УДК 519.111: 621.391 DOI: 10.26565/2519-2310-2019-2-01

МАТЕМАТИЧНА МОДЕЛЬ ПРОЦЕСУ ТАБЛИЧНОЇ РЕАЛІЗАЦІЇ ОПЕРАЦІЇ АЛГЕБРАЇЧНОГО МНОЖЕННЯ В КЛАСІ ЗАЛИШКІВ

Віктор Краснобаєв, Михайло Зуб, Олеся Решетняк,
Андрій Д'яченко, Ірина Локоткова, Костянтин Мисливцев

Харківський національний університет імені В.Н. Каразіна, майдан Свободи, 4, Харків, 61022, Україна
v.a.krasnobaev@gmail.com, mishazub007@gmail.com, lesyandr13@gmail.com
andrey.090220@gmail.com, lokotosyk@ukr.net, kostyavtx@gmail.com

Рецензент: Олександр Кузнецов, д.т.н., проф., академік Академії наук прикладної радіоелектроніки, Харківський національний університет імені В.Н. Каразіна, майдан Свободи 6, Харків, 61022, Україна
kuznetsov@karazin.ua

Надійшло: Вересень 2019.

Анотація: *На підставі властивостей класу залишків в статті синтезована математична модель процесу табличної реалізації модульного множення, як для позитивного, так і для негативного числових діапазонів обробки інформації засобами обробки цілочисельної інформації. Дана модель рекомендована до практичного застосування при розробці методів і алгоритмів швидкої обробки криптографічної інформації. Пошук шляхів спрощення структури табличного операційного пристрою засобу обробки цілочисельної інформації зумовив необхідність вдосконалення математичної моделі, методів і алгоритмів реалізації модульних операцій, що дозволяють підвищити ефективність застосування табличній арифметики в класі залишків. Особливістю реалізації даної моделі є можливість зменшення кількості обладнання операційного пристрою засобу обробки цілочисельної інформації за рахунок скорочення на (50-70)% логічних елементів "І" в вузлах таблиці постійний запам'ятовуючий пристрій, безпосередньо реалізують операцію модульного множення за довільним m_i модулю класу залишків. Це можливо за рахунок використання властивостей симетрії таблиці реалізації $a_i b_i (\mathrm{mod}\ m_i)$ модульної операції множення.*

Ключові слова: *клас залишків; реалізація таблиць; математична модель; операція алгебраїчне множення.*

1 Вступ

Складність завдань, які вирішуються сучасними системами і засобами обробки цілочисельної інформації (ЗОІ), обумовлює до них підвищені вимоги щодо якості обробки інформації [1-8]. Рішення широкого кола складних обчислювальних задач вимагає (наприклад, реалізація асиметричних криптографічних алгоритмів, оптимізація обчислень в теорії сигналів та шумостійке кодування [4, 8-11], реалізація симетричних крипто-примітивів [12-18] та багато іншого [19-22]) значних обсягів розрахунків, які проводяться в реальному часі функціонування ЗОІ. В цьому аспекті пошук методів і засобів підвищення продуктивності обробки цифрової інформації, є актуальним [23-30].

У будь-якій позиційній системі числення (ПСЧ) виконання арифметичних операцій передбачає послідовну обробку всіх розрядів операндів за правилами, що визначаються змістом даної операції, і не може бути закінчено до тих пір, поки не будуть послідовно визначені значення всіх проміжних результатів з урахуванням всіх міжрозрядних зв'язків операндів. Таким чином, ПСЧ, в якій представляється і обробляється інформація в сучасних обчислювальних машинах, мають істотний недолік - наявність логічних зв'язків між двійковими розрядами в оброблюваних операндах. Даний недолік робить істотний вплив на методи реалізації арифметичних операцій, ускладнюють апаратуру і обмежують швидкодію. Тому природно вишукування такої машинної арифметики, в якій би порозрядні зв'язку були б ослаблені, або відсутні взагалі. Відзначимо, будь-яка система числення в більшій мірі впливає на структуру і принципи функціонування операційного пристрою (ОП) ЗОІ.

Пошук шляхів підвищення продуктивності обробки інформації позиційних ЗОІ реального часу привів до необхідності проведення досліджень можливості використання табличного методу (табличної арифметики) реалізації модульних операцій. У загально-

му випадку табличне ОП ЗОІ, призначене для реалізації арифметичних операцій (які реалізується в унітарній коді), являє собою двовхідний постійний запам'ятовуючий пристрій (ПЗП). Для кожного з входів ПЗП кількість вхідних шин для *l*-байтового (8l двійкових розряди) ОП одно 28l. При цьому загальна кількість логічних схем збігу "І" в вузлах ПЗП (яке в основному і визначає загальну кількість обладнання табличного ОП ЗОІ) рівно

$$N_{l\,ПСЧ} = 2^{8l} \times 2^{8l} = 2^{16l}.$$

Виходячи з цього, очевидно, що таблична реалізація цілочисельних модульних арифметичних операцій в ПСЧ може бути доцільна тільки для значення *l=1*. Дійсно, в цьому випадку

$$N_{1ПСЧ} = 2^{16} = 65536,$$

що є прийнятним кількістю обладнання ОП для сучасного розвитку елементної бази. Однак, як зазначено вище, тенденція розвитку систем і засобів обробки криптографічного інформації (ЗОКІ) спрямована на збільшення довжини розрядної сітки ЗОІ. Вже зараз необхідно для практичного використання ЗОКІ з l = 4 і l = 8. В цьому випадку

$$N_{4ПСЧ}=2^{32}\times 2^{32}=2^{64} \text{ і } N_{8ПСЧ}=2^{64}\times 2^{64}=2^{128}.$$

Якщо врахувати, наприклад, що 2^{32}=4294967296, 2^{64}=18446744073709551616, а $2^{128} \approx 3{,}4\times 10^{38}$, то очевидно, що табличний метод реалізації арифметичних операцій в ПСЧ практично не можливо застосувати.

Інші результати використання табличного методу реалізації арифметичних операцій можна отримати, якщо розглянути ЗОКІ в непозиційній системі числення класу залишків (КЗ). Клас залишків має унікальну властивість незалежності один від одного залишків за прийнятою системі підстав. Ця незалежність відкриває широкі можливості у побудові не тільки нової машинної арифметики, а й принципово нової схемної реалізації ЗОКІ, яка в свою чергу помітно розширює застосування табличної арифметики [1-3, 23-26]. Дійсно, в загальному випадку, для *l*-байтових машинних слів, при реалізації алгоритмів модульної обробки інформації для табличного ОП ЗОІ в КЗ не обходимо

$$N_{lКЗ} = \sum_{i=1}^{n} m_i^2$$

схем збігу І, а для ОП ЗОІ в КЗ з l=4 и l=8 відповідно маємо $N_{4КЗ}$=2397 і $N_{8КЗ}$=13275, що цілком прийнято при реалізації арифметичних операцій додавання, віднімання і множення тим більше використовуючи сучасну елементну мікроелектронну базу (НВІС, ПЛМ або ПЛІС). Вищезазначена обставина підтверджує доцільність і ефективність проведення практичних досліджень та розробки табличних методів і алгоритмів реалізації модульних операцій в КЗ.

Відзначимо основні переваги табличного методу побудови ОП ЗОІ в КЗ. По-перше, високу швидкодію виконання арифметичних операцій. Результат операції може бути отриманий в момент надходження вхідних операндів в табличний процесор, тобто практично за один такт роботи ЗОІ. Таким чином, час виконання арифметичних операцій в КЗ порівняно з тактовою частотою обчислювача, що принципово неможливо для позиційних обчислювальних машин при існуючій елементній базі. По-друге, табличні ОП мають високу надійність, так як реалізуються у вигляді набору, по числу n модулів m_i КЗ, компактних ПЗП. В цьому випадку весь тракт, що складається з *n* (по числу модулів m_i КЗ), обробки інформації ОП будується за блоковим принципом, що покращує безвідмовність і ремонтопридатність ЗОІ. По-третє, відзначимо простоту технічної реалізації ОП ЗОІ в КЗ, що складається в основному з регістрів, табличних суматорів, шифраторів і дешифраторів і уніфікацію його обладнання для довільного модуля $\{m_i\}, i = \overline{1,n}.$

Відзначимо, необхідність розробки методів і алгоритмів арифметичного множення чисел необхідно попередньо мати і надалі використовувати математичну модель (ММ) процесу табличній реалізації операції модульного множення в КЗ.

2 Огляд джерел

У літературі описані ММ, на підставі яких реалізовані табличні методи і алгоритми модульного множення чисел в непозиційної системі числення КЗ [1-3, 27-30]. Пошук шляхів спрощення структури табличного ОП ЗОІ зумовив необхідність вдосконалення ММ, методів і алгоритмів реалізації модульних операцій, що дозволяють підвищити ефективність застосування табличній арифметики в КЗ. Так в [1, 2, 23] представлена ММ процесу табличної реалізації операції арифметичного модульного множення в КЗ. Особливістю реалізації даної моделі є можливість зменшення кількості обладнання ОП ЗОІ за рахунок скорочення на (50-70)% логічних елементів "І" в вузлах таблиці ПЗП, безпосередньо реалізують операцію модульного множення за довільним m_i модулю КЗ. Це можливо за рахунок використання властивостей симетрії таблиці реалізації $a_i b_i (\mathrm{mod}\, m_i)$ модульної операції множення.

В КЗ число А представляється у вигляді сукупності залишків $\{a_i\}$ по n модулях (підстав) $\{m_i\}$, де:

$$a_i = A - [A / m_i] \cdot m_i; \quad M = \prod_{i=1}^{n} m_i .$$

У цьому випадку число А в КЗ представляється в наступному вигляді

$$A = (a_1, a_2, ..., a_n).$$

Нехай задана пара операндів

$$A = (a_1, ..., a_n) \text{ та } B = (b_1, ..., b_n)$$

в КЗ з попарно взаємно простими основами $m_1,\ldots,m_n$.. Відповідно до правил виконання арифметичних операцій в КЗ кожній парі залишків a_i і b_i ставлять у відповідність величина $(a_i \otimes b_i) \bmod m_i$. Таким чином, весь машинний тракт обчислювальної операції $(A \otimes B) \bmod M$ в КЗ можна представити у вигляді n незалежних однотипних ПЗП.

Розглянемо процедуру реалізації операції модульного множення (найбільш трудомістку арифметичну операцію). Складемо таблицю з числових значень $a_i b_i (\mathrm{mod}\, m_i)$. Ця таблиця симетрична щодо діагоналей, вертикалі і горизонталі, що проходять між числами

$$\frac{(m_i - 1)}{2} \text{ та } \frac{(m_i + 1)}{2} \text{ для } m_i \text{ - непарного числа.}$$

Симетричність щодо лівої діагоналі визначається комутативністю операції множення

$$a_i \cdot b_i = b_i \cdot a_i .$$

Симетричність щодо правої діагоналі визначається тим, що

$$a_i \cdot b_i \equiv [(m_i - b_i)(m_i - a_i)] \bmod m_i .$$

Симетричність щодо вертикалі і горизонталі визначається з умови кратності по модулю m_i суми симетричних чисел:

$$a_i b_i \equiv [m_i - a_i (m_i - b_i)] \bmod m_i ,$$

$$a_i b_i \equiv [m_i - b_i (m_i - a_i)] \bmod m_i .$$

Використовуючи властивості симетрії можна повністю відновити таблицю даних модульного множення $a_i b_i (\mathrm{mod}\, m_i)$. Для цього достатньо мати числову інформацію тільки її восьмий частини. Звідси виникає можливість спростити таблицю (зменшити кількість схем збігу ПЗП) модульного множення.

Для реалізації операції $a_i b_i (\mathrm{mod}\, m_i)$ має бути ефективним, з точки зору швидкодії виконання операції множення, в чотири рази зменшити таблицю модульного множення. Для вирішення поставленого завдання необхідно ввести ознака, що визначає місце розташування вхідних чисел в кожному з чотирьох квадрантів таблиці $a_i b_i (\mathrm{mod}\, m_i)$.

Розглянемо один з можливих варіантів кодування вхідних операндів a_i і b_i таблиці по модулю m_i за допомогою коду інформаційного стиснення даних (КІСД).

Нехай дано вхідні операнди a_i та b_i. Значення a_i (або b_i), що лежать в діапазоні $\left[0, \frac{m_i-1}{2}\right)$, можуть бути закодовані довільним чином, а значення a_i (або b_i), що лежать в діапазоні $\left[\frac{m_1+1}{2}, m_i-1\right)$, кодуються, як $m_i - a_i$(або $m_i - b_i$). Для відмінності діапазонів вводиться ознака γ_a (γ_b) КІСД, певний в такий спосіб:

$$\gamma_a\ (\gamma_b) = \begin{cases} 0, \textit{ якщо } 0 \le a_i(b_i) \le \dfrac{m_i-1}{2}, \\ 1, \textit{ якщо } \dfrac{m_i+1}{2} \le a_i(b_i) \le m_i - 1, \end{cases}$$

де $0 \le a^*(b^*) \le (m_i - 1)/2.$

Процедура визначення результату операції модульного множення, за допомогою введеного коду інформаційного стиснення даних, наступний: якщо задані два числа в КІСД виду

$$a_i = (\gamma_a, a_i^*), b_i = (\gamma_b, b_i^*),$$

то для отримання твіру цих чисел по модулю m_i, досить отримати добуток $a_i^* b_i^* (\mathrm{mod}\, m_i)$ і інвертувати його узагальнену ознаку γ_i в разі, якщо γ_a відмінно від γ_b, тобто

$$a_i b_i (\mathrm{mod}\, m_i) = (\gamma_i, a_i^* b_i^* (\mathrm{mod}\, m_i)), \quad \text{де } \gamma_i = \begin{cases} \overline{\gamma_i}, \textit{ якщо } \gamma_a \ne \gamma_b, \\ \gamma, \textit{ якщо } \gamma_a = \gamma_b. \end{cases}$$

Запропонований варіант реалізації модульних операцій в КЗ дозволяють оптимізувати структуру ЗОІ шляхом підвищення ефективності використання табличній арифметики. Скорочення кількості обладнання ПЗП, що складають основну частину ОП, дозволяє підвищити на дійсні показники (збільшити ймовірність безвідмовної роботи P(t), зменшити час відновлення $T_в$) і поліпшити експлуатаційно-технічні показники (зменшити масу і габаритні розміри, зменшити споживану потужність і поліпшити технічне обслуговування ЗОІ в КЗ).

З огляду на КІСД, математична модель процесу табличної реалізації в позитивному числовому діапазоні двох чисел в КЗ випаде наступними математичними співвідношеннями:

$$\begin{aligned} C = A \cdot B (\mathrm{mod}\, M) = [(a_1, a_2, ..., a_i, ..., a_n) \cdot (b_1, b_2, ..., \\ ,..., b_i, ..., b_n)] \mathrm{mod}\, M = [(a_1 \cdot b_1) \mathrm{mod}\, m_1, (a_2 \cdot b_2) \mathrm{mod}\, m_2, ..., \\ ,..., (a_i \cdot b_i) \mathrm{mod}\, m_i, ..., (a_n \cdot b_n) \mathrm{mod}\, m_n] = \\ = \{[(\gamma_{a_1}, a_1^*) \cdot (\gamma_{b_1}, b_1^*)] \mathrm{mod}\, m_1, [(\gamma_{a_2}, a_2^*) \cdot \\ \cdot (\gamma_{b_2}, b_2^*) \mathrm{mod}\, m_2], ..., (\gamma_{a_i}, a_i^*) \cdot (\gamma_{b_i}, b_i^*) \mathrm{mod}\, m_i], ..., \\ ,..., [(\gamma_{a_n}, a_n^*) \cdot (\gamma_{b_n}, b_n^*)] \mathrm{mod}\, m_n\} = \{[\gamma_1, (a_1^* \cdot b_1^*) \mathrm{mod}\, m_1], [\gamma_2, (a_2^* \cdot b_2^*) \mathrm{mod}\, m_2], ..., \\ ,..., [\gamma_i, (a_i^* \cdot b_i^*) \mathrm{mod}\, m_i], ..., [\gamma_n, (a_n^* \cdot b_n^*) \mathrm{mod}\, m_n]\} = (c_1, c_2, ..., c_i, ..., c_n). \end{aligned} \tag{1}$$

При цьому ознака γ_{a_i} (γ_{b_i}) коду (γ_{a_i}, a_i^*) $((\gamma_{b_i}, b_i^*))$ КІСД таблиці модульного множення для довільного m_i модуля КЗ визначається наступним чином. Для m_i - парного

$$\gamma_{a_i}(\gamma_{b_i}) = \begin{cases} 0, \textit{ якщо } 0 \le a_i(b_i) \le m_i/2, \\ 1, \textit{ якщо } m_i/2 < a_i(b_i) \le m_i - 1. \end{cases} \tag{2}$$

Для m_i - непарного

$$\gamma_{a_i}(\gamma_{b_i}) = \begin{cases} 0, & якщо\ 0 \le a_i(b_i) \le (m_i - 1)/2, \\ 1, & якщо\ (m_i - 1)/2 < a_i\ (b_i) \le m_i - 1. \end{cases} \quad (3)$$

при цьому $0 \le a_i(b_i) \le m_i - 1$.

Числова частина $a_i^*\ (b_i^*)$ КІСД визначається так. Для m_i - парного це буде

$$a_i^*\ (b_i^*) = \begin{cases} a_i\ (b_i),\ якщо\ 0 \le a_i(b_i) \le m_i/2; \\ \overline{a_i}\ (\overline{b_i}) = m_i - a_i(b_i),\ якщо\ m_i/2 < a_i(b_i) \le m_i - 1, \end{cases} \quad (4)$$

при цьому $0 \le a_i^*(b_i^*) \le m_i/2$.

Для m_i -непарного

$$a_i^*(b_i^*) = \begin{cases} a_i(b_i),\ якщо\ 0 \le a_i(b_i) \le (m_i - 1)/2, \\ \overline{a_i}(\overline{b_i}) = m_i - a_i(b_i),\ якщо\ (m_i - 1)/2 < a_i(b_i) \le m_i - 1, \end{cases} \quad (5)$$

при цьому $0 \le a_i^*(b_i^*) \le (m_i - 1)/2$.

Якщо $(a_i \cdot b_i) \bmod m_i$ модульного множення визначається в КІСД як $[\gamma_i, (a_i^* \cdot b_i^*) \bmod m_i]$, тоді

$$(a_i \cdot b_i) \bmod m_i = \begin{cases} (a_i^* \cdot b_i^*) \bmod m_i, \\ якщо\ (\gamma_{a_i} + \gamma_{b_i}) = 0\ (\bmod 2); \\ m_i - (a_i^* \cdot b_i^*) \bmod m_i, \\ якщо\ (\gamma_{a_i} + \gamma_{b_i}) = 1\ (\bmod 2), \end{cases} \quad (6)$$

при цьому $0 \le (a_i^* \cdot b_i^*) \bmod m_i \le m_i - 1$.

Таким чином, сукупність виразів (2) - (6) є ММ процесу табличної реалізації модульного арифметичного множення в КЗ.

Недолік розглянутої ММ полягає в тому, що її використання не дає можливості створити табличний метод реалізації операції алгебраїчного множення в КЗ.

Мета статті - розробити ММ процесу табличної реалізації множення в КЗ як для позитивного, так і для негативного числових діапазонів.

2 Основна частина

Для побудови ММ процесу табличної реалізації множення в КЗ, як для позитивного, так і для негативного числових діапазонів представимо вхідні числа А і В у наступному вигляді (штучна форма представлення чисел в КЗ [4])

$A' = A + m/2$ та $B' = B + m/2$, для m – парних чисел;

$A' = A + (m-1)/2$ та $B' = B + (m-1)/2$, для m – непарних чисел.

Якщо, наприклад, m парне число, тоді виконуються наступні співвідношення

$$\begin{cases} -m/2 \le A(B) < m/2, \\ 0 \le A'(B') < m - 1, \\ -m/2 \le A \cdot B < m/2, \\ 0 \le (A \cdot B)' < m - 1. \end{cases}$$

Очевидно, що

$$(A \cdot B)' = A \cdot B + m/2. \quad (7)$$

Тоді маємо

$$(A'\cdot B')\bmod m=\left[\ (A+\ {}^{m}\!/_{2})(B+\ {}^{m}\!/_{2})\ \right]\bmod m=$$
$$=\left[\ AB(\bmod\ {}^{m}\!/_{2})+{}^{m}\!/_{2}\cdot(A+B+\ {}^{m}\!/_{2})\ \right]\bmod m. \quad (8)$$

З виразу (8) очевидно, що

$$A\cdot B=A'\cdot B'-{}^{m}\!/_{2}\cdot(A+B+{}^{m}\!/_{2}) \quad (9)$$

Підставимо вираз (9) в формулу (7). Отримаємо, що

$$(A\cdot B)'=A'\cdot B'-{}^{m}\!/_{2}\cdot(A+B+{}^{m}\!/_{2})+{}^{m}\!/_{2} \quad (10)$$

У виразі (10) є член, який має числове значення m / 2. Він і обумовлює помилку в обчисленні значення $A'\cdot B'(\bmod m)$. Таким чином формули для обчислення AB (mod m) мають такий вигляд для m парних чисел

$$\left[(A\cdot B)\bmod\ {}^{m}\!/_{2}\ \right]'=(A'\cdot B')\bmod m+{}^{m}\!/_{2}, \quad (11)$$

або

$$\left[\ (A\cdot B)\bmod\ {}^{m}\!/_{2}\ \right]'=(A'\cdot B')\bmod m. \quad (12)$$

Для m непарного маємо

$$\left[\ (A\cdot B)\bmod{}^{(m-1)}\!/_{2}\ \right]'=(A'\cdot B')\bmod m+{}^{(m-1)}\!/_{2}, \quad (13)$$

або

$$\left[\ (A\cdot B)\bmod{}^{(m-1)}\!/_{2}\ \right]'=(A'\cdot B')\bmod m. \quad (14)$$

З огляду на вираження (7) ÷ (14), побудуємо ММ процесу модульного множення для позитивного і негативного (алгебраїчне множення) цілочисельних числових діапазонів.

$$a_i'=a_i+m_i/2,\ a_i'=a_i'+(m_i-1)/2;\ a_i'=[\gamma'_{a_i},(a_i')^*]$$
$$b_i'=b_i+m_i/2,\ b_i'=b_i'+(m_i-1)/2;\ b_i'=[\gamma'_{b_i},(b_i')^*] \quad (15)$$

Для m_i - парного

$$\gamma'_{a_i}(\gamma'_{b_i})=\begin{cases}0,\ якщо\ 0\le a_i'(b_i')\le m_i/2,\\ 1,\ якщо\ m_i/2<a_i'(b_i')\le m_i-1.\end{cases} \quad (16)$$

Для m_i - непарного

$$\gamma'_{a_i}(\gamma'_{b_i})=\begin{cases}0,\ якщо\ 0\le a_i'(b_i')\le (m_i-1)/2,\\ 1,\ якщо\ (m_i-1)/2<a_i'(b_i')\le m_i-1.\end{cases} \quad (17)$$

Числова частина $(a_i')^*\ [(b_i')^*]$ КІСД визначається наступним чином. Для m_i- парного

$$(a_i')^*[(b_i')^*]=\begin{cases}a_i'\ (b_i'),\ якщо\ 0\le a_i'(b_i')\le m_i/2;\\ \overline{a_i'}\ (\overline{b_i'})=m_i-a_i'(b_i'),\\ якщо\ m_i/2<a_i'(b_i')\le m_i-1,\end{cases} \quad (18)$$

при цьому $0\le(a_i')^*\ [(b_i')^*]\le m_i/2$. Для m_i- непарного числа

$$(a_i')^*[(b_i')^*]=\begin{cases}a_i'\ (b_i'),\ якщо\ 0\le a_i'(b_i')\le (m_i-1)/2;\\ \overline{a_i'}\ (\overline{b_i'})=m_i-a_i'(b_i'),\\ якщо\ (m_i-1)/2<a_i'(b_i')\le m_i-1,\end{cases} \quad (19)$$

при цьому $0 \le (a_i')^* [(b_i')^*] \le (m_i - 1)/2$.

Результат $(a_i' \cdot b_i') \bmod m_i$ операції визначається в КІСД, тобто у вигляді

$$\left\{\gamma_i', [(a_i')^* (b_i')^*] \bmod m_i\right\},$$

тоді

$$(a_i' \cdot b_i') \bmod m_i = \begin{cases} [(a_i')^* \cdot (b_i')^*] \bmod m_i, \\ якщо\ (\gamma'_{a_i} + \gamma'_{b_i}) = 0 \pmod 2; \\ m_i - [(a_i')^* \cdot (b_i')^*] \bmod m_i, \\ якщо\ (\gamma'_{a_i} + \gamma'_{b_i}) = 1 \pmod 2, \end{cases} \tag{20}$$

при цьому $0 \le [(a_i')^* \cdot (b_i')^*] \bmod m_i \le m_i - 1$.

Формула для визначення добутку двох чисел в КЗ має такий вигляд:

$$\begin{aligned} &(A \cdot B) \bmod M = (A' \cdot B') \bmod M = [(a_1', a_2', ..., a_i', ..., \\ &..., a_n') \cdot (b_1', b_2', ..., b_i', ..., b_n')] = [(a_1' \cdot b_1') \bmod m_1, \\ &(a_2' \cdot b_2') \bmod m_2, ..., (a_i' \cdot b_i') \bmod m_i, ..., (a_n' \cdot b_n') \bmod m_n]. \end{aligned} \tag{21}$$

Так як усі модулі $\{m_i\}$, $i = \overline{1, n}$ КЗ, (*за винятком можливо тільки однієї основи*), непарні числа, то у подальшому, без втрати спільності міркувань, будемо вважати що основа КЗ - непарні числа. Формула (21) з урахуванням КІСД має такий вигляд

$$\begin{aligned} &(A' \cdot B') \bmod M = (\{[\gamma'_{a_1}, (a_i')^*] \cdot [\gamma'_{b_1}, (b_1')^*]\} \bmod m_1, \\ &\{[\gamma'_{a_2}, (a_2')^*] \times [\gamma'_{b_2}, (b_2')^*]\} \bmod m_2, ..., \{[\gamma'_{a_i}, (a_i')^*] \times \\ &\times [\gamma'_{b_i}, (b_i')^*]\} \bmod m_i, ..., [\gamma'_{a_n}, (a_n')^*] \cdot [\gamma'_{b_n}, (b_n')^*]\} \bmod m_n) = \\ &= (\{\gamma_1', [(a_1')^* \cdot (b_1')^*] \bmod m_1\}, \{\gamma_2', [(a_2')^* \cdot (b_2')^*] \bmod m_2\}, \\ &..., \{\gamma_i', [(a_i')^* \cdot (b_i')^*] \bmod m_i\}, ..., \{\gamma_n', [(a_n')^* \times (b_n')^*] \bmod m_n\}), \end{aligned} \tag{22}$$

де

$$\begin{aligned} (a_i' \cdot b_i') \bmod m_i &= \{[\gamma'_{a_i}, (a_i')^*] \cdot [\gamma'_{b_i}, (b_i')^*]\} \bmod m_i = \\ &= \{\gamma_i', [(a_i')^* \cdot (b_i')^*]\} \bmod m_i. \end{aligned} \tag{23}$$

Виходячи з (22) ÷ (23) де, а також враховуючи, що (15) ÷ (21), для m – непарного отримаємо наступні співвідношення для реалізації модульної операції алгебраїчного множення в КЗ

$$\begin{cases} \{(a_i \cdot b_i) \bmod [(m_i - 1)/2]\}' = \{[(\gamma_{a_i}, a_i) \times \\ \times (\gamma_{b_i}, b_i)] \bmod [(m_i - 1)/2]\}' = (a_i' \cdot b_i') \bmod m_i + \\ + (m_i - 1)/2 = \{[\gamma'_{a_i}, (a_i')^*] \cdot [\gamma'_{b_i}, (b_i')^*]\} \bmod m_i + \\ + (m_i - 1)/2 = \{\gamma_i', [(a_i')^* \cdot (b_i')^*] \bmod m_i + (m_i - 1)/2; \\ \{(a_i \cdot b_i) \bmod [(m_i - 1)/2]\}' = \{[(\gamma_{a_i}, a_i) \times \\ \times (\gamma_{b_i}, b_i)] \bmod [(m_i - 1)/2]\}' = (a_i' \cdot b_i') \bmod m_i = \\ = \{[\gamma'_{a_i}, (a_i')^*] \cdot [\gamma'_{b_i}, (b_i')^*]\} \bmod m_i = \\ = \{\gamma_i', [(a_i')^* \cdot (b_i')^*] \bmod m_i\}. \end{cases} \tag{24}$$

Для m_i – парного числа отримаємо

$$
\begin{cases}
(a_i \cdot b_i) \bmod [m_i / 2]\}' = \{[\,(\gamma_{a_i}, a_i) \times \\
\times (\gamma_{b_i}, b_i)\,] \bmod [m_i / 2]\}' = \\
= (a_i' \cdot b_i') \bmod m_i + m_i / 2 = \{[\,\gamma_{a_i}', (a_i')^*\,] \times \\
\times [\gamma_{b_i}', (b_i')^*\,]\} \bmod m_i + m_i / 2 = \{\gamma_i', (a_i')^* \times \\
\times (b_i')^*\,]\} \bmod m_i + m_i / 2; \\
\{(a_i \cdot b_i) \bmod [m_i / 2]\}' = \{[\,(\gamma_{a_i}, a_i) \cdot (\gamma_{b_i}, b_i)] \bmod [m_i / 2]\}' = \\
= (a_i' \cdot b_i') \bmod m_i = \{[\gamma_{a_i}', (a_i')^*] \cdot [\gamma_{b_i}', (b_i')^*]\} \bmod m_i = \\
= \{\gamma_i', [\,(a_i')^* \cdot (b_i')^*\,] \bmod m_i.
\end{cases}
\tag{25}
$$

Співвідношення (24) ÷ (25) є математичною моделлю процесу табличної реалізації операцій алгебраїчного множення в КЗ.

4 Висновки

Таким чином, на підставі властивостей КЗ в статті синтезована математична модель процесу табличної реалізації модульного множення, як для позитивного, так і для негативного числових діапазонів обробки інформації ЗОІ. Дана модель рекомендована до практичного застосування при розробці методів і алгоритмів швидкої обробки криптографічної інформації.

Посилання

[1] Akushsky I. Ya.,Yuditsky DI. Machine arithmetic in residual classes, Moscow: Soviet radio, 1968, 440 p. (In Russian)

[2] Torgashov V. A. The system of residual classes and reliability of digital computers, Moscow: Soviet radio, 1973, 118 p. (In Russian)

[3] Krasnobayev V., Kuznetsov A., Koshman S., Moroz S. (2019) Improved Method of Determining the Alternative Set of Numbers in Residue Number System. In: Chertov O., Mylovanov T., Kondratenko Y., Kacprzyk J., Kreinovich V., Stefanuk V. (eds) Recent Developments in Data Science and Intelligent Analysis of Information. ICDSIAI 2018. Advances in Intelligent Systems and Computing, vol 836. Springer, Cham, pp. 319-328, 05 August 2018.

[4] F. Barsi and P. Maestrini, "Error Correcting Properties of Redundant Residue Number Systems," in IEEE Transactions on Computers, vol. C-22, no. 3, pp. 307-315, March 1973.

[5] V.A. Krasnobayev, A.S. Yanko, S.A. Koshman. “A Method for arithmetic comparison of data represented in a residue number system” Cybernetics and Systems Analysis, vol. 52, issue 1, pp. 145-150, January 2016.

[6] G. Harman and I. E. Shparlinski, "Products of Small Integers in Residue Classes and Additive Properties of Fermat Quotients," in International Mathematics Research Notices, vol. 2016, no. 5, pp. 1424-1446, Jan. 2016.

[7] V. Krasnobayev, A. Kuznetsov, M. Zub, K. Kuznetsova. Methods for comparing numbers in non-positional notation of residual classes. In Proceedings of the Second International Workshop on Computer Modeling and Intelligent Systems (CMIS-2019), Zaporizhzhia, Ukraine, April 15-19, 2019., pp. 581–595. 2019.

[8] D. I. Popov and A. V. Gapochkin, "Development of Algorithm for Control and Correction of Errors of Digital Signals, Represented in System of Residual Classes," 2018 International Russian Automation Conference (RusAutoCon), Sochi, 2018, pp. 1-3.

[9] Yu.V. Stasev, A.A. Kuznetsov, A.M. Nosik. “Formation of pseudorandom sequences with improved autocorrelation properties.” Cybernetics and Systems Analysis, vol. 43, Issue 1, pp. 1-11, January 2007.

[10] A. Kuznetsov, A. Kiian, K. Kuznetsova, et al. Soft decoding based on ordered subsets of verification equations of turbo-productive codes. In Proceedings of the Second International Workshop on Computer Modeling and Intelligent Systems (CMIS-2019), Zaporizhzhia, Ukraine, April 15-19, 2019., pp. 873–884. 2019

[11] A. A. Kuznetsov, I. P. Kolovanova, D. I. Prokopovych-Tkachenko, T. Y. Kuznetsova. “Analysis and Studying of the Properties of Algebraic Geometric Codes.” Telecommunications and Radio Engineering, Volume 78, 2019, Issue 5, pp. 393-417.

[12] B. Wang and L. Liu, "A flexible and energy-efficient reconfigurable architecture for symmetric cipher processing," 2015 IEEE International Symposium on Circuits and Systems (ISCAS), Lisbon, 2015, pp. 1182-1185.

[13] A. Kuznetsov, Y. Gorbenko, A. Andrushkevych and I. Belozersev, "Analysis of block symmetric algorithms from international standard of lightweight cryptography ISO/IEC 29192-2," 2017 4th International Scientific-Practical Conference Problems of Infocommunications. Science and Technology (PIC S&T), Kharkov, 2017, pp. 203-206.

[14] I. Gorbenko, A. Kuznetsov, M. Lutsenko and D. Ivanenko, "The research of modern stream ciphers," 2017 4th International Scientific-Practical Conference Problems of Infocommunications. Science and Technology (PIC S&T), Kharkov, 2017, pp. 207-210.

[15] M. E. Pamukov, V. Poulkov, A. Mihovska, N. R. Prasad and R. Prasad, "Lightweight robust cryptographic combiner for mobile devices: Crypto roulette," 2014 IEEE 19th International Workshop on Computer Aided Modeling and Design of Communication Links and Networks (CAMAD), Athens, 2014, pp. 188-192.

[16] A. Kuznetsov, I. Kolovanova and T. Kuznetsova, "Periodic characteristics of output feedback encryption mode," 2017 4th International Scientific-Practical Conference Problems of Infocommunications. Science and Technology (PIC S&T), Kharkov, 2017, pp. 193-198.

[17] Z. Dai, X. Yu, J. Su and X. Chen, "Accelerated Flexible Processor Architecture for Crypto Information," 2007 2nd International Conference on Pervasive Computing and Applications, Birmingham, 2007, pp. 399-403.

[18] I. Gorbenko, O. Kuznetsov, Y. Gorbenko, A. Alekseychuk and V. Tymchenko, "Strumok keystream generator," 2018 IEEE 9th International Conference on Dependable Systems, Services and Technologies (DESSERT), Kyiv, Ukraine, 2018, pp. 294-299.

[19] Runovski, K., & Schmeisser, H. (2004). On the convergence of fourier means and interpolation means. Journal of Computational Analysis and Applications, 6(3), 211-227.

[20] Gnatyuk, V. A. (2001). Mechanism of laser damage of transparent semiconductors. Physica B: Condensed Matter, 308-310, 935-938.

[21] Tkach, B. P., & Urmancheva, L. B. (2009). Numerical-analytic method for finding solutions of systems with distributed parameters and integral condition. Nonlinear Oscillations, 12(1), 113-122.

[22] Chornei, R., Hans Daduna, V. M., & Knopov, P. (2005). Controlled markov fields with finite state space on graphs. Stochastic Models, 21(4), 847-874.

[23] Y. N. Kocherov, D. V. Samoylenko and A. I. Koldaev, "Development of an Antinoise Method of Data Sharing Based on the Application of a Two-Step-Up System of Residual Classes," 2018 International Multi-Conference on Industrial Engineering and Modern Technologies (FarEastCon), Vladivostok, 2018, pp. 1-5.

[24] C. Fan and G. Ge, "A Unified Approach to Whiteman's and Ding-Helleseth's Generalized Cyclotomy Over Residue Class Rings," in IEEE Transactions on Information Theory, vol. 60, no. 2, pp. 1326-1336, Feb. 2014.

[25] M. Kasianchuk, I. Yakymenko, I. Pazdriy, A. Melnyk and S. Ivasiev, "Rabin's modified method of encryption using various forms of system of residual classes," 2017 14th International Conference The Experience of Designing and Application of CAD Systems in Microelectronics (CADSM), Lviv, 2017, pp. 222-224.

[26] V.A. Krasnobayev, S.A. Koshman, M.A. Mavrina. "A Method for Increasing the Reliability of Verification of Data Represented in a Residue Number System" Cybernetics and Systems Analysis, , vol. 50, issue 6, pp. 969–976, November 2014.

[27] K. Tao, L. Peng, K. Liang and B. Zhuo, "Irregular repeat accumulate low-density parity-check codes based on residue class pair," 2017 IEEE 9th International Conference on Communication Software and Networks (ICCSN), Guangzhou, 2017, pp. 127-131.

[28] V. Krasnobayev, A. Kuznetsov, A. Kononchenko, T. Kuznetsova. Method of data control in the residue classes. In Proceedings of the Second International Workshop on Computer Modeling and Intelligent Systems (CMIS-2019), Zaporizhzhia, Ukraine, April 15-19, 2019., pp. 241–252. 2019.

[29] V. Krasnobayev, S. Koshman, A. Yanko and A. Martynenko, "Method of Error Control of the Information Presented in the Modular Number System," 2018 International Scientific-Practical Conference Problems of Infocommunications. Science and Technology (PIC S&T), Kharkiv, Ukraine, 2018, pp. 39-42.

[30] Krasnobayev V. A. Method for realization of transformations in public-key cryptography. Telecommunications and Radio Engineering. - Volume 66, 2007 Issue 17, pp. 1559-1572.

Reviewer: Alexandr Kuznetsov, Doctor of Sciences (Engineering), Full Prof., Academician of the Academy of Applied Radioelectronics Sciences, V.N. Karazin Kharkiv National University, Kharkov, Ukraine.
E-mail: kuznetsov@karazin.ua

Received: September 2019.

Authors:

Viktor Krasnobayev, Doctor of Sciences (Engineering), Full Prof., Academician of the Academy of Applied Radioelectronics Sciences, V.N. Karazin Kharkiv National University, Kharkov, Ukraine.
E-mail: v.a.krasnobaev@gmail.com

Mikhail Zub, student, V.N. Karazin Kharkiv National University, Kharkov, Ukraine.
E-mail: mishazub007@gmail.com

Olesya Reshetnyak, student, V.N. Karazin Kharkiv National University, Kharkov, Ukraine.
E-mail: lesyandr13@gmail.com

Andrey Dyachenko, student, V.N. Karazin Kharkiv National University, Kharkov, Ukraine.
E-mail: andrey.090220@gmail.com

Irina Lokotkova, student, V.N. Karazin Kharkiv National University, Kharkov, Ukraine.
E-mail: lokotosyk@ukr.net

Konstantin Myslyvtsev, student, V.N. Karazin Kharkiv National University, Kharkov, Ukraine.
E-mail: kostyavtx@gmail.com

Mathematical model of the process of tabular's implementation of the operation algebraic multiplication in the residues class.

Abstract. Based on the properties of the class of residues in the article, a mathematical model of the process of tabular implementation of modular multiplication was synthesized, for both positive and negative numerical ranges of information processing by means of integer information processing. This model is recommended for practical application in the development of methods and algorithms for rapid processing of cryptographic information. Finding ways to simplify the structure of the table operating device integer information processing has led to the need to improve the mathematical model, methods and algorithms for modular operations, which increase the efficiency of the use of table arithmetic in the class of residues. A feature of the implementation of this model is the possibility of reducing the number of equipment operating device integer information by reducing the (50-70)% of logical ele-

ments "And" in the nodes of the table permanent storage device, directly implement the operation of modular multiplication by arbitrary m_i module residual class. This is possible by using the symmetry properties of the a_ib_i (mod m_i) implementation table of the modular multiplication operation.

Keywords: Residues Class; Tabular's Implementation; Mathematical Model; Operation Algebraic Multiplication.

Рецензент: Александр Кузнецов, д.т.н., проф., академик Академии наук прикладной радиоэлектроники, Харьковский национальный университет им. В.Н. Каразина, Харьков, Украина.
E-mail: kuznetsov@karazin.ua

Поступила: Сентябрь 2019.

Авторы:

Виктор Краснобаев, д.т.н., проф., академик Академии наук прикладной радиоэлектроники, Харьковский национальный университет им. Каразина.
E-mail: v.a.krasnobaev@gmail.com

Михаил Зуб, студент факультета компьютерных наук, Харьковский национальный университет им. Каразина.
E-mail: mishazub007@gmail.com

Олеся Решетняк, студент факультета компьютерных наук, Харьковский национальный университет им. Каразина.
E-mail: lesyandr13@gmail.com

Андрей Дьяченко, студент факультета компьютерных наук, Харьковский национальный университет им. Каразина.
E-mail: andrey.090220@gmail.com

Ирина Локоткова, студентка факультета компьютерных наук, Харьковский национальный университет им. Каразина.
E-mail: lokotosyk@ukr.net

Константин Мисливцев, студент факультета компьютерных наук, Харьковский национальный университет им. Каразина.
E-mail: kostyavtx@gmail.com

Математическая модель процесса табличной реализации операции алгебраического умножения в классе вычетов.

Аннотация. На основании свойств класса вычетов в статье синтезирована математическая модель процесса табличной реализации модульного умножения, как для положительного, так и для отрицательного числовых диапазонов обработки информации средствами обработки целочисленной информации. Данная модель рекомендована к практическому применению при разработке методов и алгоритмов быстрой обработки криптографической информации. Поиск путей упрощения структуры табличного операционного устройства средства обработки целочисленной информации обусловил необходимость совершенствования математической модели, методов и алгоритмов реализации модульных операций, позволяющих повысить эффективность применения табличной арифметики в классе остатков. Особенностью реализации данной модели является возможность уменьшения количества оборудования операционного устройства средства обработки целочисленной информации за счет сокращения на (50-70)% логических элементов "И" в узлах таблицы постоянное запоминающее устройство, непосредственно реализующие операцию модульного умножения по произвольному m_i модулю класса остатков. Это возможно за счет использования свойств симметрии таблицы реализации a_ib_i (mod m_i) модульной операции умножения.

Ключевые слова: класс вычетов; табличная реализация; математическая модель; операция алгебрическое умножение.