УДК 681.3.05 **doi: 10.26906/SUNZ.2021.4.083**

А. С. Янко, О. В. Шефер, Я. Е. Денисенко

Національний університет «Полтавська політехніка імені Юрія Кондратюка», Полтава, Україна

ПОБУДОВА МАТЕМАТИЧНОЇ МОДЕЛІ СПЕЦПРОЦЕСОРА ОБРОБКИ КРИПТОГРАФІЧНОЇ ІНФОРМАЦІЇ НА ОСНОВІ ВИКОРИСТАННЯ ОСНОВНИХ ВЛАСТИВОСТЕЙ НЕПОЗИЦІЙНИХ КОДОВИХ СТРУКТУР

Анотація. Досліджено принципи реалізації арифметичних операцій у системі залишкових класів (СЗК). Використання розглянутих принципів та основних властивостей СЗК відкриває широкі можливості в побудові не тільки нової машинної арифметики, але й принципово нової схемної реалізації процесорів. На основі дослідженої інформації було побудовано математичну модель спецпроцесора обробки криптографічної інформації (СОКІ) на основі використання основних властивостей непозиційних кодових структур. На основі даних досліджень було проведемо порівняльний аналіз надійності потроєного позиційного СОКІ з мажоритарним елементом СОКІ у СЗК по безвідмовності, застосовуючи розглянуту надійнісну модель.

Ключові слова: комп'ютерна система, непозиційна система числення, система залишкових класів, система числення, спецпроцесор обробки криптографічної інформації.

Вступ

У даний момент неможливо уявити собі автоматичну чи комп'ютерну систему (КС) без того, щоб її центральну частина не складали процесори, що виконують функції обробки інформації та управління. У КС дії проводяться над числами, представленими у вигляді спеціальних машинних кодів у прийнятій системі числення. Залежно від способу зображення чисел, за допомогою цифр, існуючі системи числення (СЧ) умовно ділять на: позиційні та непозиційної системи.

Протягом останніх років результати, що проводилися щодо пошуку шляхів підвищення продуктивності КС, методів організації ефективної системи виявлення та виправлення помилок і побудови високонадійних обчислювальних комплексів довели, що в межах позиційної СЧ (ПСЧ) не можна очікувати скільки-небудь задовільного результату без істотного збільшення робочих частот елементів й ускладнення апаратурною частини КС. Також необхідно додати, що ПСЧ, в яких представляється і обробляється інформація в сучасних КС обробки даних, мають істотний недолік — наявність міжрозрядних зв'язків, які накладають свій відбиток на способи реалізації арифметичних операцій, ускладнюють апаратуру і обмежують швидкодію. Міжрозрядний зв'язок сприяє значному зниженню надійності, оскільки одиночна помилка в результаті переповнення розряду переноситься до наступного, сприяючи блок помилок.

На даний час існує цілий ряд галузей науки і техніки, де інформація особливо чутлива до внутрішніх помилок, що вносяться процесором під час виконання певних задач (реалізації арифметичних операцій), до одних з таких відноситься криптографія.

Зі стрімким розвитком криптографії виникла гостра необхідність швидкої та надійної оброки масивів криптографічної інформації. Сучасна прикладна криптографія проявляє усе більш виражену тенденцію до обліку вимог, пов'язаних з особливостями електронних інформаційних технологій.

В даний час використання шифрування для захисту інформації приймає усе більш виражений технологічний характер.

Технологічний характер вживання шифрування виявляється: у масовості вживання; у різноманітності вирішуваних завдань; у різноманітності умов вживання; у спеціалізації для вирішення конкретних завдань. Тому розробка швидкодіючого та надійного спецпроцесора обробки криптографічної інформації (СОКІ) являється однією із важливих завдань сьогодення.

Аналіз останніх досліджень і публікацій. Першим в СРСР в кінці 50-х років на непозиційну систему числення (НСЧ) звернув увагу Федір Вікторович Лукін. Один з провідних теоретиків в області НСЧ в системі залишкових класів (СЗК) і активних учасників її практичного застосування став доктор технічних наук, професор, академік НАН Казахстану Вільжан Мавлютинович Амербаєв [1].

Дана область зацікавила математика І. Я. Акушського і його начальника, провідного розробника КС обробки даних Д. І. Юдицького, які стали згодом основоположниками СЗК в СРСР. Напрацювання даних науковців довело, що в СЗК з'явилася можливість розпаралелити процес виконання арифметичних операцій: всі операції над залишками в кожній основі виконуються окремо і незалежно (паралельно), отже, в зв'язку з їх малою розрядністю, нескладно і швидко. Малорозрядність залишків забезпечує можливість реалізації табличній арифметики, при якій результат операції не вирахував кожен раз, а, одного разу розрахований, поміщається в запам'ятовуючий пристрій (ЗП) і при необхідності зчитується з нього, тобто, операція в СЗК при табличній арифметиці виконується за один період синхронізуючої частоти (машинний такт) [2]. Дослідження вчених призвели до створення досить своєрідної машинної арифметики названою системою залишкових класів.

Метою статті є побудова математичної моделі СОКІ на основі використання основних властивостей непозиційних кодових структур в СЗК та порівняльний аналіз надійності СОКІ різних видів.

Виклад основного матеріалу

У даній системі числення числа представляються своїми залишками від ділення на обрану систему основ, і всі раціональні операції можуть виконуватися паралельно над цифрами кожного розряду окремо. Основні властивості СЗК (незалежність залишків, рівноправність залишків, малорозрядність залишків) дозволяють усунути недоліки ПСЧ. Спільне використання першої і другої властивостей (незалежності й рівноправності залишків) обумовлює наявність в СОКІ одночасно трьох основних видів резервування: структурного, інформаційного та функціонального. А така властивість СЗК, як малорозрядність залишків дає можливість широкого вибору реалізації арифметичних операцій, заснованих на наступних методах:

- суматорному методі (на базі малорозрядних двійкових суматорів);
- табличному методі (на основі використання таблиць постійного ЗП (ПЗП));
- методі кільцевого зсуву, що заснований на використанні кільцевих регістрів зсуву.

Проаналізуємо властивості та особливості методів технічної реалізації арифметичних операцій у СЗК.

Аналіз відомих методів показав, що найбільш оптимальним з точки зору максимальної швидкодії виконання арифметичних операцій і забезпечення заданого рівня надійності функціонування СОКІ є табличний метод реалізації модульних операцій. Показано, що задачі, пов'язані з необхідністю використання табличної арифметики доцільно і ефективно вирішувати тільки у СЗК [3].

Результати аналізу основних властивостей СЗК дозволяють зробити висновок про те, що СОКІ, що функціонують у СЗК, відносяться до швидкодіючих та надійних об'єктів.

Зазначені особливості структури та принципів функціонування СОКІ в СЗК сприяють розробці ефективних й оптимальних методів резервування, що не мають аналогів в ПСЧ.

СЗК є досить своєрідною системою числення і, як усі існуючі системи числення, накладає обмеження не на структуру всієї машини в цілому, а лише на структуру арифметичного пристрою в світлі своєрідного трактування алгоритмів реалізації ряду операцій арифметичного пристрою. Тому у даній стаття буде розглянуто й досліджено структуру моделі СОКІ, що функціонують у СЗК.

Структурна схема СОКІ у СЗК являє собою набір управляючих пристроїв (мікропроцесорів), що функціонують у відповідному тракті незалежно один від одного і паралельно в часі, причому кожна по своєму, певному модулю m_i.

У цьому випадку пристрої введення та виведення вирішують також відповідно завдання перетворення вхідної інформації СОКІ з позиційного коду в код СЗК і навпаки.

Тобто структура СОКІ у СЗК представляє собою послідовне з'єднання каналів обробки інформації (КОІ).

Для підвищення надійності СОКІ у відповідних КОІ вводяться резервні тракти обробки інформації (ТОІ).

При проектуванні та експлуатації СОКІ дуже часто виникає завдання не тільки забезпечити необхідну надійність шляхом резервування, а й реалізувати це якомога більш економно. При цьому для СОКІ доводиться враховувати обмеження в габаритах, вазі, споживаної електроенергії, вартості та інших характеристиках.

Інакше кажучи, виникає задача оптимального резервування.

Синтезуючи структуру СОКІ у класі залишків ймовірність безвідмовної роботи СОКІ у ПСЧ можна визначити як ймовірність безвідмовної роботи СОКІ у ПСЧ для випадку ковзного резервування з навантаженим резервом.

У цьому випадку формула для визначення імовірності безвідмовної роботи СОКІ у СЗК прийме вигляд такого виразу:

$$P_{C3K}^{(k)}(t) = \\ = \sum_{i=0}^{k} C_{k+n}^{i} P_1^{k+n-i}(t) \sum_{j=0}^{i} (-1)^j C_i^j P_1^j(t). \quad (1)$$

Тут $P_1(t) = e^{-\lambda_1 t}$ – ймовірність безвідмовної роботи тракту СОКІ по найбільшій (найменш надійній) основі m_{n+k} СЗК, де λ_1 – інтенсивність відмов обладнання тракту СОКІ у СЗК найбільшій основі m_{n+k}.

Співвідношення (1) може бути використане для розрахунку імовірності безвідмовної роботи СОКІ в СЗК при таких припущеннях:

– відмови трактів СОКІ задовольняють умовам найпростішого потоку. В цьому випадку для розрахунку показників безвідмовності використовується експоненціальний розподіл, так як він достатньо обґрунтований теоретично, підтверджений експериментально і забезпечений відомостями про інтенсивність відмов елементів спецпроцесора обробки криптографічної інформації;

– комутуючі пристрої ідеальні (тобто ймовірність безвідмовної роботи комутатора дорівнює одиниці);

– інформаційні і контрольні тракти СОКІ рівнонадійні, тобто ймовірність безвідмовної роботи всіх трактів СОКІ приймається рівною імовірності безвідмовної роботи $P_1(t)$ тракту СОКІ по найбільшій основі СЗК m_{n+k}, що має найменшу ймовірність безвідмовної роботи;

– не враховується можливість відновлення трактів СОКІ у СЗК, які відмовили [4].

Відмітимо, що реальна надійність СОКІ у СЗК буде вищою, ніж та, що визначається співвідношенням (1), тому що дана формула не враховує можливість заміни одним контрольним трактом по основі m_j одного або одночасно декількох непрацездатних інформаційних трактів за умови:

$$m_j \geq \prod_{i=1}^{r} m_{k_i}, \quad (2)$$

де r – максимальне число трактів, які заміняються одним контрольним працездатним трактом по основі m_j.

Проведемо порівняльний аналіз надійності потроєного позиційного СОКІ з мажоритарним елементом СОКІ у СЗК по безвідмовності, застосовуючи розглянуту надійнісну модель.

Позначимо через λ_E інтенсивність відмов обладнання, віднесену до одного двійкового розряду (до одиниці розрядної сітки) [5]. В цьому випадку ймовірність безвідмовної роботи обладнання, віднесена до одного двійкового розряду СОКІ дорівнює:

$$P_E(t) = e^{-\lambda_E t}, \tag{3}$$

де λ_E – інтенсивність відмов обладнання, віднесену до одного двійкового розряду (до одиниці розрядної сітки). Для позиційного l-байтового СОКІ ймовірність безвідмовної роботи дорівнює:

$$P_0(t) = e^{-\lambda_0 t}, \tag{4}$$

де $\lambda_0 = 8\, l\, \lambda_E$.

З врахуванням λ_0 вираз (4) набуває наступного вигляду:

$$P_0(t) = e^{-\lambda_E l t}. \tag{5}$$

Відомо, що ймовірність безвідмовної роботи для потроєної мажоритарної структури, яка містить три СОКІ та ідеальний мажоритарний елемент, дорівнює [6-8]:

$$\begin{aligned} P_M(t) &= 3P_0^2(t) - 2P_0^3(t) = \\ &= e^{-16\lambda_E t}\left(3 - 2e^{-8\lambda_E t}\right). \end{aligned} \tag{6}$$

Для ЕОМ в СЗК ймовірність безвідмовної роботи тракту по довільній основі $m_i \left(i = \overline{1, n+k}\right)$:

$$P_1(t) = e^{-\lambda_1 t}; \tag{7}$$

або

$$P_1(t) = e^{-\lambda_E \alpha_{n+k} t}, \tag{8}$$

де $\alpha_{n+k} = [\log_2(m_{n+k} - 1)] + 1$.

Ймовірність безвідмовної роботи СОКІ у СЗК визначається відповідно до виразу (5).

Нехай $l = 1$ (однобайтовий СОКІ) і $k = 1$. Тоді з урахуванням критерію мінімальності апаратурної надлишковості СОКІ систему залишкових класів можна представити у виді набору наступних основ $m_1 = 3$, $m_2 = 4$, $m_3 = 5$, $m_4 = = 7$, $m_5 = 11$.

При цьому:

$$\prod_{i=1}^{4} m_i = 420 \succ 2^8 = 256, \tag{9}$$

і найбільший спільний дільник (НСД) $(m_i, m_j) = 1$ для $i \neq j$. В цьому випадку співвідношення (1) прийме вигляд:

$$\begin{aligned} P_{СЗК}^{(1)}(t) &= 5P_1^4(t) - 4P_1^5(t) = \\ &= e^{-16\lambda_E t}\left(5 - 4e^{-4\lambda_E t}\right), \end{aligned} \tag{10}$$

Позначимо $\lambda^* = 8\lambda_E$. При цьому вирази (6) і (10) можна записати наступним чином:

$$P_M(t) = e^{-2\lambda^* t}(3 - 2e^{-\lambda^* t}). \tag{11}$$

$$P_{СЗК}^{(1)}(t) = e^{-2\lambda^* t}\left(5 - 4e^{-0.5\lambda^* t}\right). \tag{12}$$

Нехай $k = 2$. У цьому випадку СЗК можна представити у виді набору таких основ: $m_1 = 3$, $m_2 = 4$, $m_3 = 5$, $m_4 = 7$, $m_5 = 11$, $m_6 = 13$.

Для даного набору основ вираження (1) запишемо наступним чином:

$$P_{СЗК}^{(2)}(t) = P_1^4(t) \cdot \left\{ \begin{array}{c} P_1^2(t) + 6P_1(t) \times \\ \times\left[1 - P_1(t)\right] + 15\left[1 - P_1(t)\right]^2 \end{array} \right\}. \tag{13}$$

Відповідно до вищенаведених виразів розраховуються значення імовірності безвідмовної роботи для потроєного позиційного СОКІ та для СОКІ у СЗК (рис. 1).

На рис. 1(а) представлено графіки залежностей $P(\lambda^* t)$ для однобайтових СОКІ: нерезервованого (I), триканального резервованого СОКІ у ПСЧ (II) і СОКІ у СЗК з параметрами $l = 1$, $n = 4$, $k = 1$ (III), а на рис. 1(б) при $k = 2$.

З рис. 1 видно, що СОКІ у СЗК з однією контрольною основою (III) більш надійніша потроєного позиційного процесора (II). При цьому критичне значення імовірності безвідмовної роботи СОКІ в класі залишків дорівнює 0,425, а критичне значення потроєної обчислювальної системи дорівнює 0,5, тобто розширюється область значень $\lambda^* t$, при яких збільшується (в порівнянні з нерезервованим позиційним СОКІ (I)) безвідмовність роботи непозиційного СОКІ.

Висновки

Основна властивість СЗК, а саме малорозрядність залишків дозволяє застосовувати табличні алгоритми реалізації арифметичних операцій, що різко підвищують надійність і продуктивність СОКІ. Показана можливість ефективного використання непозиційного кодування для покращення основних характеристик спецпроцесора обробки криптографічної інформації [9].

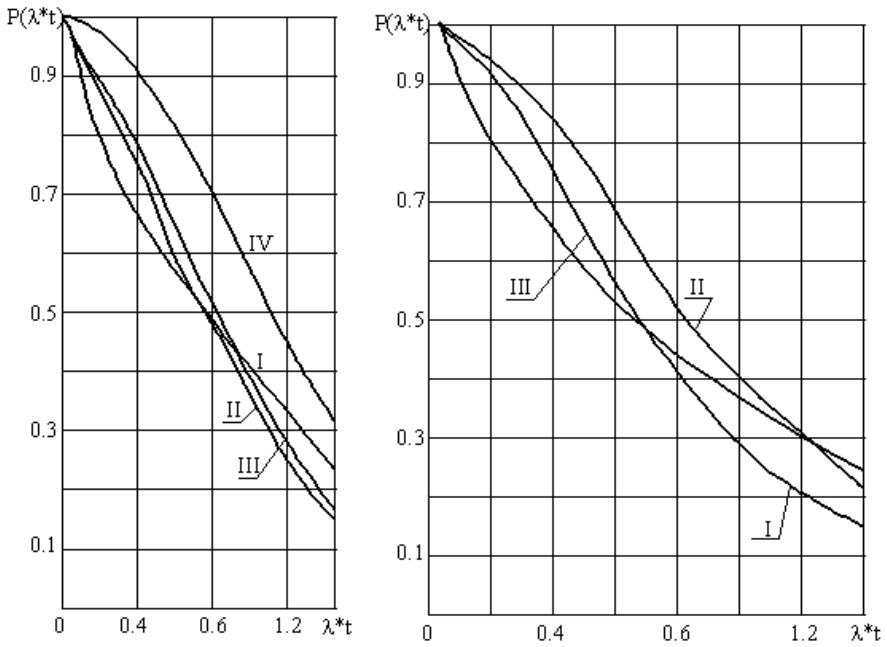
Результати досліджень показали, що СЗК при меншій додатково введеній кількості обладнання забезпечує не меншу надійність, чим потроєна або дубльована мажоритарна структура в ПСЧ, що дуже важливо при побудові спецпроцесора обробки криптографічної інформації.

Сформульовано та досліджено принципи обробки інформації в СЗК.

Проведено дослідження впливу основних властивостей СЗК на архітектуру і принципи функціонування СОКІ.

Розроблено та досліджено структуру математичної моделі надійності спецпроцесора обробки криптографічної інформації у СЗК.

Проведено порівняльний аналіз надійності СОКІ у СЗК і подібної тройованної мажоритарної структури в ПСЧ.



а б

Рис. 1. Графіки залежностей імовірності безвідмовної роботи $P(\lambda^* t)$:
а – при $k = 1$; б – при $k = 2$

СПИСОК ЛІТЕРАТУРИ

1. Krasnobayev V., Kuznetsov A., Yanko A., Koshman S., Zamula A. and Kuznetsova T. Data processing in the system of residual classes. Monograph. ASC Academic Publishing, 2019, 208 p.
2. Акушский И.Я,. Юдицкий Д.И. Машинная арифметика в остаточных классах. – М.: Сов. Радио, 1968. – 444 с.
3. Krasnobayev V., Yanko A. and Koshman S. A. Method for arithmetic comparison of data represented in a residue number system. Cybernetics and Systems Analysis, vol. 52, Issue 1, 2016, pp. 145–150.
4. Tuazon. J. O. Residue number system in computer arithmetic. Doctor of Philosophy, Iowa State University, Digital Repository, Ames, 1969.
5. Yadin A. *Computer Systems Architecture*. Chapman and Hall/CRC, 2016.
6. Donets V., Kuchuk N., Shmatkov S. Development of software of e-learning information system synthesis modeling process. *Сучасні інформаційні системи*. 2018. Т. 2, № 2. С. 117–121. DOI: https://doi.org/10.20998/2522-9052.2018.2.20
7. Кучук Н.Г., Гавриленко С.Ю., Лукова-Чуйко Н.В., Собчук В.В. Перерозподіл інформаційних потоків у гіперконвергентній системі / С.Ю. Гавриленко. *Сучасні інформаційні системи*. 2019. Т. 3, № 2. С. 116-121. DOI: https://doi.org/10.20998/2522-9052.2019.2.20
8. Nechausov A., Mamusuĉ I., Kuchuk N. Synthesis of the air pollution level control system on the basis of hyperconvergent infrastructures. Сучасні інформаційні системи. 2017. Т. 1, № 2. С. 21 – 26. DOI: https://doi.org/10.20998/2522-9052.2017.2.04
9. ISCI'2019: Information Security in Critical Infrastructures. Collective mono-graph. Edited by Ivan D. Gorbenko and Alexandr A. Kuznetsov. ASC Academic Publishing, Minden, Nevada USA, 2019, 445 p. – ISBN: 978-0-9989826-8-7 (Hardback), ISBN: 978-0-9989826-9-4 (Ebook)

Received (Надійшла) 27.10.2021
Accepted for publication (Прийнята до друку) 17.11.2021

Construction of mathematical model of special processor for processing of cryptographic information on the basis of use of main properties of non-positional codes

A. Yanko, O. Shefer, Y. Denysenko

Abstract. The principles of realization of arithmetic operations in the system of residual classes (SRC) are investigated. Studies have shown that in this number system, numbers are represented by their remainders from the division into the selected system of bases, and all rational operations can be performed in parallel over the digits of each digit separately. The main properties of SRC (independence of residues, equality of residues, low-bit residues) allow to eliminate the shortcomings of the positional number system. The joint use of the first and second properties (independence and equality of residues) determines the presence of three main types of redundancy in special processor of processing of the cryptographic information (SPPCI) at the same time: structural, informational and functional. And such a property of SRC as low-bit residues allows a wide choice of implementation of arithmetic operations. The use of the considered principles and basic properties of SRC opens wide possibilities in construction not only of new machine arithmetic, but also fundamentally new circuit realization of processors. On the basis of the researched information the mathematical model of the SPPCI on the basis of use of the basic properties of non-positional code structures was constructed. Based on these researches, we conducted a comparative analysis of the reliability of the triple positional SPPCI with the majority element of SPPCI in SRC on reliability, applying the considered reliable model.

Keywords: computer system, non-positional number system, number system, residual class system, special processor of cryptographic information processing.