УДК 004.722

Краснобаєв В.А., доктор технічних наук, професор,
Нечипоренко Б.В., студент групи 601-ТСм
Полтавський національний технічний університет
імені Юрія Кондратюка

ПІДВИЩЕННЯ ПРОДУКТИВНОСТІ ПРОЦЕСОРА ОБРОБКИ КРИПТОГРАФІЧНОЇ ІНФОРМАЦІЇ В МОДУЛЯРНІЙ СИСТЕМІ ЧИСЛЕННЯ НА ОСНОВІ ЗАСТОСУВАННЯ ПРИНЦИПУ КІЛЬЦЕВОГО ЗСУВУ

В статті розглянуто процес обробки інформації у системі залишкових класів (СЗК) модульної системи числення (МСЧ). Проведено дослідження впливу основних властивостей СЗК на архітектуру та принципи функціонування спеціалізованого СОКІ. Розроблено структуру та математичну модель надійності спецпроцесору обробки криптографічної інформації (СОКІ) у СЗК. Пропонується аналіз продуктивності та надійності СОКІ у МСЧ.

Ключові слова: *система залишкових класів, модульна система числення, спеціалізований обчислювальний пристрій, криптографічна система, електронно-обчислювальна машина, система числення, спецпроцесор обробки криптографічної інформації.*

Вступ

В даний час криптографічні методи знайшли широке вживання не лише для захисту інформації від несанкціонованого доступу, але і як основа багатьох нових електронних інформаційних технологій – електронний документообіг, електронні гроші, таємне електронне голосування і ін. Сучасна криптографія вирішує наступні три основні проблеми: забезпечення конфіденційності (секретності); забезпечення аутентифікації інформації і джерела повідомлень; забезпечення анонімності (наприклад, приховування переміщення електронних

грошей від одного суб'єкта до іншого).

Перша проблема відома, останні ж дві є відносно новими, і з їх рішенням пов'язаний ряд перспективних напрямів теоретичній і практичній криптографії.

Розробка швидкісних блокових шифрів є важливим завданням прикладної криптографії, В цьому напрямку існує велика кількість пропозицій з боку російських і зарубіжних криптографів. Характерним для більшості нових швидкісних шифрів є використання передобчислювань, що здійснюють розширення секретного ключа. При створенні програмних шифрів вживання складних алгоритмів передобчислювань з метою спрощення шифруючих перетворень в багатьох застосуваннях є виправданим. В даний час криптографічні методи знайшли широке вживання не лише для захисту інформації від несанкціонованого доступу, але і як основа багатьох нових електронних інформаційних технологій – електронний документообіг, електронні гроші, таємне електронне голосування і інші.

Дослідження впливу основних властивостей СЗК на архітектуру та принципи функціонування спеціалізованого СОКІ

Основні властивості системи залишкових класів:

1) незалежність залишків;

2) рівноправність залишків;

3) малорозрядність залишків.

Розглянемо як ці властивості впливають на структуру та принцип функціювання спеціалізованого обчислюваного пристрою.

1) Незалежність залишків дає можливість побудови ЕОМ у вигляді набору (по числу залишків СЗК) інформаційно незалежних трактів, що працюють паралельно у часі. При такій побудові ЕОМ обчислювана система в СЗК має модульність конструкції, що дозволяє здійснювати ремонт і технічне обслуговування не перериваючи розв’язування задач, і для здійснення профілактичних заходів ЕОМ не потрібен висококваліфікований обслуговуючий персонал. Окрім цього помилки, що виникли у тракті m_i, не “розмножуються” в інші тракти ЕОМ, при цьому байдуже чи мала місце на цій

підставі однократна чи багаторазова, чи навіть пачка помилок довжиною більш m_i–1 двійкових розрядів. Таким чином, помилка, що виникла в довільному тракті m_i ЕОМ у СЗК або збережеться в цьому тракті до кінця обчислень або у процесі подальших обчислень самоусунеться (наприклад, якщо після виникнення збою в залишку a_i проміжний результат стане числом, що має нульову цифру в залишку по m_i). У цьому випадку за допомогою СЗК можна побудувати систему виправлення помилок при введенні мінімальної надлишковості, що використовує динаміку обчислювального процесу, увівши поняття альтернативної сукупності.

Основна ідея визначення помилкового залишку $a_i = a_i + \Delta a_i$ полягає в тому, що для одержаної в результаті операції послідовності неправильних операндів A_i (i = 1, 2, 3, ..., ρ) у динаміці обчислювального процесу, не перериваючи розв'язання задачі, послідовно визначаються умовні альтернативні сукупності $W(A) = W_{i-1}(A) \Lambda W_i(A)$. За визначений час умовна альтернативна сукупність стягається до помилкового залишку (або двох залишків m_i і m_n). Після цього відомими методами проводиться корекція спотвореного залишку a_i. Відмінною рисою даного методу корекції помилок є можливість виправляти помилки без зупинки обчислень, що можливо для ЕОМ, які функціонують в реальному часі.

2) Рівноправність залишків. Будь-який залишок a_i числа $A_к$ у СЗК несе інформацію про все вихідне число, що дає можливість чисто програмними методами замінити спотворений тракт по модулю m_i на справний (контрольний) тракт по модулю m_i ($m_i < m_i$), не перериваючи розв'язання задачі. Окрім того, ЕОМ в СЗК з двома контрольними основами зберігає свою працездатність при відмові будь-яких двох обчислювальних трактів. При виникненні третьої чи навіть четвертої відмови, ЕОМ все ще може виконувати програму при деякому зменшенні точності чи швидкості обчислень, тобто ЕОМ в СЗК є винятково "живучою", наближаючись в цьому плані до живих організмів. Відзначимо, що дана особливість обумовлює одну із самих чудових властивостей СЗК: та сама ЕОМ може мати різну надійність при розв'язанні задач в залежності від вимог, які висуваються до точності, обсягу пам'яті і

швидкодії машини при їх розв’язанні, тобто в процесі розв’язання різних задач на ЕОМ у СЗК можливе здійснення “обмінних” операцій між точністю, швидкодією і надійністю.

3) Малорозрядність залишків дозволяє застосовувати табличні методи реалізації арифметичних операцій. У цьому випадку більшість арифметичних операцій здійснюється за один такт, що різко підвищує швидкодію використання раціональних операцій. Одночасно табличні методи використання арифметичних операцій дозволяють створити на базі матричних схем високонадійні обчислювальні пристрої.

Отже, розглянуті властивості СЗК, при використанні її в СОКІ, дозволяють значно підвищити ефективність функціонування ЕОМ.

Додавання, віднімання і множення в СЗК здійснюється по дуже простому алгоритму: ці операції модульні і здійснюються незалежно по кожному модулю СЗК в межах розрядної сітки (0, М).

Приклад:

Додати два числа А = (0, 01, 000), В = (1, 10, 001).

	$m_1 =$ 2	$m_2 =$ 3	$m_3 =$ 5
A =	0	01	000
+	+	+	+
B =	1	10	001
C =	1	00	001

, де $c = (c_1, c_2, c_3) = (1, 00, 001)$;

$c_1 = (0 + 1) = 1 \pmod 2$;

$c_2 = (01 + 10) = 00 \pmod 3$;

$c_3 = (000 + 001) = 001 \pmod 5$.

Суматор та пристрій для складання і віднімання по модулю СЗК представлений на Рис.1 та Рис.2.

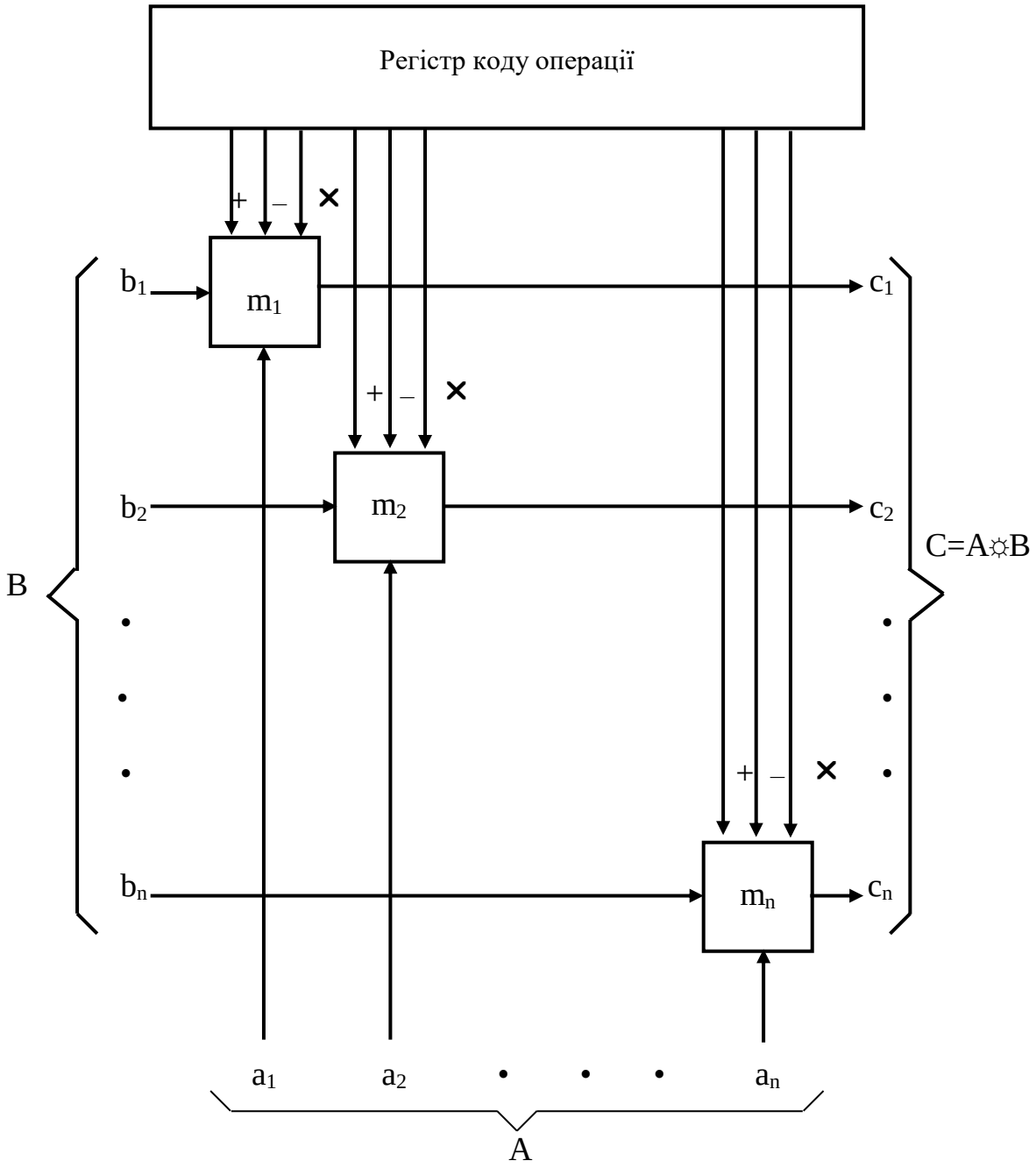

Рис.1. Суматор в системі залишкових класів.

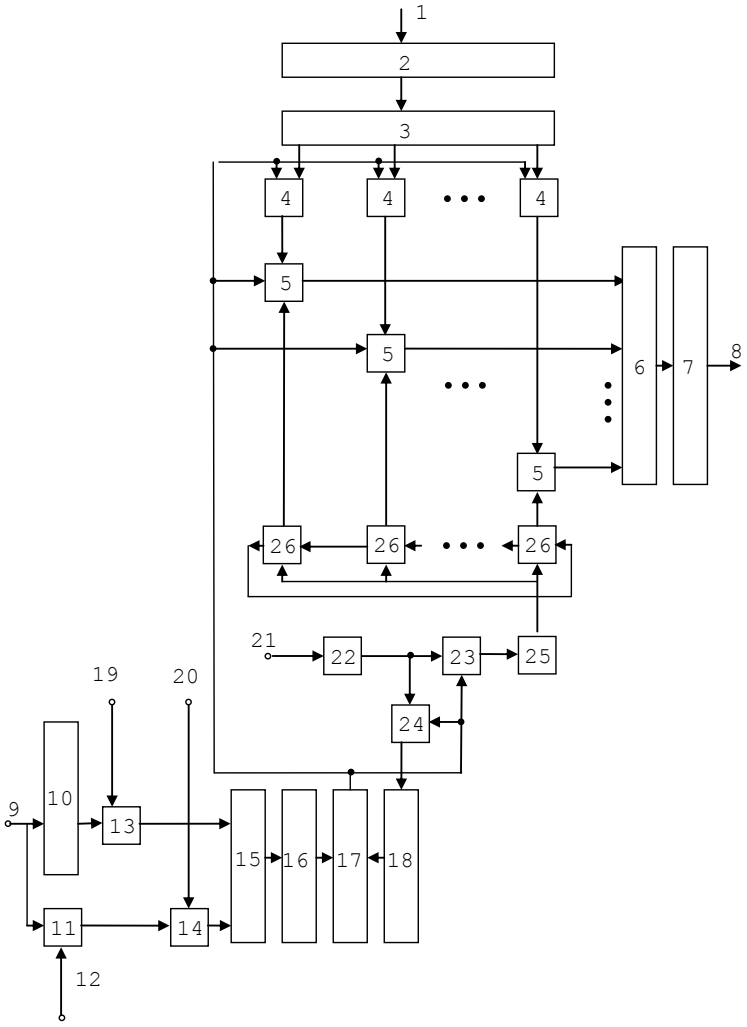

Рис. 2. Пристрій для складання і віднімання по модулю СЗК

Структура та математична модель надійності СОКІ у МСЧ

Синтезуючи структуру СОКІ у системі залишкових класів ймовірність безвідмовної роботи СОКІ у ПСЧ можна визначити як ймовірність безвідмовної роботи ЕОМ у ПСЧ для випадку резервування з навантаженим резервом. В цьому випадку формула для визначення імовірності безвідмовної роботи СОКІ у МСЧ матиме наступний вигляд:

$$P_{C3K}^{(k)}(t) = \sum_{i=0}^{k} C_{k+n}^{i}\, p_1^{k+n-i}(t) \sum_{j=0}^{i} (-1)^j C_i^j\, p_1^j(t). \qquad (1.1)$$

Тут $p_1(t) = e^{-\lambda_1 t}$ – ймовірність безвідмовної роботи тракту ЕОМ по найбільшій (найменш надійній) основі m_{n+k} СЗК, де λ_1 – інтенсивність відмов обладнання тракту ЕОМ у СЗК найбільшій основі m_{n+k}.

Співвідношення (1.1) може бути використане для розрахунку імовірності безвідмовної роботи ЕОМ в СЗК при наступних припущеннях:

– інформаційні і контрольні тракти ЕОМ рівнонадійні, тобто ймовірність безвідмовної роботи всіх трактів ЕОМ приймається рівною імовірності безвідмовної роботи $p_1(t)$ тракту ЕОМ по найбільшій основі СЗК m_{n+k}, що має найменшу ймовірність безвідмовної роботи;

– не враховується можливість відновлення трактів ЕОМ у СЗК, які відмовили.

Реальна надійність ЕОМ у СЗК буде вищою, ніж та, що визначається співвідношенням (1.1), тому що дана формула не враховує можливість заміни одним контрольним трактом по основі m_j одного або одночасно декількох непрацездатних інформаційних трактів за умови:

$$m_j \geq \prod_{i=1}^{r} m_{k_i} , \qquad (1.2)$$

де r – максимальне число трактів, які заміняються одним контрольним працездатним трактом за основою m_j.

Аналіз продуктивності та надійності СОКІ у МСЧ

Проведемо порівняльний аналіз надійності потроєної позиційної ЕОМ з ідеальним мажоритарним елементом ЕОМ у СЗК та ідеальним комутатором по безвідмовності, застосовуючи розглянуту надійну модель. Позначимо через $\lambda_э$ інтенсивність відмов обладнання, віднесену до одного двійкового розряду (до одиниці розрядної сітки СЕОМ). В цьому випадку ймовірність безвідмовної роботи обладнання, віднесена до одного двійкового розряду ЕОМ дорівнює:

$$P_Э(t) = e^{-\lambda_Э t} . \qquad (1.3)$$

Для позиційної *l*-байтової ЕОМ ймовірність безвідмовної роботи дорівнює:

$$P_0(t) = e^{-\lambda_0 t}, \qquad (1.4)$$

де $\lambda_0 = 8\, l\, \lambda_E$.

З врахуванням λ_0 вираз (1.4) набуває наступного вигляду:

$$P_0(t) = e^{-\lambda_E l t}. \qquad (1.5)$$

Відомо, що ймовірність безвідмовної роботи для потроєної мажоритарної структури, яка містить і ідеальний мажоритарний елемент, дорівнює:

$$P_M(t) = 3P_0^2(t) - 2P_0^3(t) = e^{-16\lambda_E t}\left(3 - 2e^{-8\lambda_E t}\right). \qquad (1.6)$$

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

$$p_1(t) = e^{-\lambda_1 t}; \qquad (1.7)$$

Ймовірність безвідмовної роботи ЕОМ у СЗК визначається відповідно до виразу (1.1).

Позначимо $\lambda^* = 8\lambda_e$. При цьому вирази (1.6) і (1.7) можна записати наступним чином:

$$P_M(t) = e^{-2\lambda^* t}(3 - 2e^{-\lambda^* t}); \qquad (1.8)$$

$$P_{СЗК}^{(1)}(t) = e^{-2\lambda^* t}\left(5 - 4e^{-0.5\lambda^* t}\right). \qquad (1.9)$$

Відповідно до виразів (1.8) і (1.9) розраховуються значення імовірності безвідмовної роботи для потроєної позиційної ЕОМ і для ЕОМ у СЗК. На рисунку представлено графіки залежностей $P(\lambda^* t)$ для однобайтових ЕОМ: нерезервованої (I), триканальної резервованої ЕОМ у ПСЧ (II) і ЕОМ у СЗК з параметрами $l = 1$, $n = 4$, $k = 1$ (III). Видно, що ЕОМ у СЗК з однією контрольною основою (III) більш надійніша потроєної позиційної обчислювальної системи (II). При цьому критичне значення імовірності безвідмовної роботи ЕОМ в класі залишків дорівнює 0,425, а критичне

значення потроєної обчислювальної системи дорівнює 0,5, тобто розширюється область значень λ^*t, при яких збільшується (в порівнянні з нерезервованою позиційною ЕОМ (I)) безвідмовність роботи непозиційної ЕОМ.

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

Для даного набору основ за виразом (1.1) отримаємо:

$$P_{СЗК}^{(2)}(t) = P_1^4(t)\left\{ P_1^2(t) + 6P_1(t)\left[1 - P_1(t)\right] + 15\left[1 - P_1(t)\right]^2 \right\}; \quad (1.10)$$

Висновки

Отже, СЗК при меншій додатково введеній кількості обладнання забезпечує не меншу надійність, чим потроєна або дубльована структура, що дуже важливо при побудові спеціалізованих ЕОМ, які функціонують в реальному масштабі часу.

Результати статті можуть бути використані при створенні модульної системи криптографічного захисту.

Література:

1. *Изотов Б. В., Молдовян А. А., Молдовян Н. А. Скоростные методы защиты информации в АСУ на базе управляемых операций // Автоматика и телемеханика. — 2001. — № 6. — С. 168—184 с.*

2. *Карякин Ю. Д. Технология «AXIS-2000» защиты материальных объектов от подделки // Управление защитой информации. — Минск. — 1997. — Т. 1. — № 2. — С. 90—98.*

3. *Кострикин А. И. Введение в алгебру. Основы алгебры: Учебник для вузов. — М.: Физматлит, 1994. — 320 с.*

4. *Крамер Г. Математические методы статистики. — М.: Мир, 1975. — 648 с.*

5. *Молдовян А. А., Молдовян Н. А. Вероятностные механизмы в недетерминированных блочных шифрах // Безопасность информационных технологий. — 1997. — №3. — С. 58—61 с.*

6. *Молдовян А. А., Молдовян Н. А. Метод скоростного преобразования для защиты информации в АСУ // Автоматика и телемеханика. — 2000. — №4. —С. 151—165 с.*

7. *Молдовян А. А., Молдовян Н. А., Молдовяну П. А. Новый метод*

криптографических преобразований для современных систем защиты ПЭВМ // Управляющие системы и машины. — Киев. — 1992. — № 9/10. — С. 44—50 с.

8. Молдовян А. А., Молдовян Н. А. Псевдовероятностные скоростные блочные шифры для программной реализации. Кибернетика и системный анализ.— Киев.—1997. — №4. —С. 133—141 с.

9. Молдовян А. А., Молдовян Н. А. Скоростные шифры на базе нового криптографического примитива// Безопасность информационных технологий. — 1999. — №1. —С. 82—88 с.