему об остатках (КТО) [3, 4]. Тогда

$$A = \left|\alpha_1 B_1 + \alpha_2 B_2 + ... + \alpha_k B_k\right|^{+}_{P_{\text{раб}}}, \qquad (8)$$

где B_i – ортогональные базисы модулярного кода СОК; r_A – ранг числа A; $i = 1, 2,\ldots, k$.

Так как значения ортогональных базисов могут быть просчитаны заранее и занесены в LUT-таблицы, то обратное преобразование МК-ПСС можно реализовать на основе LUT-таблиц, что позволит сократить временные затраты на перевод.

Однако в процессе обратного преобразования на основе КТО может возникнуть ситуация, когда результат суммирования будет больше, чем рабочий диапазон $P_{\text{раб}}$. Но число A, представленное в МК, не может выходить за пределы $P_{\text{раб}}$. Для этого необходимо из суммы вычесть значение рабочего диапазона до выполнения условия $A < P_{\text{раб}}$. Для этого используется позиционная характеристика ранг r_A числа A. Тогда (9) можно представить

$$A = \sum_{i=1}^{k} \alpha_i B_i - r\ P_{\text{раб}}. \qquad (9)$$

Для вычисления r_A можно провести операцию целочисленного деления числа A на $P_{\text{раб}}$. Данная операция должна проводиться после получения результата суммирования. В работе [5] представлены алгоритмы деления с восстановлением и без восстановления остатков. Так, при использовании алгоритма деления с восстановлением остатка время вычисления одного разряда частного определяется как

$$t_1^{DIV} = (2t_{SUM} + t_{SH}), \qquad (10)$$

где t_{SUM} – время выполнения суммирования; t_{SUM} – время выполнения операции сдвига.

Снизить временные затраты возможно за счет использования алгоритма деления без восстановления остатка, для которого время вычисления одного разряда частного равно

$$t_2^{DIV} = (t_{SUM} + t_{SH}). \qquad (11)$$

При использовании операции деления при вычислении ранга r_A временные затраты на выполнение обратного преобразования МК-ПСС будут определяться

$$T_{\text{МК–ПСС}}^{DIV} = T_{SUM} + T_R + T_{MUL} + T_{SUB}, \qquad (12)$$

где T_{SUM} – время суммирования произведений остатков МК на ортогональные базисы; T_R – время вычисления ранга числа; T_{MUL} – время умножения ранга числа на $P_{\text{раб}}$; T_{SUB} – время выполнения операции вычитания.

Сократить временные затраты можно за счет использования модифицированного алгоритма вычисления ранга в МК. Так как значение r_A зависит от количества оснований МК, то его вычисления вводят дополнительное основание p_g, удовлетворяющее

$$\text{НОД}(P_{\text{раб}}, p_g) = 1, p_g > r_{\max}, \qquad (13)$$

где $r_{\max}$ – максимальное возможное значение ранга при переводе МК-ПСС.

Введение нового основания p_g делает справедливым следующее выражение

$$\alpha_g \equiv \left(\sum_{i=1}^{k} \alpha_i B_i - r_A P_{\text{раб}}\right) \bmod p_g. \qquad (14)$$

Тогда получаем

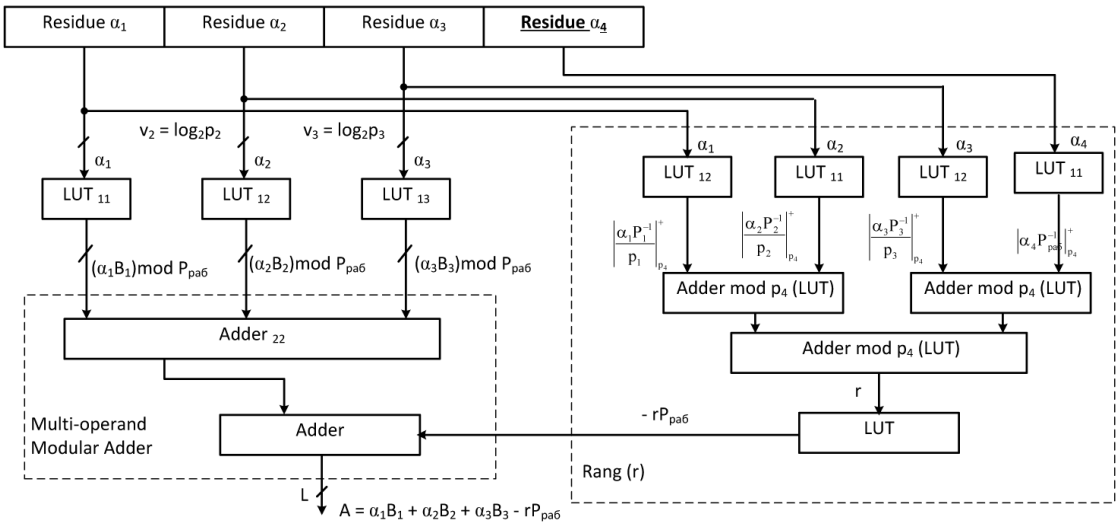
$$r_A P_{\text{раб}} = \left(\sum_{i=1}^{k} \alpha_i B_i - \alpha_g\right) \bmod p_g. \qquad (15)$$

Разделим обе части выражения (15) на рабочий диапазон. Тогда получаем

$$r_A = \left(\sum_{i=1}^{k} \alpha_i B_i P_{\text{раб}}^{-1} - \alpha_g P_{\text{раб}}^{-1}\right) \bmod p_g. \qquad (16)$$

Воспользуемся свойствам ортогональных базисов. Тогда имеем

$$\nu_i = P_i^* \big/ P_{\text{раб}} = p_i^{-1}. \qquad (17)$$



Структурная модель обратного преобразователя МК-ПСС

Подставим (17) в выражение (16). Положив, что $\nu_g = P_{\text{раб}i}^{-1} \bmod p_g$, получаем

$$r_A = \left(\sum_{i=1}^{k} \left| \alpha_i m_i \right|_{p_i}^{+} \nu_i + \alpha_g (p_g - \nu_g \right) \bmod p_g. \qquad (18)$$

Вычисленное значение ранга числа r_A умножается на величину (- $P_{\text{раб}}$). Для этого можно использовать LUT-таблицу. Полученный результат подается на сумматор, где он суммируется с результатом $\sum_{i=1}^{k} \alpha_i B_i$. В результате получается позиционный код числа A. На основании разработанной математической модели преобразования МК-ПСС была создана структурная модель кодопреобразователя, которая показана на рисунке.

Результаты исследования и их обсуждение

Рассмотрим применение разработанных математической и структурной моделей преобразователя МК-ПСС. Для системы аутентификации КА взяты $p_1 = 11$, $p_2 = 13$ и $p_3 = 19$.

Вычислим значение ортогонального базиса для первого основания кода СОК $p_1 = 11$. Тогда на основе алгоритма [3] имеем:

1. Вычислим значение $P_1^* = P_{\text{раб}} \big/ p_1 = p_2 p_3 = 247$.
2. Вычислим остаток полученного произведения $\delta_1 \equiv P_1^* \bmod p_1 = 247 \bmod 11 = 5$.
3. Значение веса ортогонального базиса $m_1 = 9$, так как $\delta_1 m_1 \bmod p_{11} = \left| 5 \cdot 9 \right|_{11}^{+} = 1$.
4. Значение ортогонального базиса равно $B_1 = m_1 P_1^* = 9 \cdot 247 = 2223$.

Аналогичным образом получаем ортогональные базисы $B_2 = 209$ и $B_3 = 286$.

Пусть число $A = 477 = (4, 9, 2)$. Так как $r_{\max} = 2$, то для вычисления ранг выбираем основание $p_4 = 7$. Тогда МК числа $A = 477 = (4, 9, 2, 1)$. Остатки числа записываются в регистры преобразователя. Затем остатки $(\alpha_1, \alpha_2, \alpha_3) = (4, 9, 2)$ поступают на входы таблиц LUT_{11} – LUT_{13}, с выхода которых снимаются значения сумму парных произведений

$$A_1 = \left| \alpha_1 m_1 \right|_{p_1}^{+} P_1^* = \left| 4 \cdot 9 \right|_{11}^{+} \cdot 247 = 741; \; A_2 = \left| \alpha_2 m_2 \right|_{p_2}^{+} P_2^* = 1881;$$

$$A_3 = \left| \alpha_3 m_3 \right|_{p_3}^{+} P_3^* = \left| 2 \cdot 2 \right|_{11}^{+} \cdot 143 = 572.$$

Результат подается на входы сумматора $Adder_{22}$, с выхода которого снимается

$$A^* = A_1 + A_2 + A_3 = 3194.$$

Параллельно с данными вычислениями происходит определение величины ранга числа. Остатки числа подаются на входы таблиц $LUT_{11} - LUT_{14}$ блока вычисления ранга. Данные ПЗУ осуществляют операцию умножения остатков кода СОК на константы v_i,

$$\nu_1 = \left|p_1^{-1}\right|_{p_4}^{+} = \left|11^{-1}\right|_7^{+} = 2;\ \nu_2 = \left|p_2^{-1}\right|_{p_4}^{+} = \left|13^{-1}\right|_7^{+} = 6;\ \nu_3 = \left|p_3^{-1}\right|_{p_4}^{+} = \left|19^{-1}\right|_7^{+} = 3;\ \nu_4 = \left|P_{\text{раб}}^{-1}\right|_{p_4}^{+} = 1.$$

Результаты умножения остатков на данные константы поступают на сумматор. Тогда

$$r_A = \left(\sum_{i=1}^{k}\left|\alpha_i m_i\right|_{p_i}^{+}\nu_i + \alpha_g(p_g - \nu_g\right)\bmod p_g = \left|\left|4\cdot 9\right|_{11}^{+}\cdot 2 + 9\cdot 6 + 4\cdot 3 + 1(7-1)\right|_7^{+} = 1.$$

Значение $r_A = 1$ подается на вход таблицы *LUT*, где умножается на величину ($- P_{\text{раб}}$). Результат подается на сумматор Adder, где суммируется с результатом A^*. Тогда имеем

$$A = A^* - r_A P_{\text{раб}} = 3194 - 1\cdot 2717 = 477.$$

Осуществим перевод МК-ПСС, используя китайскую теорему об остатках

$$A = \sum_{i=1}^{3}\left|\alpha_i m_i\right|_{p_i}^{+} P_i^* - r_A P_{\text{раб}} = 741 + 1881 + 572 - 1\cdot 2717 = 477.$$

Временные затраты на обратное преобразование МК-ПСС при использовании разработанной математической и структурной моделей составят

$$T_{\text{МК-ПСС}}^{\text{МК}} = T_{SUM}^{\text{МК}} + T_{SUB} = (T_{LUT} + T_{Adder}) + T_{SUB}. \quad (19)$$

Время считывания данных из LUT-таблицы будет определяться $\tau_э$ – временем срабатывания логических схем совпадения, т.е. $T_{LUT} = \tau_э$. При использовании алгоритма суммирования CAS для нахождения суммы двух операндов достаточно двух тактов работы одноразрядного сумматора t_{SUM}. Так как в сумматоре *Adder* складывается k парных произведений $\alpha_i B_i$, то справедливо

$$T_{Adder} = 2(k-1)t_{SUM} = 6(k-1)\tau_э. \quad (20)$$

Так как операция выполняется на позиционном сумматоре, то $T_{SUB} = 2t_{SUMэ} = 6\tau$. Тогда

$$T_{\text{МК}-\text{ПСС}}^{\text{МК}} = T_{SUM}^{\text{МК}} + T_{SUB} = (T_{LUT} + T_{Adder}) + T_{SUB} = 19\tau.$$

Определим временные затраты на преобразование МК-ПСС с использованием алгоритма деления с восстановлением остатка. Так как $r_{\max} = 2$, то время вычисления ранга

$$T_R^1 = r_{\max}(2t_{SUM} + t_{SH}) = 2(2\cdot 3\tau_э + 2\tau_э) = 16\tau_э,$$

где $t_{SUM} = 3\tau_э;\ t_{SH} = 2\tau_э$.

При использовании алгоритма деления без восстановления остатка получаем

$$T_R^2 = r_{\max}(t_{SUM} + t_{SH}) = 2(3\tau_э + 2\tau_э) = 10\tau_э.$$

Тогда время обратного преобразования МК-ПСС будет равно

$$T_{\text{МК-ПСС}}^{DIV1} = T_{SUM} + T_R^1 + T_{MUL} + T_{SUB} = 13\tau_э + 16\tau_э + \tau_э + 6\tau_э = 36\tau_э.$$

$$T_{\text{МК-ПСС}}^{DIV2} = T_{SUM} + T_R^2 + T_{MUL} + T_{SUB} = 13\tau_э + 10\tau_э + \tau_э + 6\tau_э = 30\tau_э.$$

Сравнительный анализ показывает, что разработанная математическая модель преобразования МК-ПСС на основе КТО позволяет в 1,94 раза быстрее выполнить обратное преобразование в позиционный код по сравнению с алгоритмом деления с восстановлением остатка, и в 1,54 раза – с без восстановления остатка. Очевидно, что разработанные математическая и структурная модели кодопреобразователя МК-ПСС целесообразно применять в системе аутентификации КА, функционирующей в модулярных кодах, так обеспечивают минимальные временные затраты.

Заключение

Для обеспечения минимальных временных затрат на аутентификацию КА целесообразно использовать МК. Однако для перехода от непозиционного МК к коду ПСС необходимо выполнить обратное преобразование. Поэтому разработка математической и структурной моделей преобразования МК-ПСС, обладающих

минимальными временными затратами, является актуальной задачей. В статье представлены математическая и структурная модель преобразования МК-ПСС на основе КТО, применение которых позволяет в 1,94 раза быстрее выполнить обратное преобразование в позиционный код по сравнению с алгоритмом деления с восстановлением остатка и в 1,54 раза – с без восстановления остатка. Очевидно, что разработанные математическая и структурная модели кодопреобразователя МК-ПСС целесообразно применять в системе аутентификации КА, функционирующей в МК, так обеспечивают минимальные временные затраты.

Исследование выполнено при финансовой поддержке РФФИ в рамках научного проекта № 18-07-01020.

Список литературы

1. Калмыков И.А., Ляхов А.В., Пашинцев В.П. Применение помехоустойчивого протокола аутентификации космического аппарата для низкоорбитальной системы спутниковой связи // Инфокоммуникационные технологии. 2015. Т. 13. № 2. С. 183–190.

2. Pashintsev V.P., Zhuk A.P., Rezenkov D.N. Application of spoof resistant authentication protocol of spacecraft in low earth orbit systems of satellite communication. International Journal of Mechanical Engineering and Technology. 2018. № 9 (5). 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. 734 p.

5. Червяков Н.И., Евдокимов А.А., Галушкин А.И., Лавриненко И.Н., Лавриненко А.В. Применение искусственных нейронных сетей и системы остаточных классов в криптографии. М.: Физматлит, 2012. 280 с.