МІНІСТЕРСТВО ОСВІТИ І НАУКИ, МОЛОДІ ТА СПОРТУ УКРАЇНИ
ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ РАДІОЕЛЕКТРОНІКИ

МАРТИНЕНКО СЕРГІЙ ОЛЕГОВИЧ

УДК 681.142:004.056

МЕТОД І ЗАСОБИ ЗНИЖЕННЯ ОБЧИСЛЮВАЛЬНОЇ СКЛАДНОСТІ КРИПТОГРАФІЧНИХ RSA–ПЕРЕТВОРЕНЬ НА ОСНОВІ МОДУЛЯРНОЇ СИСТЕМИ ЧИСЛЕННЯ

05.13.05 – комп’ютерні системи та компоненти

АВТОРЕФЕРАТ
дисертації на здобуття наукового ступеня
кандидата технічних наук

Харків – 2012

Дисертацією є рукопис.

Роботу виконано у Харківському національному технічному університеті сільського господарства імені Петра Василенка, Міністерство освіти і науки, молоді та спорту України.

Науковий керівник: доктор технічних наук, професор
Краснобаєв Віктор Анатолійович,
Харківський національний технічний університет сільського господарства імені Петра Василенка, професор кафедри автоматизації та комп'ютерно-інтегрованих технологій.

Офіційні опоненти: доктор технічних наук, професор
Кривуля Геннадій Федорович,
Харківський національний університет радіоелектроніки, завідувач кафедри автоматизації проектування обчислювальної техніки;

доктор технічних наук, професор
Кузнецов Олександр Олександрович, Харківський університет Повітряних Сил ім. І. Кожедуба, начальник кафедри бойового застосування та експлуатації АСУ.

Захист відбудеться "___" _____ 2012 року. о ___ годині на засіданні спеціалізованої вченої ради Д64.052.01 у Харківському національному університеті радіоелектроніки за адресою: 61166, м. Харків, просп. Леніна, 14.

З дисертацією можна ознайомитися у бібліотеці Харківського національного університету радіоелектроніки за адресою: 61166, м. Харків, просп. Леніна, 14.

Автореферат розісланий "___"_____ 2012 р.

Вчений секретар спеціалізованої вченої ради _____ Є.І. Литвинова

ЗАГАЛЬНА ХАРАКТЕРИСТИКА РОБОТИ

Характерним для сучасного технологічного застосування криптографічних технічних засобів (embedded processor, processor node) реалізації криптографічних перетворень (КП) є істотне зростання вимог щодо швидкості обробки КП і надійності (відмовостійкості) їх функціонування.

Під обчислювально-складними задачами КП розуміють задачі, що заздалегідь мають розв'язки, але для його знаходження необхідно проведення надзвичайно великої кількості операцій обчислювача (універсальних ЕОМ або спецпроцесора обробки криптографічної інформації (СОКІ)).

Існують два принципові шляхи зниження обчислювальної складності реалізації криптографічного алгоритму: часткове скорочення кількості операцій і зменшення часу реалізації кожної операції. Перший шлях припускає зміну (модифікацію) алгоритму, це дуже трудомісткий процес і навряд чи це доцільно і взагалі можливо. Другий шлях – базується на зменшенні (зниженні) часу виконання модульних операцій в криптоалгоритмі, які в сучасних СОКІ реалізуються в звичайній двійковій позиційній системі числення (ПСЧ).

У даній дисертаційній роботі вирішується науково-технічна задача зниження обчислювальної складності RSA криптоперетворень шляхом зменшення часу реалізації арифметичних операцій.

Пошуки шляхів зниження обчислювальної складності КП (підвищення продуктивності обробки криптографічної інформації) без зниження відмовостійкості СОКІ реального часу показали, що в межах ПСЧ цього досягти практично неможливо. Дослідження в цьому напрямі відомих авторів (Валах М., Свобода А., Сабо Н., Акушський І.Я., Юдицкий Д.І., Глушков В.М., Долгов О.І., Торгашев В.А., Морозов В.Н., Фінько О.А., Синьков М.В., Амербаєв В.М., Євстигнеєв В.Г., Інютін С.А., Коляда А.А., Пак І.Т., Черв'яков М.І., Вишинський В.А., Овчаренко Л.А., Лебедєв Е.К., Краснобаєв В.А., Blum T., Paar C., Kawamura S., Ko Ae M., Sano F., Shimbo A., Paulier P., Thornton M.A., Dreschler R., Miller D.M.) і багатьох інших вчених показали, що використання як системи числення непозиційної модулярної системи числення (МСЧ), може вирішити науково-технічну задачу зниження обчислювальної складності криптосистеми без зниження відмовостійкості функціонування СОКІ реального часу.

Таким чином, недоліки сучасних СОКІ, обумовлені використанням двійкової ПСЧ, а також вимоги щодо суттєвого підвищення продуктивності обробки криптографічних алгоритмів (КА) системами обробки інформації реального часу, і отримані попередні позитивні результати використання МСЧ для підвищення продуктивності та відмовостійкості спецпроцесора обробки інформації реального часу визначили тему, загальну науково-технічну задачу, мету і частинні задачі даної дисертаційної роботи.

Науково-технічна задача – розробка методів підвищення швидкодії реалізації RSA криптоперетворень на основі використання модулярної системи числення.

Зв'язок роботи з науковими програмами, планами і темами. Дослідження, результати яких викладені в дисертації, проводилися відповідно до державних планів НДР, програм і договорів, які виконувалися у Харківському національному університеті радіоелектроніки, Національному аерокосмічному університеті ім. Н.Е. Жуковського (ХАІ) і Харківському національному технічному університеті сільського господарства ім. Петра Василенка на кафедрі автоматизації та комп'ютерно-інтегрованих технологій:

– «Дослідження та розробка високоефективних мікроелектронних обчислювальних і керуючих пристроїв з нетрадиційною архітектурою» (Харківський національний технічний університет сільського господарства ім. Петра Василенка, (ДР № 0104U005149, 2004-2006 г.);

– «Розробка та дослідження надшвидкодіючих і надійних систем і засобів обробки цифрової інформації на основі використання непозиційних кодових структур модулярної арифметики» (Харківський національний технічний університет сільського господарства імені Петра Василенка (ДР № 0107U001631, 2007-2010 р.).

Участь автора у зазначених науково-дослідних темах і проектах, в яких дисертант був безпосереднім виконавцем, полягає в розробці безпосередньо методу і засобів зниження обчислювальної складності RSA криптосистеми на основі використання МСЧ.

Мета дослідження – розробка моделей та методів зниження обчислювальної складності RSA криптоперетворень за рахунок використання адитивно-мультиплікативних властивостей полів Галуа .

Для досягнення поставленої мети необхідно вирішити такі завдання:

– провести дослідження особливостей структури та процесу функціонування існуючих обчислювальних систем обробки криптографічної інформації та проаналізувати методи зниження обчислювальної складності RSA криптосистем;

– розробити метод зниження обчислювальної складності криптографічних RSA перетворень;

– розробити математичну модель безвідмовності спецпроцесора обробки криптографічної інформації;

– розробити метод швидкої реалізації арифметичних операцій в полях Галуа;

– розробити технічні засоби обробки криптографічної інформації.

Об'єкт дослідження – процес обробки криптографічної інформації в модулярній системі числення.

Предмет дослідження – методи і засоби зниження обчислювальної складності криптографічних RSA - перетворень на основі модулярної системи числення з використанням принципу кільцевого зрушення.

Методи дослідження – аналіз і синтез, теорія чисел – під час розробки методів і засобів реалізації арифметичних операцій в полях Галуа на основі застосування модулярної системи числення шляхом використання принципу кільцевого зрушення, а також під час розробки методу вибору основ МСЧ; теорія ймовірностей і теорія надійності – під час дослідження методів підвищення безвідмовності спецпроцесора обробки криптографічної інформації, що функціонує в модулярній системі числення.

Наукова новизна отриманих результатів:

1. Вперше запропоновано метод обробки криптоперетворень RSA, який характеризується використанням принципу кінцевого зрушення та базується на застосуванні модулярної системи числення, що дозволяє зменшити обчислювальну складність RSA криптографічних перетворень.

2. Удосконалено математичну модель безвідмовності спецпроцесора обробки криптографічної інформації, яка відрізняється урахуванням надійності контрольних трактів, що дає можливість оцінити надійність спецпроцессора обробки криптографічної інформації.

3. Удосконалено метод виконання цілочисельних арифметичних операцій в модулярній системі числення, який на відміну від аналогів ураховує адитивно-мультиплікативні властивості полів Галуа, що дозволяє підвищити швидкодію спецпроцессора обробки криптографичної інформації.

Практичне значення отриманих результатів:

1. Розроблений в дисертаційній роботі метод зниження обчислювальної складності RSA криптоперетворень доведено до практичної реалізації у системах криптографічного захисту інформації, що дозволило знизити обчислювальну складність до 40%.

2. Удосконалені методи виконання арифметичних операцій в модулярній системі числення завдяки їх реалізації на основі застосування кільцевого зрушення є науково-методичною основою для практичного створення сучасних СОКІ. Застосування розроблених методів дозволило підвищити ефективність модулярної системи числення у 2–6 разів у залежності від типу операцій, що реалізуються в RSA-криптоалгоритмах.

3. Оцінка обчислювальної складності КА RSA, результати розрахунків і порівняльного аналізу продуктивності й надійності, виконані в дисертаційній роботі, показали, що зі збільшенням числового діапазону обробки інформації, що характерно для сучасної тенденції розвитку СОКІ, ефективність застосування МСЧ зростає в 1,5–2 рази.

4. На основі розроблених у дисертації методів синтезовано алгоритми обробки інформації, на основі яких запропоновано клас технічних засобів на які отримано патенти України.

Результати дисертаційної роботи впроваджено: у ЗАТ «Інститут інформаційних технологій» при виконанні НДР № 237-1 (прикладна), №ДР 0109U002573, м. Харків (акт від 22.04.2010 р.), а також у ДП ХПЗ ім. Т. Г. Шевченка, м. Харків (акт від 28.01.2010 р.)

Особистий внесок здобувача Усі основні наукові і практичні результати дисертації отримано особисто автором. У роботах, опублікованих у співавторстві, здобувачеві належать: [1] – метод виконання арифметичних операцій в модулярній системі числення на основі застосування принципу кільцевого зрушення, шляхом урахування властивостей полів Галуа; [2] – концепція зниження обчислювальної складності реалізації криптоперетворень на основі використання МСЧ; [3] – метод піднесення чисел до квадрата за модулем модулярної системи числення; [4] – метод виявлення помилок у спецпроцесорі обробки криптографічної інформації; [5] – математична модель безвідмовності спецпроцесора обробки крип-

тографічної інформації в модулярній системі числення, [6] – метод обробки криптоперетворень RSA, що базується на застосуванні модулярної системи числення; [7] – метод обробки криптографічної інформації в МСЧ; [8] – метод виконання арифметичних операцій в модулярній системи числення на основі застосування принципу кільцевого зрушення шляхом урахування властивостей полів Галуа; [9] – метод контролю інформації у МСЧ; [10] – алгоритм для виявлення помилок інформації у МСЧ; [11] – алгоритм для виявлення і виправлення помилок інформації у МСЧ; [12] – блок для поєднання одночасного виконання операцій додавання та віднімання чисел за модулем m_i; [13] – модель процесу додавання чисел за модулем m_i МСЧ; [14] – блок контролю помилок; [15] – алгоритм для піднесення чисел до квадрата за модулем m_i МСЧ; [16] – синтез архітектури комп'ютерної системи обробки криптографічної інформації на основі МСЧ; [17] – оптимізація структури системи обробки криптографічної інформації в модулярній системі числення; [18] – методи реалізації криптографічних RSA перетворень на основі використання МСЧ; [19] – метод зниження обчислювальної складності алгоритму обробки цифрової інформації на основі використання МСЧ.

Апробація результатів дисертації. Результати наукових досліджень докладалися, обговорювалися і були схвалені на 4 міжнародних науково-технічних семінарах, науково-технічних конференціях і симпозіумах: "Інтегровані комп’ютерні технології в машинобудуванні ІКТМ–2009", м. Харків, НАУ ХАІ, 2009р.; "Проблемы информатики и моделирования", м. Харків, НТУ ХПІ, 2009р.; "Компьютерное моделирование в наукоемких технологиях", м. Харків, НУ ім. Каразіна, 2010р.; "Перспективные компьютерные управляющие и телекоммуникационные системы для железнодорожного транспорта Украины", 23–я міжнародна науково-практична конференція, 23–29 вересня 2010, Алушта, Україна.

Публікації. Основні результати дисертації опубліковані в 19 друкованих працях, серед яких 4 статті в наукових журналах, 4 статті в збірках наукових праць, які входять до переліку наукових фахових видань України, 7 патентів України, а також 4 тези доповідей в збірниках науково-технічних міжнародних конференцій.

У додатку наведено акти реалізації дисертаційних досліджень (додаток А), а також результати розрахунку констант нулевізації в МСЧ (додаток Б).

Структура та обсяг дисертації. Дисертація складається із вступу, чотирьох розділів, висновків, списку використованої літератури і двох додатків. Повний обсяг дисертації складає 207 сторінок, 146 сторінок основного тексту, зокрема: рисунків на 12 окремих сторінках, таблиць на 7 окремих сторінках, бібліографія з 120 найменуваннями на 14 сторінках, 2 додатки на 28 сторінках.

ОСНОВНІЙ ЗМІСТ РОБОТИ

Вступ дисертаційної роботи містить: обґрунтування актуальності теми дослідження; інформацію про зв’язок дисертаційної роботи з науковими програмами; мету роботи та частинні задачі досліджень; формулювання об’єкта, предмета і методів дослідження; характеристику наукової новизни та практичної значущості

одержаних результатів досліджень, а також особистого внеску здобувача. Наведено дані щодо реалізації, апробації та публікації наукових і практичних результатів дисертації.

У першому розділі досліджено структуру, зміст, концепцію та тенденції розвитку і реалізації криптографічних RSA перетворень. Було проведено узагальнення даних про обчислювальну складність існуючих КП. Проаналізовано види арифметичних перетворень і типи арифметичних й інших операцій, що входять у криптографічні алгоритми.

Таблиця 1

Складність і час реалізації криптоалгоритмів

Розмір поля (біт)	Порядок криптосистеми (біт)	Складність $Q\sqrt{n}$	Час реалізації [MIPS-роки]
163	160	2^{80}	$9{,}6\ 10^{11}$
191	186	2^{93}	$7{,}9\ 10^{15}$
239	234	2^{117}	$1{,}6\ 10^{23}$
359	354	2^{177}	$1{,}5\ 10^{41}$
431	426	2^{233}	10^{52}

Проаналізовано види арифметичних перетворень і типи арифметичних і інших операцій (рис. 1), що входять в криптографічні алгоритми.

Рис. 1. Арифметичні перетворення в кінцевих полях Галуа

Результати проведених досліджень щодо вимог реалізації сучасних і перспективних задач і алгоритмів КП показали, що одним з головних завдань сучасної криптографії є зниження їх обчислювальної складності. Шлях вирішення даної задачі неможливий без використання продуктивних обчислювальних апаратних засобів обробки криптографічної інформації реального часу. Проведені в дисертації дослідження існуючих і можливих перспективних методів зниження обчислювальної складності КП показали наступне. По-перше, в звичайних двійкових ПСЧ не завжди можна отримати істотні позитивні результати у цьому напрямі без

погіршення деяких характеристик і показників СОКІ. По-друге, попередні результати досліджень впливу властивостей МСЧ на структуру і принципи функціонування спецпроцесора обробки криптографічної інформації показали, що використання непозиційного кодування криптографічної інформації та подальша її обробка дозволили виявити об'єктивні передумови для підвищення продуктивності СОКІ.

У другому розділі вперше розроблено метод обробки криптоперетворень RSA. Показано, що криптографічні перетворення RSA практично складаються з двох основних типів модульних операцій: операції модульного множення і операцій піднесення чисел до квадрата за модулем m простого числа. Реалізація даних операцій і складає основну обчислювальну складність криптографічних перетворень RSA.

У двійкових позиційних системах числення операція додавання двох чисел $A = a_{\rho-1} \cdot 2^{\rho-1} + a_{\rho-2} \cdot 2^{\rho-2}, + \ \cdots \ +, a_1 \cdot 2 + a_0,$ і $B = b_{\rho-1} \cdot 2^{\rho-1} + b_{\rho-2} \cdot 2^{\rho-2}, + \ \cdots \ +, b_1 \cdot 2 + b_0,$ здійснюється за допомогою використання суматора. Під додаванням розуміється процес перетворення слів виду $S = s_{\rho-1} \cdot 2^{\rho-1} + s_{\rho-2} \cdot 2^{\rho-2}, + \ \cdots \ +, s_1 \cdot 2 + s_0$.

Спрощена схема організації процесу додавання двох чисел у ПСЧ наведена на рис. 2. Значення S_{i+1} суми $(i+1)$-го розряду суматора, а також значення цифри C_{i+1} переносу в сусідній старший розряд суматора визначаються співвідношеннями (1) і (2)

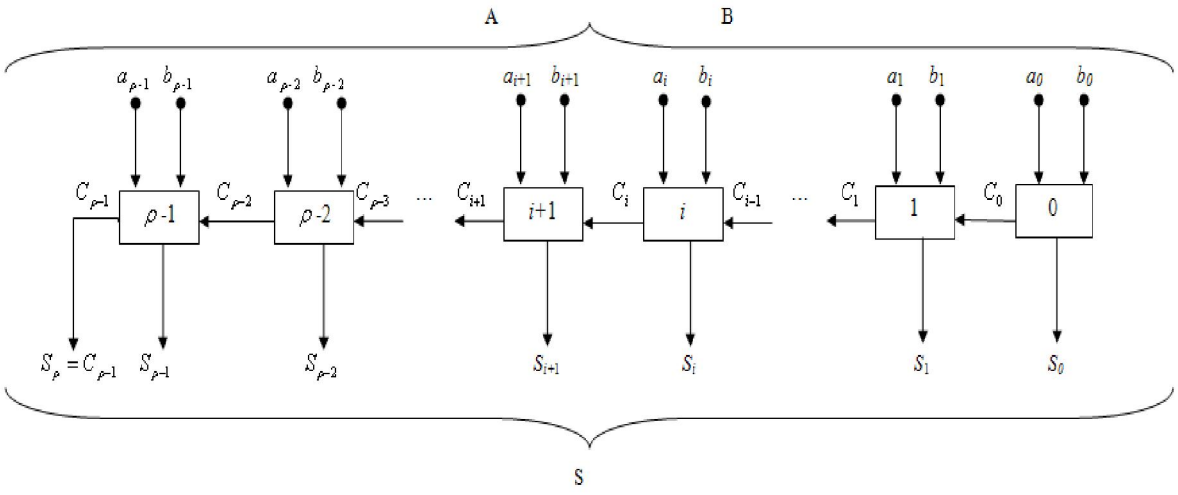
$$\begin{cases} C_{i+1} = a_{i+1} \wedge b_{i+1} \vee \left(a_{i+1} \vee b_{i+1}\right) \wedge c_i; \\ S_{i+1} = \left(a_{i+1} \oplus b_{i+1}\right) \bmod 2 \vee c_i. \end{cases} \quad (1)$$

$$\begin{cases} C_0 = a_0 \wedge b_0; \\ S_0 = \left(a_0 \oplus b_0\right) \bmod 2, \end{cases} \quad (2)$$

де: a_{i+1}, b_{i+1} – значення $(i+1)$-х розрядів чисел, відповідно $A_{ПСЧ}$ і $B_{ПСЧ}$; a_0, b_0 – значення нульових розрядів чисел, відповідно, $A_{ПСЧ}$ і $B_{ПСЧ}$; C_0 – значення сигналу перенесення нульового розряду суматора; S_0 – значення суми нульового розряду $(a_i, b_i, c_i, s_i \in 0,1)$. Аналіз процесу додавання двох чисел у позиційному суматору показав основну складність процесу реалізації арифметичних операцій у ПСЧ – це організація процесу створення та розповсюдження цифр C_i переносу від молодшого розряду суматора до старшого розряду. Наявність міжрозрядних зв’язків суматора у ПСЧ обумовлює такі основні недоліки:

– значна тривалість виконання арифметичних операцій, яка залежить від величини l в розрядній сітці суматора (для отримання кінцевого результату операції доводиться чекати кінця розповсюдження перенесень C_i на всю довжину машинного слова СОКІ);

– помилка, що виникла в одному двійковому розряді суматора, в процесі перенесення від молодших розрядів до старших розповсюджується по всій довжині машинного слова – відмова (перебій) схеми обробки інформації одного двійкового розряду суматора здатна викликати не тільки одноразові, але і багаторазові помилки в отриманому результаті підсумовування.



$$A=\overline{a_{\rho-1}a_{\rho-2}\ldots a_{i+1}a_i\ldots a_1a_0}=a_{\rho-1}\cdot 2^{\rho-1}+a_{\rho-2}\cdot 2^{\rho-2}+\ldots+a_{i+1}\cdot 2^{i+1}+a_i\cdot 2^i+\ldots+a_1\cdot 2+a_0.$$

$$B=\overline{b_{\rho-1}b_{\rho-2}\ldots b_{i+1}b_i\ldots b_1b_0}=b_{\rho-1}\cdot 2^{\rho-1}+b_{\rho-2}\cdot 2^{\rho-2}+\ldots+b_{i+1}\cdot 2^{i+1}+b_i\cdot 2^i+\ldots+b_1\cdot 2+b_0.$$

$$S=\overline{s_{\rho-1}s_{\rho-2}\ldots s_{i+1}s_i\ldots s_1s_0}=s_{\rho-1}\cdot 2^{\rho-1}+s_{\rho-2}\cdot 2^{\rho-2}+\ldots+s_{i+1}\cdot 2^{i+1}+s_i\cdot 2^i+\ldots+s_1\cdot 2+s_0.$$

Рис. 2. Спрощена схема двійкового суматора у ПСЧ

Алгоритм реалізації арифметичної операції додавання у ПСЧ подано виразами (3)

$$\begin{cases} C_{\rho-1}=S_\rho=a_{\rho-1}\wedge b_{\rho-1}\vee\left(a_{\rho-1}\vee b_{\rho-1}\right)\wedge c_{\rho-2}=a_{\rho-1}\wedge b_{\rho-1}\vee\left(a_{\rho-1}\vee b_{\rho-1}\right)\wedge \\ \wedge\left[a_{\rho-2}\wedge b_{\rho-2}\vee(a_{\rho-2}\vee b_{\rho-2})\wedge c_{\rho-3}\right]=\overset{\rho-1}{\underset{i=1}{V}}(a_{\rho-i}\wedge b_{\rho-i}\vee a_{\rho-i}\vee b_{\rho-i})\vee(a_0\wedge b_0). \\ S_{\rho-1}=(a_{\rho-1}+b_{\rho-1})\bmod 2\vee c_{\rho-2}=(a_{\rho-1}+b_{\rho-1})\bmod 2\vee(a_{\rho-2}\wedge b_{\rho-2}\vee a_{\rho-2}\vee b_{\rho-2})\wedge c_{\rho-3}= \\ =(a_{\rho-1}+b_{\rho-1})\bmod 2\vee(a_{\rho-2}\wedge b_{\rho-2}\vee a_{\rho-2}\vee b_{\rho-2})\vee(a_{\rho-3}\wedge b_{\rho-3}\vee a_{\rho-3}\vee b_{\rho-3})\wedge c_{\rho-4}= \\ =(a_{\rho-1}+b_{\rho-1})\bmod 2\vee(a_{\rho-2}\wedge b_{\rho-2}\vee a_{\rho-2}\vee b_{\rho-2})\wedge(a_{\rho-3}\wedge b_{\rho-3}\vee a_{\rho-3}\vee b_{\rho-3})\wedge\ldots\wedge(a_0\wedge b_0)= \\ =(a_{\rho-1}+b_{\rho-1})\bmod 2\cdot\overset{\rho-2}{\underset{i=1}{V}}(a_{\rho-1-i}\wedge b_{\rho-1-i}\vee a_{\rho-1-i}\vee b_{\rho-1-i})\vee(a_0\wedge b_0). \end{cases} \quad (3)$$

На основі результатів досліджень методів і засобів зниження обчислювальної складності RSA КА у розділі було запропоновано шлях, заснований на використанні в СОКІ непозиційної системи числення – МСЧ. У розділі наведено дані про МСЧ, і узагальнено методи технічної реалізації модульних операцій. З метою зниження обчислювальної складності криптографічних перетворень RSA у розділі запропоновано і обґрунтовано метод технічної реалізації криптографічних перетворень (модульних арифметичних операцій) в МСЧ на основі принципу кільцевого зрушення. На рис. 3 наведено метод обробки криптоперетворень RSA.

Сутність розробленого в дисертації методу зниження обчислювальної складності криптографічних RSA перетворень на основі використання МСЧ полягає у реалізації сукупності операцій, дій і прийомів, що направлено на підвищення про-

1. Вибір МСЧ

Виходячи з l довжини машинного слова (розрядної сітки) СОКІ і методу технічної реалізації модульних операцій вибирається сукупність $\{m_i\}$ $(i=\overline{1,n})$ основ (модулей) МСЧ. При цьому необхідно виконання умов:

$$\text{НЗД}\ (m_i, m_j)=1\ \ (i,j=\overline{1,n};\ i\neq j;\ M=\prod_{i=1}^{n} m_i).$$

$$f_{МДКО}=\sum_{i=1}^{m}\left(\{[\log_2(m_i-1)]+1\}\right),\ f_{МУКО}=\sum_{i=1}^{n} m_i .$$

2. Представлення коду МСЧ

$$M_{МСЧ}=\left\{\left(A_{ПСЧ}-\left[A_{ПСЧ}/m_1\right]\bullet m_1\right),\left(A_{ПСЧ}-\left[A_{ПСЧ}/m_2\right]\bullet m_2\right),\ldots,\right.$$
$$\left.\left(A_{ПСЧ}-\left[A_{ПСЧ}/m_i\right]\bullet m_i\right),\ldots,\left(A_{ПСЧ}-\left[A_{ПСЧ}/m_n\right]\bullet m_n\right)\right\},$$

де $a_i\equiv A_{ПСЧ}(\bmod m_i)$

3. Реалізація арифметичних операцій в МСЧ

$$(A\otimes B)\bmod M=(a_1,a_2,\ldots,a_i,\ldots,a_n)\otimes(b_1,b_2,\ldots,b_i,\ldots,b_n)=$$
$$=\left\{(a_1\otimes b_1)\bmod m_1,(a_2\otimes b_2)\bmod m_2,(a_i\otimes b_i)\bmod m_i,\ldots,(a_n\otimes b_n)\bmod m_n\right\}.$$
$$a_i\equiv A_{ПСЧ}(\bmod m_i),\ b_i\equiv B_{ПСЧ}(\bmod m_i).$$

4. Представлення позиційного коду

$$A_{МСЧ}=(a_1,a_2,\ldots,a_i,\ldots,a_n),m_1,m_2,\ldots,m_i,\ldots,m_n .$$

$$\begin{cases}B_1=(1,0,\ldots,0,\ldots,0),\\B_2=(0,1,\ldots,0,\ldots,0),\\\vdots\\B_i=(0,0,\ldots,1,\ldots,0),\\\vdots\\B_n=(0,0,\ldots,0,\ldots,1).\end{cases}\qquad\begin{cases}a_1\equiv A_{ПСЧ}(\bmod m_1),\\a_2\equiv A_{ПСЧ}(\bmod m_2),\\\vdots\\a_i\equiv A_{ПСЧ}(\bmod m_i),\\\vdots\\a_n\equiv A_{ПСЧ}(\bmod m_n).\end{cases}\qquad A_{ПСЧ}=\left(\sum_{i=1}^{n}a_i b_i\right)\bmod M .$$

Рис. 3. Метод обробки криптопертворень RSA

дуктивності реалізації арифметичних модульних операцій: представлення та обробка інформації в СОКІ здійснюється в МСЧ; реалізація арифметичних модульних операцій в СОКІ проводиться на основі запропонованих у дисертації методів обробки інформації, заснованих на принципі кільцевого зрушення; проведення операцій контролю, діагностики та корекції помилок у СОКІ, пропонується здійс-

нювати за рахунок використання інформаційної надмірності вмісту розрядів кільцевих регістрів зрушення; використання удосконаленого в дисертації методу підвищення відмовостійкості СОКІ в МСЧ; використання розроблених у дисертації методів і засобів виконання арифметичних операцій на основі ПКЗ, шляхом урахування властивостей полів Галуа.

У третьому розділі вдосконалено математичну модель безвідмовності спецпроцесора обробки криптографічної інформації. Використовується відома в теорії надійності формула вірогідності безвідмовної роботи для ковзного резервування з ненавантаженим резервом в ПСЧ. Враховуючи, що вірогідність безвідмовної роботи обчислювального тракту СОКІ в МСЧ дорівнює $P_1(t) = e^{-\lambda_1 t}$, вірогідність безвідмовної роботи автомата надійності дорівнює $P_{АН}(t) = e^{-\lambda_A t}$ і частота відмов дорівнює $\lambda_1 e^{-\lambda_1 t}$ отримаємо формулу для визначення вірогідності безвідмовної роботи СОКІ у наступному вигляді

$$P_{МСЧ}^{(k+r)}(t) = e^{-n\lambda_1 t}\sum_{i=1}^{k+r}\left(n\frac{\lambda_1}{\lambda_A}\right)^i - n\frac{\lambda_1}{\lambda_A}e^{-(\lambda_A+n\lambda_1)t}\sum_{i=0}^{k+r-1}\sum_{j=0}^{k+r-1-i}\left(n\frac{\lambda_1}{\lambda_A}\right)^j\frac{(n\lambda_1 t)}{i!}. \qquad (4)$$

Математична модель (ММ) надійності (4) покладена в основу методу підвищення надійності СОКІ в МСЧ. Окрім цього, метод підвищення надійності СОКІ в МСЧ враховує основні властивості модулярної арифметики, що обумовлює урахування наступних видів резервування.

Структурне резервування. Математична модель надійності СОКІ у МСЧ побудована на основі введення вторинної структурної надмірності, застосовуючи структурне резервування. Інформаційні та контрольні обчислювальні тракти СОКІ відіграють роль основних елементів резервованої системи, а резервні обчислювальні тракти - роль резервних елементів.

Інформаційне резервування. Виявляється у використанні додаткової інформації, що вводиться за допомогою використання контрольних обчислювальних трактів СОКІ за основами m_{n+1} і m_{n+2} МСЧ. При виникненні помилок, викликаних перебоями в одному з обчислювальних трактів m_j $(j = \overline{1, n+2})$ СОКІ за однією з робочих або контрольних основами МСЧ, вони усуваються відомими методами.

Функціональне резервування. Цей вид резервування виявляється у випадку, якщо виконується умова $m_j \geq \prod_{i=1}^{r} m_i$,тобто, якщо один обчислювальний тракт СОКІ у МСЧ може одноразово взяти на себе функції r обчислювальних трактів, що відмовили. Це рівноцінно додаванню до k контрольних ще r резервних обчислювальних трактів.

Суть удосконалення запропонованого методу полягає в підвищенні точності оцінки вірогідності безвідмовної роботи СОКІ в МСЧ. Окрім цього, урахування в ММ співвідношення $m_j \geq \prod_{i=1}^{r} m_{k_i}$ дозволяє підвищити безвідмовність функціонування СОКІ за рахунок ефекту додаткового введення до основних (робочих) додатково r резервних обчислювальних трактів.

На рис. 4 і 5 наведено графи функціонування СОКІ в МСЧ відповідно у режимах заміни та деградації.

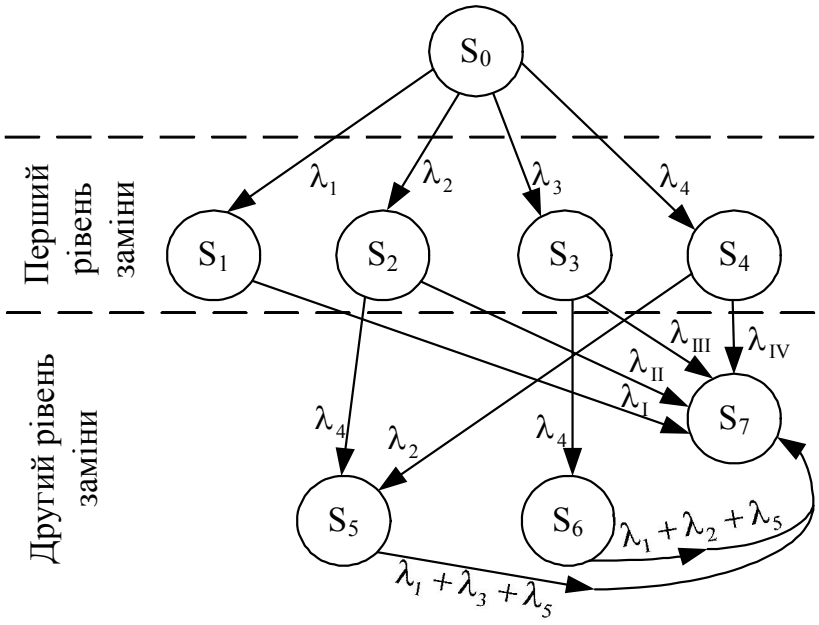


Рис. 4. Граф функціонування СОКІ в режимі заміни

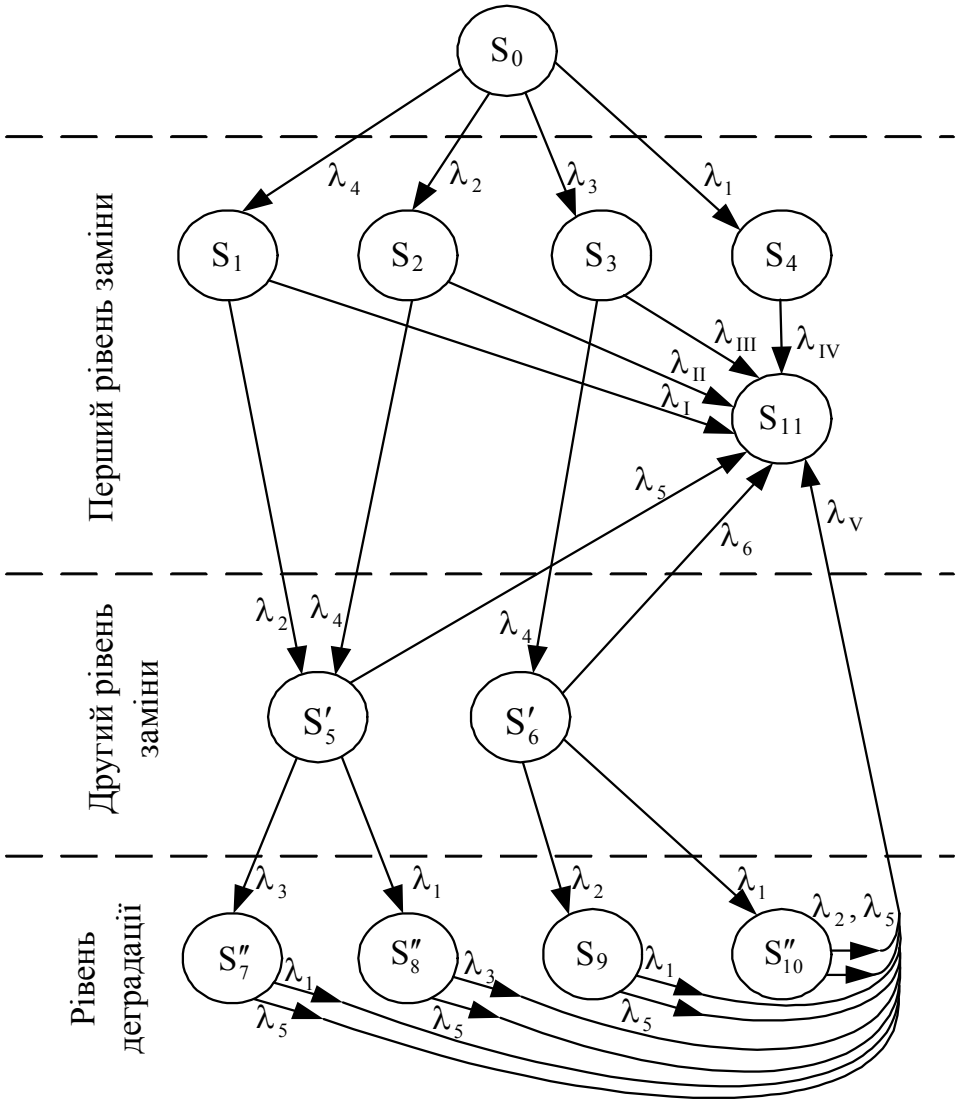


Рис. 5. Граф функціонування СОКІ у режимі деградації

На рис. 6 наведено деякі результати розрахунку і порівняльного аналізу надійності СОКІ в МСЧ і обчислювальних системах обробки криптографічної інформації у двійковій ПСЧ (I). За даними графіків видно, що СОКІ в МСЧ з двома контрольними основами (IV) набагато надійніше тройованої обчислювальної системи в ПСЧ (II) і надійніше СОКІ в МСЧ з однією контрольною основою (III). З графіків видно, що із збільшенням кратності резервування безвідмовність СОКІ в МСЧ підвищується, що відповідає положенням загальної теорії надійності.

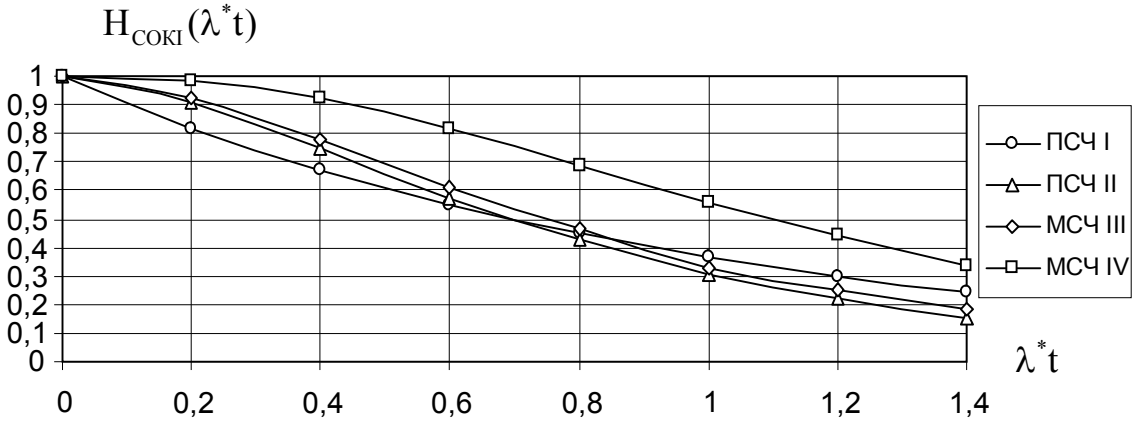


Рис. 6. Графіки залежностей $H^{(k)}_{СОКІ}(\lambda^* t)$

У четвертому розділі вдосконалено метод виконання арифметичних операцій в модулярній системі числення, на основі відомого принципу кільцевого зрушення, відповідно до якого синтезовані алгоритми для його реалізації (5).

$$\begin{aligned}
&(a_i-\beta_i)=\left[a_i+(m_i-b_i)\right]\bmod m_i,\ (a_i+\beta_i)=\left[a_i-(m_i-b_i)\right]\bmod m_i,\\
&a_i+\beta_i=a_i^{'}+\beta_i^{'}=(a_i+m_i/2)+(\beta_i-m_i/2),\\
&\left\{a_i\beta_i(\bmod m_i)+\left[(m_i-a_i)\beta_i\right]\bmod m_i\right\}\bmod m_i\equiv 0(\bmod m_i),\\
&\left[(m_i-a_i)\beta_i\right]\bmod m_i\equiv m_i-a_i\beta_i(\bmod m_i),
\end{aligned}\qquad (5)$$

$a_i\beta_i(\bmod m_i)\equiv m_i-\left[(m_i-a_i)\beta_i\right]\bmod m_i$. У розділі було виведено і доведено ряд аналітичних виразів, що визначають: час додавання двох залишків $(a_i+b_i)\bmod m_i$ у МСЧ (вираз $T^{(+)}_{\substack{мсч\\ m_i}}=K_{1i}\cdot K_{2i}\cdot t_{сов}$, де K_{1i} – значення другого b_i додатка у сумі $(a_i+b_i)\bmod m_i$ (кількість розрядів КРС, на яке в позитивному напрямі зрушується початковий вміст КРЗ), тобто, $K_{1i}=\overline{0,m_i-1}$; K_{2i} – кількість двійкових розрядів в одному розряді КРЗ за модулем m_i, тобто $K_{2i}=\left[\log(m_i-1)\right]+1$; $K_{1i}\cdot K_{2i}$ – кількість одноразово зсунутих двійкових розрядів КРЗ; $t_{зруш}=3\cdot\tau_B$ – час "зрушення" одного двійкового розряду; τ_B – час спрацьовування одного логічного вентиля. В цьому випадку для довільного модуля m_i МСЧ час додавання двох залишків a_i і b_i

можна подати величиною $T^{(+)}_{\substack{мсч \\ m_i}} = 3 \cdot K_{1i} \cdot \{[\log_2(m_i - 1)] + 1\} \cdot \tau_B$). При цьому максимальний $T^{(+)}_{\substack{мсч \\ m_i}}$ час визначення результату операції модульного додавання для довільного модуля m_i МСЧ дорівнює значенню $T^{(+)}_{\substack{мсч \\ m_i \\ \max}} = 3 \cdot (m_i - 1) \cdot \{[\log_2(m_i - 1)] + 1\} \cdot \tau_B$, а максимальний час додавання двох чисел $A = (a_1, a_2, \cdots, a_n)$ і $B = (b_1, b_2, \cdots, b_n)$ дорівнює $T^{(+)}_{\substack{мсч \\ m_n \\ \max}} = 3 \cdot (m_n - 1) \cdot \{[\log_2(m_n - 1)] + 1\} \cdot \tau_B$. У загальному випадку час додавання двох чисел $A = (a_1, a_2, \cdots, a_n)$ и $B = (b_1, b_2, \cdots, b_n)$ у МСЧ за ПКЗ визначається часом $T^{(+)}_{\substack{мсч \\ m_i}}$ реалізації модульної операції $(a_i + b_i) \bmod m_i$ у BT_i, для якого виконується умова $K_{1i} \cdot K_{2i} = \max$,для усіх $BT_j (j = \overline{1, n};\ i \neq j)$.

З метою реалізації однієї з основних операцій RSA КП у розділі розроблено методи визначення значення $a_i^2 (\text{mod m})$, де a_i, m – натуральні числа і $0 \le a_i \le m - 1$. У разі технічної реалізації операції $a_i^2 \pmod m$ у дисертації розглянуто усі три можливі варіанти значення m.

Перший варіант для $m = 2n + 1$ непарного ($n = 0, 1, 2, \ldots$). У цьому випадку в роботі показано наступне математичне співвідношення $a_i^2 (\bmod m) = (m - a_i)^2 \bmod m$. (6). Дійсно, нехай a_i^2 подамо у вигляді $a_i^2 = km + \alpha (0 \le \alpha \le m - 1)$, тобто $a_i^2 \equiv \alpha (\bmod m)$. Тоді $(m - a_i)^2 = m^2 - 2ma_i + a_i^2 = m^2 - 2ma_i + km + \alpha$. В цьому випадку $(m^2 - 2ma_i + km + \alpha) \equiv \alpha (\bmod m)$. Дана рівність справедлива для m парного і непарного.

Другий варіант для $m = 2n$ парного і $m/2$ також парного чисел. У цьому випадку $\frac{m}{2}$ ціле число і, отже $\left(\frac{m}{2}\right)^2 = \frac{m}{4} \cdot m \equiv 0 (\bmod m)$. Отже, алгоритм функціонування пристрою, відповідно до другого варіанту, визначається математичним співвідношенням $\left(\frac{m}{2}\right)^2 = 0 \,(\text{mod } m)$ (7).

Третій варіант для $m = 2n$ парного і $m/2$ непарного чисел. Для даного варіанта виконується умова $\left(\frac{m}{2}\right)^2 \equiv \frac{m}{2} (\bmod m)$ (8). Дійсно, вираз (8) легко подати у вигляді $\frac{m}{2} \cdot \left(\frac{m}{2} - 1\right) = 0 \,(\text{mod } \frac{m}{2} \cdot 2)$ (9). З теорії чисел відомо, що порівнянність $A \equiv B (\bmod m)$ двох чисел A і B за модулем m рівнозначно подільності числа $A - B$ на модуль m. З виразу (9) видно, що число $\frac{m}{2} \cdot \left(\frac{m}{2} - 1\right)$ ділиться на модуль

$m = \frac{m}{2} \cdot 2$. Перший доданок $\frac{m}{2}$ добутку (9) ділиться на $\frac{m}{2}$, а другий $\frac{m}{2} - 1$ доданок ділиться на 2, оскільки за умовою $\frac{m}{2}$ – непарне число. Таким чином показано справедливість порівняння (8), що є алгоритмом визначення значення $a_i^2 (\mathrm{mod}\, m)$ для третього варіанта.

Використовуючи алгоритми (вирази (5) – (8)) у дисертації синтезовано клас обчислювальних засобів для реалізації модульних арифметичних та інших операцій, що входять у склад КА RSA, на яких отримано 7 патентів України. Це підтверджує новизну і практичну значущість отриманих у дисертації науково-практичних результатів. Деякі з обчислювальних засобів для реалізації модульних арифметичних операцій у спрощеному вигляді наведено на рис. 7 і 8.

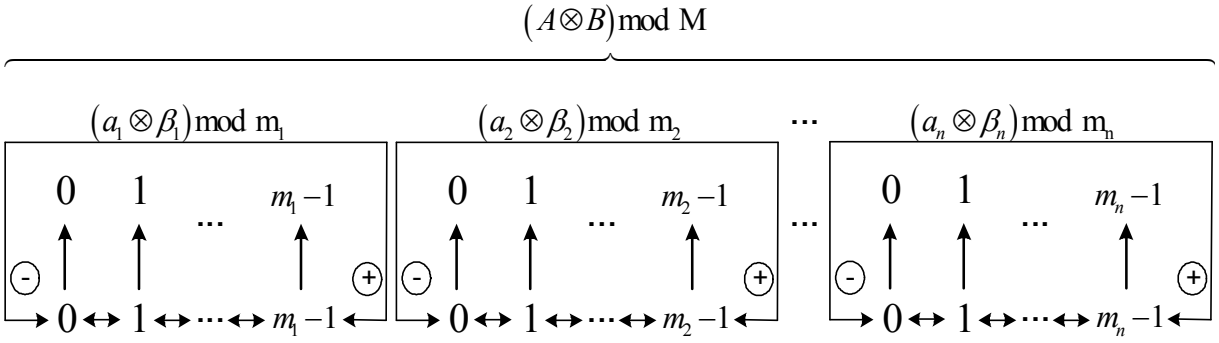


Рис. 7. Схема операційного пристрою СОКІ в МСЧ

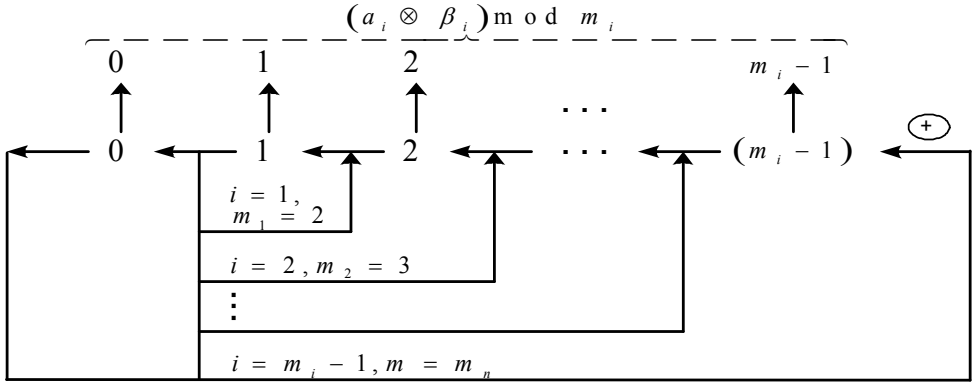


Рис. 8. Схема операційного пристрою СОКІ в МСЧ

У таблицях 1 і 2 подано деякі результати розрахунків і порівняльного аналізу обчислювальної складності КП RSA.

Результати розрахунків і порівняльного аналізу показали високу ефективність застосування МСЧ.

У додатках наведено акти реалізації дисертаційних досліджень та результати розрахунку констант нулевизації МСЧ.

Таблиця 1

Дані розрахунку і порівняльного аналізу часу операції додавання

l (ρ)	Двійкова ПСЧ	Модулярна система числення				Виграш [%]	
	$T^{(+)}_{ПСЧ}/3\cdot\tau_B$	m_n	K	$T^{(+)}_{МСЧ\ \max}/3\cdot\tau_B$			
				МДКЛ	МУКЛ	МДКЛ	МУКЛ
1 (8)	15	7	3	9	3	40	80
2 (16)	31	13	4	24	6	22	80
3 (24)	47	19	5	45	9	5	81
4 (32)	63	29	5	70	14	–	78
8 (64)	127	53	6	159	27	–	71

Таблиця 2

Розрахункові дані і порівняльний аналіз обчислювальної складності КА RSA

Тип операції	МСЧ				Виграш (рази)			
	МДКЛ		МУКЛ		МДКЛ		МУКЛ	
	Max.	Min.	Max.	Min.	Max.	Min.	Max.	Min.
Модульне множення	2030	298	756	30	-	6,9	2,7	68,2
Піднесення до квадрата за модулем	2030	298	756	30	-	6,9	2,7	68,2

ВИСНОВКИ

У дисертаційній роботі на основі застосування модулярної системи числення вирішено науково-технічну задачу розробки методів і засобів зниження обчислювальної складності RSA криптоперетворень без зменшення відмовостійкості функціонування спецпроцесора обробки криптографічної інформації. Отримано такі наукові результати:

1. Новий метод зниження обчислювальної складності криптографічних RSA перетворень шляхом застосування принципу кільцевого зрушення, який забезпечує зниження обчислювальної складності криптоалгоритмів RSA на два порядки. Зі збільшенням довжини розрядної сітки (це характерно для сучасної тенденції розвитку спецпроцесорів обробки криптографічної інформації) ефективність використання розробленого методу зростає.

2. Удосконалено математичну модель оцінки безвідмовності спецпроцесора обробки криптографічної інформації в модулярній системі числення, яка базується на використанні принципів активної та пасивної відмовостійкості з урахуванням властивостей і правил подання й обробки інформації в модулярній системі числення. Проведений розрахунок значення коефіцієнта ефективності і порівня-

льний аналіз безвідмовності показали, що в режимі заміни обчислювальних трактів СОКІ модулярна система числення в 1,5 рази ефективніша, ніж двійкова позиційна система числення. У режимі поступової деградації застосування модулярної системи числення вдвічі ефективніше двійкової позиційної системи числення.

3. Удосконалено метод виконання цілочисельних арифметичних операцій в модулярній системі числення за рахунок використання властивостей модулярної арифметики, що дозволяє зменшити обчислювальну складність RSA-криптоалгоритмів.

4. Метод швидкої реалізації арифметичних операцій в полях Галуа реалізовано в алгоритмі виконання арифметичних операцій, що входять в криптоалгоритми RSA. Використовуючи розроблені алгоритми в дисертації синтезовано клас обчислювальних засобів для реалізації модульних операцій. На спосіб обробки інформації та обчислювальні засоби для реалізації модульних операцій у модулярній системі числення отримано 7 патентів України, що підтверджує новизну і практичну значущість отриманих у дисертації науково-практичних результатів. Результати дисертаційної роботи впроваджено у ЗАТ "Інститут інформаційних технологій" (акт від 22.04.2010 р.), а також у ДП ХПЗ ім. Т. Г. Шевченка (акт від 28.01.1010 р).

СПИСОК ОПУБЛІКОВАНИХ ПРАЦЬ ЗА ТЕМОЮ ДИСЕРТАЦІЇ

1. Краснобаев В. А. Метод обработки криптографической информации в модулярной системе счисления, основанный на принципе кольцевого сдвига / В.А. Краснобаев, С.О. Мартыненко, Ж.В. Дейнеко, А.А. Замула, А.А. Баклыков // Прикладная радиоэлектроника. – 2009. – № 3, т. 8. – С. 343–350.

2. Мартыненко С. О. Метод снижения вычислительной сложности реализации RSA криптопреобразований на основе использования принципа кольцевого сдвига в модулярной системе счисления / С.О. Мартыненко, В.А. Краснобаев, А.А. Замула, О.М. Халина // Прикладная радиоэлектроника. – 2010. –№ 3, т. 9. – С. 454–459.

3. Мартыненко С. О. Метод возведення чисел в квадрат по модулю М модулярной системы счисления / С.О. Мартыненко, В.А. Краснобаєв // Радіоелектронні і комп'ютерні системи. – 2010. – № 5 (46). – С. 165–171.

4. Мартыненко С. О. Метод обнаружения ошибок в спецпроцессоре обработки криптографической информации / С.О. Мартыненко, В.А. Краснобаєв // Радиоэлектроника и информатика. – 2010. – № 1 (48). – С. 75–78.

5. Мартыненко С. О. Математическая модель безотказности спецпроцессора обработки криптографической информации в модулярной системе счисления / С. О. Мартыненко, М. В. Дугин, В. А. Краснобаев // Системи обробки інформації. – Харків : ХВУ , 2010. – Вип. 6 (87). – С. 219 – 222.

6. Краснобаев В.А. Методы реализации криптографических RSA преобразований на основе использования модулярной системы счисления / В.А. Краснобаев, С.О. Мартыненко, Л.С. Сорока // Вісник ХНУ ім. В. Н. Каразіна. – 2010. – № 890. – С. 132–144.

7. Мартыненко С. О. Исследование возможностей применения кодов модулярной системы счисления для создания системы обработки криптографической

информации реального времени / С.О. Мартыненко, В.А. Краснобаев // Збірник наукових праць ХУПС. – Харків: 2009. – Вип. 3(21). – С. 138–143.

8. Мартиненко С. О. Метод технічної реалізації арифметичних операцій у модулярній системі числення на основі використання принципу кільцевого зсуву / С.О. Мартиненко, В.А. Краснобаєв, С.О. Кошман, О.А. Замула, М.С. Деренько // Вісник ХНТУСГ імені Петра Василенка, 2009. – Вип. 87. – С. 71–73.

9. Пат. 35147 Україна, МПК (2009) G06F 11/08. Спосіб виявлення помилок у системі обробки цифрової інформації, що функціонує у модулярній системі числення / Горбенко І.Д., Мартиненко С.О., Замула О.А., Краснобаєв В.А., Горбенко Ю.І.; заявник та патентовласник Горбенко І.Д., Мартиненко С.О., Замула О.А., Краснобаєв В.А., Горбенко Ю.І. – № u 2009 11295; заявл. 06.11.2009; опубл. 11.05.2010, Бюл. № 9. – 4 с.: ил

10. Пат. 49054 Україна, МПК (2009) G06F 11/08. Пристрій для виявлення помилок у модулярній системі числення / Горбенко І. Д., Мартиненко С. О., Замула О. А., Краснобаєв В. А., Горбенко Ю. І., Дейнеко Ж. В.; заявник та патентовласник Горбенко І. Д., Мартиненко С. О., Замула О. А., Краснобаєв В. А., Горбенко Ю. І., Дейнеко Ж. В. – № u 2009 12062; заявл. 24.11.2009; опубл. 12.04.2010, Бюл. № 7. – 10 с.:2 ил.

11. Пат. 47563 Україна, МПК (2009) G06F 11/08. Пристрій для виявлення та виправлення помилок у модулярній системі числення / Мартиненко С.О., Кошман С.О., Барсов В.І., Краснобаєв В.А., Сорока Л.С.; заявник та патентовласник Мартиненко С.О., Кошман С.О., Барсов В.І., Краснобаєв В.А., Сорока Л.С. – № u 2009 09006; заявл. 31.08.2009; опубл. 10.02.2010, Бюл. № 3. – 11 с.: ил.

12. Пат. 49712 Україна, МПК (2009) G06F 7/00. Пристрій для додавання і віднімання чисел за модулем М модулярної системи числення / Горбенко І. Д., Мартиненко С.О., Замула О.А., Краснобаєв В.А., Бобух В.А., Горбенко Ю.І.; заявник та патентовласник Горбенко І.Д., Мартиненко С.О., Замула О.А., Краснобаєв В.А., Бобух В.А., Горбенко Ю.І. – № u 2009 11297; заявл. 06.11.2009; опубл. 11.05.2010, Бюл. № 9. – 10 с.:1 ил.

13. Пат. 50024 Україна, МПК (2009) G06F 7/00. Пристрій для складання чисел за модулем М модулярної системи числення / Барсов В.І., Мартиненко С.О., Краснобаєв В.А., Сорока Л.С.; заявник та патентовласник Барсов В.І., Мартиненко С.О., Краснобаєв В.А., Сорока Л.С. – № u 2009 11285; заявл. 06.11.2009; опубл. 25.05.2010, Бюл. № 10. – 16 с.:1 ил.

14. Пат. 50417 Україна, МПК (2009) G06F 7/74. Пристрій для додавання та віднімання чисел за модулем М модулярної системи числення з контролем помилок / Барсов В.І., Мартиненко С.О., Краснобаєв В.А.; заявник та патентовласник Барсов В.І., Мартиненко С.О., Краснобаєв В.А. – № u 2009 12507; заявл. 03.12.2009; опубл. 10.06.2010, Бюл. № 11. – 10 с.: ил.

15. Пат. 51512 Україна, МПК (2009) G06F 7/74. Пристрій для піднесення чисел до квадрата за модулем m модулярної системи числення / Барсов В.І., Мартиненко С.О., Краснобаєв В.А.; заявник та патентовласник Барсов В.І., Мартиненко С.О., Краснобаєв В.А. – № u 2009 12508; заявл. 03.12.2009; опубл. 26.07.2010, Бюл. № 14. – 4 с.: ил.

16. Мартыненко С. О. Синтез архитектуры компьютерной системы обработки криптографической информации на основе модулярной арифметики / С.О. Ма-

ртыненко // Проблемы информатики и моделирования : тез. докл. Девятой международной науч.–техн. конференции. – Харьков, 26–28 ноября 2009 г. – С. 51.

17. Мартыненко С. О. Задача оптимизации структуры системы обработки криптографической информации в модулярной системе счисления / С.О. Мартыненко // Інтегровані комп'ютерні технології в машинобудуванні ІКТМ–2009: тез. допов. Міжнародної науково–технічної конференції. – Харків, 2009. – С. 241.

18. Краснобаев В.А. Методы реализации криптографических RSA преобразований на основе использования модулярной системы счисления / В.А. Краснобаев, С.О. Мартыненко, Л. С. Сорока // Компьютерное моделирование в наукоемких технологиях КМТН–2010: тез. докл. Научно–технической конференции с международным участием. – Харьков, 18–21 мая 2010 г. – Ч. 1. – С. 190–193.

19. Мартыненко С. О. Метод снижения вычислительной сложности алгоритма обработки цифровой информации на основе использования кодов модулярной системы счисления / С.О. Мартыненко, М.В. Дугин, В.А. Краснобаев // Перспективные компьютерные управляющие и телекоммуникационные системы для железнодорожного транспорта Украины: тез. докл. 23–ей международной научно–практической конференции: – Алушта, 23–29 сентября 2010 г. – С. 57–61.

АНОТАЦІЯ

Мартиненко С. О. Метод і засоби зниження обчислювальної складності криптографічних RSA перетворень на основі модулярної системи числення. – На правах рукопису.

Дисертація на здобуття вченого ступеня кандидата технічних наук за спеціальністю 05.13.05 – комп'ютерні системи і компоненти. – Харківський національний університет радіоелектроніки, Харків, 2012.

Мета роботи – зниження обчислювальної складності RSA КП без зниження відмовостійкості функціонування спецпроцесора обробки криптографічної інформації (СОКІ). Науково-технічна задача – розробка методів і засобів зниження обчислювальної складності RSA КП без зниження відмовостійкості функціонування СОКІ на основі використання модулярної системи числення (МСЧ).

Наукова новизна отриманих результатів полягає у тому що: 1) уперше розроблено метод обробки криптоперетворень RSA, який характеризується використанням принципу кінцевого зрушення та базується на застосуванні модулярної системи числення, що дозволяє знизити обчислювальну складність RSA криптографічних перетворень; 2) удосконалено математичну модель безвідмовності спецпроцесора обробки криптографічної інформації, яка відрізняється урахуванням надійності контрольних трактів, що дає можливость оцінити надійність спецпроцессора обробки криптографічної інформації; 3) Удосконалено метод виконання цілочисельних арифметичних операцій в модулярній системі числення, який на відміну від аналогів ураховує адитивно-мультиплікативні властивості полів Галуа, що дозволяє підвищити швидкодію спецпроцессора обробки криптографічної інформації.

Ключові слова: обчислювальна складність, криптографічний алгоритм, спецпроцесор, поля Галуа, модулярна система числення, принцип кільцевого зрушення.

АННОТАЦИЯ

Мартыненко С. О. Метод и средства снижения вычислительной сложности криптографических RSA преобразований на основе модулярной системы счисления. – На правах рукописи.

Диссертация на соискание ученой степени кандидата технических наук по специальности 05.13.05 – компьютерные системы и компоненты. – Харьковский национальный университет радиоэлектроники, Харьков, 2012.

Диссертация посвящена разработке метода снижения вычислительной сложности RSA криптопреобразований (КП) на основе использования непозиционных кодовых структур в модулярной системе счисления (МСС).

Существуют два принципиальных пути снижения вычислительной сложности реализации криптографического алгоритма: частичное сокращение количества операций и уменьшение времени реализации каждой операций. Первый путь предполагает изменение (модификацию) алгоритма (определение и выделение смежных и параллельных ветвей реализации операций КП, с целью возможности организации параллельной обработки криптографической информации, уменьшение длительности последовательной цепи вычислений и т.п.). Это весьма трудоемкий процесс и вряд ли это целесообразно и вообще возможно. Второй путь основан на уменьшении (снижении) времени выполнения модульных операций в криптоалгоритме (КА), которые в современных вычислителях реализуются в обычной двоичной позиционной системе счисления.

Цель работы – снижение вычислительной сложности RSA КП без снижения отказоустойчивости функционирования спецпроцессора обработки криптографической информации (СОКИ). Научно-техническая задача – разработка методов и средств снижения вычислительной сложности RSA КП без снижения отказоустойчивости функционирования СОКИ на основе использования МСС.

Научная новизна полученных результатов состоит в следующем. 1. Впервые разработан метод обработки криптопреобразований, который основан на применении модулярной системы счисления путем использовании принципа кольцевого сдвига, что позволяет снизить вычислительную сложность RSA криптографических преобразований. 2. Усовершенствована математическая модель безотказности спецпроцессора обработки криптографической информации, которая отличается учетом надежности контрольных трактов, что дает возможность оценить надежность спецпроцессора обработки криптографической информации. 3. Усовершенствован метод выполнения целочисленных арифметических операций в модулярной системе счисления, который в отличие от аналогов учитывает аддитивно-мультипликативные свойства полей Галуа, что позволяет увеличить быстродействие спецпроцессора обработки криптографической информации.

Практическое значение полученных результатов. Разработанный в диссертационной работе метод снижения вычислительной сложности RSA криптопреобразований, а также усовершенствованные методы выполнения арифметических операций в модулярной системе счисления, путем учета свойств полей Галуа, являются научно-методологической основой для практического создания СОКИ в МСС. Оценка вычислительной сложности КА RSA, результаты расчетов и срав-

нительного анализа производительности и надежности, проведенные в диссертационной работе, показали, что с увеличением числового диапазона обработки информации, это характерно для современной тенденции развития СОКИ, эффективность применения МСС для реализации криптографических преобразований существенно возрастает.

Ключевые слова: вычислительная сложность, криптографический алгоритм, спецпроцессор, поля Галуа, модулярная система счисления, принцип кольцевого сдвига.

ABSTRACT

Sergey O. Martynenko Method and tools for reducing the computational complexity, cryptography RSA–transformations on the basis of modular number system. – Manuscript.

Dissertation for the degree of candidate of technical sciences on speciality 05.13.05 – the computer systems and components. – Kharkiv National University of Radio Electronics, Kharkiv, 2012.

The purpose of work is reducing computational complexity of RSA CC without the reducing of fault–tolerance functioning of the special processor handling cryptographic information (SPHCI). Scientific and technical task – methods and techniques to reduce computational complexity without reducing RSA CC without the reducing of failover of functioning of SPHCI on the basis of the use of modular number system (MNS).

The scientific novelty of received results consists in following: 1) for the first time developed a method for processing of cryptotrasformations, which is based on the use of a modular system by using the principle of circular shift, which reduces the computational complexity of the RSA cryptographic; 2) improved mathematical model of the fail-safe for the special processor handling cryptographic information which is different considering the reliability of the control tracts, which makes it possible to assess the reliability of special processor handling of cryptographic information; 3) improved method for performing integer arithmetic in the modular number system, which is unlike analogues takes into account the additive-multiplicative properties of Galois fields, thus increasing the speed of processing special processor cryptographic information.

Keywords: computational complexity, cryptographic algorithms, cryptographic special processor, Galois fields, modular number system, the principle of circular shift processing.

Відповідальний випусковий Руденко О.Г.

Підп. до друку Формат 60х84 1/16. Спосіб друку – ризографія.
Умов.друк.арк. Облік. вид.арк. Тираж 100 прим.
Ціна договірна Зам №

ХНУРЕ. Україна. 61166, Харків, просп. Леніна, 14

Віддруковано в навчально-науковому
видавничо-поліграфічному центрі ХНУРЕ
61166, Харків, просп. Леніна, 14