МІНІСТЕРСТВО ОСВІТИ І НАУКИ, МОЛОДІ ТА СПОРТУ УКРАЇНИ

ТЕРНОПІЛЬСЬКИЙ НАЦІОНАЛЬНИЙ ЕКОНОМІЧНИЙ УНІВЕРСИТЕТ

Якименко Ігор Зіновійович

УДК 681.3.06

МЕТОДИ ТА АЛГОРИТМИ ОПРАЦЮВАННЯ ІНФОРМАЦІЙНИХ ПОТОКІВ В КОМП'ЮТЕРНИХ МЕРЕЖАХ ЗА УМОВИ ЗАСТОСУВАННЯ ЕЛІПТИЧНИХ КРИВИХ

05.13.05 – комп'ютерні системи та компоненти

Автореферат
дисертації на здобуття наукового ступеня
кандидата технічних наук

Тернопіль – 2012

Дисертацією є рукопис.
Робота виконана в Тернопільському національному економічному університеті Міністерства освіти і науки, молоді та спорту України.

Науковий керівник: доктор технічних наук, професор
Николайчук Ярослав Миколайович,
Тернопільський національний економічний університет, завідувач кафедри спеціалізованих комп'ютерних систем.

Офіційні опоненти:
доктор технічних наук, професор
Бєссалов Анатолій Володимирович,
Національний технічний університет України «Київський політехнічний інститут», професор кафедри математичних методів захисту інформації;

доктор технічних наук, професор
Головко Володимир Адамович,
Брестський державний технічний університет, завідувач кафедри інтелектуальних інформаційних технологій.

Захист відбудеться 22 березня 2012 року о 16^{00} годині на засіданні спеціалізованої вченої ради К.58.082.02 у Тернопільському національному економічному університеті за адресою: 46004, м. Тернопіль, вул. Львівська, 11 (корпус 11, зал засідань вченої ради).

З дисертацією можна ознайомитися у бібліотеці Тернопільського національного економічного університету за адресою: 46004, м. Тернопіль, вул. Львівська, 11.

Автореферат розісланий 21 лютого 2012 р.

Вчений секретар
спеціалізованої вченої ради Яцків В.В

Підписано до друку 17. 02. 2012 р.
Фомат 60х90/16. Гарнітура Times.
Папір офсетний. Друк на дублікаторі.
Ум. друк. арк. 0,9. Зам. № А007-12. Тираж 150 прим.

Свідоцтво про внесення суб'єкта видавничої справи
до Державного реєстру видавців ДК №3467 від 23.04.2009 р.

Віддруковано у видавництві ТНЕУ
46020 Тернопіль, вул. Львівська, 11
тел. (0352) 47-58-72

ЗАГАЛЬНА ХАРАКТЕРИСТИКА РОБОТИ

Актуальність теми. Створення розвиненого і захищеного інформаційного суспільства є невід'ємною умовою розвитку держави. Глибока технологічна реформа, що проходить сьогодні в Україні, спрямована на впровадження низки важливих комп'ютеризованих інформаційних систем і мереж зв'язку, телекомунікаційних систем, систем прийняття рішень та ін.

Важливим аспектом розвитку досліджень в цій галузі є врахування принципово нових відмінностей між комп'ютеризованими системами та комп'ютерними мережами. Виходячи з визначення комп'ютерної системи як взаємодії сукупності системних об'єктів, вона, як показано в роботах американського вченого Дж. Мартіна та українських вчених О.В.Палагіна, В. А. Стеклова, Я.М. Николайчука, і т.д. включає в себе п'ять системних об'єктів: Р – процесори, Д – дані, СПД – систему передавання даних, О – оператори і ОУ – об'єкти управління. При цьому комунікаційним компонентом комп'ютеризованих систем є комп'ютерні мережі, які в склад своїх компонентів включають процесори, дані і СПД.

При проектуванні та вдосконаленні сучасних комп'ютерних мереж (КМ), які обслуговують проблемно-орієнтовані та спеціалізовані комп'ютерні системи (СКС), актуальною задачею є дотримання умов високоефективного захисту інформаційних потоків (ІП) від несанкціонованого доступу.

Вагомий внесок у дослідження проблеми захисту інформаційних потоків комп'ютерних систем та мереж вклали вітчизняні та зарубіжні вчені: Задірака В. К., Широчин В. П., Горбенко І. Д., Долгов В. І., Бессалов А. В., Воєводін В. В., Головко В. А., Мельникова О. А., Качко О. Г., Р. Шуф, В. Міллер, Н. Кобліц, А. Лєнстра, Т. Ланге, К. Фокс, В. Лі, Ф. Гонсалес та ін.

Аналіз стану захисту ІП в комп'ютеризованих системах свідчить, що в цілому розв'язання цієї задачі далекий від досконалості. Тим більше, що виникає потреба у побудові стійких і продуктивних методів та алгоритмів шифрування ІП у КМ з врахуванням тенденцій зростання вимог до необхідного рівня їх захисту. До таких методів можна віднести алгоритми з використанням математичного апарату еліптичних кривих (ЕК), які, як показав світовий досвід, забезпечують високий рівень захисту в порівнянні з відомими.

Тому розробка підходів, методів, алгоритмів та комп'ютерних засобів захисту інформації з використанням мережевих технологій та високопродуктивних спецпроцесорів на основі різних теоретико-числових базисів (ТЧБ) є актуальною науковою задачею.

Зв'язок роботи з науковими програмами, планами і темами. Представлені в дисертації дослідження виконані у рамках науково-дослідних робіт кафедри комп'ютерної інженерії Тернопільського національного економічного університету "Методи та засоби реалізації алгоритмів захисту інформації, стійких

до атак на реалізацію” (Державний реєстраційний номер 0105U008181) та “Паралельні методи та засоби реалізації алгоритмів захисту інформації в комп’ютерних мережах з використанням математичного апарату еліптичних кривих” (Державний реєстраційний номер 0109U000035).

Мета і задачі дослідження. Метою дисертаційної роботи є зменшення складності та підвищення швидкодії алгоритмів мережного та програмно-апаратного опрацювання ІП за умови застосування ЕК.

Для досягнення поставленої мети в дисертаційній роботі необхідно розв‘язати низку взаємопов’язаних **задач**:

– дослідити системні характеристики різних класів архітектур та трафіків КМ, оцінити їх емерджентність та проаналізувати сучасний рівень захисту ІП у КМ;

– розробити методи та дослідити швидкодіючі алгоритми опрацювання ІП на основі матрично-модульних перетворень ТЧБ Крестенсона-Радемахера, ТЧБ Крестенсона в задачах захисту інформації;

– дослідити особливості та оцінити часову складність основних операцій алгоритму Шуфа в задачах захисту ІП з застосуванням ЕК;

– розробити функціональну структуру спеціалізованого програмно-апаратного засобу опрацювання ІП за умови застосування ЕК.

Об'єкт дослідження – процеси програмно-апаратного опрацювання інформаційних потоків у комп’ютерних мережах за умови застосування еліптичних кривих.

Предмет дослідження – методи, алгоритми та засоби зменшення часової складності опрацювання інформаційних потоків на основі використання теоретико-числових базисів Радемахера-Крестенсона.

Методи дослідження. В дисертаційній роботі використані математичні основи теорії чисел, алгебри Евкліда та теорії полів Галуа, теорії інформації, теорії алгоритмів, математичні основи ортогональних функцій та теоретико-числових базисів Радемахера-Крестенсона, теорії графів та теорії цифрових автоматів.

Наукова новизна отриманих результатів полягає в наступному:

Вперше:

–розроблено метод опрацювання інформаційних потоків у комп’ютерних мережах за умови застосування ЕК на основі матричних програмно-апаратних засобів, які на відмінну від існуючих дали змогу шляхом застосування теоретико-числових базисів Радемахера-Крестенсона зменшити часову складність з експоненційної до лінійної або лінійно-логарифмічної.

– побудовано аналітичні вирази характеристик часової складності формування та опрацювання інформаційних потоків за умови застосування еліптичних кривих з використанням системи числення залишкових класів, теоретико-числових базисів Радемахера-Крестенсона, розмежованої системи

числення Радемахера-Крестенсона, які склали теоретичну основу зменшення часової складності компонентів алгоритму Шуфа, що на відмінну від існуючих дало можливість підвищення рівня захисту інформаційних потоків в сучасних та проектованих комп'ютерних мереж;

– розроблено теоретичні засади матрично-модульних операцій модулярного множення та експоненціювання, які на відмінну від відомих ґрунтуються на використанні теоретико-числових базисів Радемахера-Крестенсона та дають змогу зменшити часову складність алгоритму пошуку порядку еліптичних кривих.

Отримав подальший розвиток:

– метод захисту інформаційних потоків з використанням еліптичних кривих на основі генерування їх параметрів, що дало змогу зменшити часову складність алгоритмів пошуку залишків чисел великої розрядності, знаходження найбільшого спільного дільника (НСД), модулярного множення, експоненціювання та пошуку оберненого елемента за модулем за рахунок використання теоретико-числових базисів Крестенсона та Радемахера-Крестенсона.

Практичне значення одержаних результатів.

1. Розроблено високопродуктивні алгоритми модулярного множення та експоненціювання, пошуку найбільшого спільного дільника, оберненого елемента за модулем, шляхом використання розробленого математичного апарату матрично-модульних операцій у базисі Крестенсона-Радемахера, що дозволило зменшити на 1-2 порядки часову складність базових операцій алгоритму Шуфа.

2. Побудовано апаратні засоби реалізації модульних операцій над числами великої розрядності та розроблено схемотехнічні рішення відповідних спеціалізованих процесорів, які можна використати в засобах шифрування інформаційних потоків.

3. Розроблено програмне забезпечення формування параметрів еліптичних кривих та спеціалізовані високопродуктивні програмно-апаратні засоби опрацювання інформаційних потоків в комп'ютерних мережах, які використовуються для підвищення рівня захисту.

Результати досліджень використані в навчальному процесі на кафедрах комп'ютерної інженерії та спеціалізованих комп'ютерних систем при викладанні дисциплін: «Комп'ютерні системи», «Захист інформації в комп'ютерних системах», «Проектування спеціалізованих комп'ютерних систем», а також впроваджені на ТОВ ТКБР «Стріла» для захисту інформаційних потоків в дистрибутивних та корпоративних комп'ютерних мережах.

Особистий внесок здобувача. Дисертаційна робота є результатом самостійної роботи автора. У друкованих працях, опублікованих у співавторстві, автору належить: [1] – метод перетворень китайської теореми про залишки в матрично-розмежованому базисі Радемахера Крестенсона; [2] – методи пошуку

найбільшого спільного дільника у базисі Крестенсона; [3] – метод шифрування на основі алгоритмів RSA та Ель-Гамаля з використанням ТЧБ Радемахера-Крестенсона; [4] – теорія та оптимізація опрацювання великорозрядних чисел у базисі Крестенсона; [16] – метод модулярного множення та експоненціювання з використанням розмежованої системи числення Радемахера-Крестенсона; [17] – алгоритм пошуку простих чисел та аналітика взаємнопростих чисел спеціального виду на основі використання базису Крестенсона; [18] – структура високопродуктивного спецпроцесора в системі залишкових класів базису Крестенсона для виконання операцій з числами великої розрядності; [7] – високопродуктивний генетичний алгоритм пошуку параметрів еліптичних кривих; [12] – метод генерування параметрів ЕК із застосуванням символів Якобі; [8] – формалізована математична модель захисту інформаційних потоків та апаратно-програмна реалізація їх опрацювання.

Апробація результатів дисертації. Основні результати дисертаційної роботи доповідались і обговорювались на:

- міжнародній конференції “Сучасні проблеми радіотехніки, телекомунікації та комп’ютерні науки”, TCSET’2004, 24–28 лютого, 2004 року;
- III Міжнародній конференції студентства та молоді "Світ інформації та телекомунікацій-2006" Україна, Київ, ДУІКТ 26–27 квітня 2006 року;
- XII науковій конференції Тернопільського державного технічного університету імені Івана Пулюя, Тернопіль, ТДТУ, 14–15 травня 2008 року;
- X міжнародній конференції «Досвід проектування і застосування САПР в мікроелектроніці», (CADSM-2009), Львів-Поляна, Україна, 19–24 лютого 2009 року;
- VII міжнародній науково-практичній конференції «Проблеми впровадження інформаційних технологій в економіці», Ірпінь, 23–24 квітня 2009 року;
- міжнародній науково-практичній конференції “Сучасні проблеми радіотехніки, телекомунікації та комп’ютерні науки”, TCSET’2010, 23–27 лютого, 2010;
- проблемно-науковій міжгалузевій конференції «Інформаційні проблеми комп’ютерних систем, юриспруденції, енергетики, економіки, моделювання та управління (ПНМК-2010), Україна, Бучач, 01–04 червня 2010 року;
- XI міжнародній науково-практичній конференції «Досвід проектування і застосування САПР в мікроелектроніці», (CADSM-2011), Поляна-Свалява, Україна , 23–25 листопада 2011року.

Публікації. Основні положення дисертаційної роботи в повному обсязі висвітлені у 18 працях, з яких 11 статей у науково-технічних журналах, (з них 2 одноосібних), які входять до переліку періодичних фахових видань, затверджених МОНмолодьспорту України, 7 публікацій у збірниках матеріалів і тезах доповідей науково-технічних конференцій.

Структура дисертації. Дисертаційна робота складається зі вступу, чотирьох розділів, загальних висновків, списку використаних джерел та додатків. Загальний

обсяг дисертації становить 201 сторінку, з них 142 сторінки основного тексту, містить 37 рисунків, 32 таблиці, 12 додатків, список використаних джерел із 122 найменувань.

ОСНОВНИЙ ЗМІСТ РОБОТИ

У **вступі** обґрунтовано актуальність виконаних досліджень, подано зв'язок дисертаційної роботи з науковими програмами та темами. Сформульовано мету та задачі досліджень, дано характеристику наукової новизни отриманих результатів і практичної значущості роботи, наведено відомості про апробацію результатів та їх впровадження.

У **першому розділі** проведено класифікацію архітектур та трафіків комп'ютерних мереж. На основі критерію емерджентності K_e досліджено ефективність трафіків різних типів мереж та встановлено, що високим рівнем емерджентності характеризуються багаторівневі зірково-магістральні та мережно-ієрархічні КМ, а також безпровідні КМ з активними ретрансляторами. Оцінено характеристики коефіцієнтів необхідного рівня захисту інформаційних потоків в мережах з різними архітектурами $K_{зе}$, які розраховані згідно виразів $K_e = \frac{n_з}{n_e}$, $K_{зе} = \frac{K_з}{K_e}$, де $n_з, n_e$ - відповідно число зв'язків та компонентів, $K_з$ - коефіцієнт захисту по характеру секретності КМ.

Наведено обґрунтування необхідності більш високого рівня захисту ІП в сучасних та проектованих КМ. Сформульовані теоретичні засади кодування та опрацювання ІП в КМ на основі ТЧБ Радемахера та Крестенсона.

Показано, що на низових рівнях систем реального часу формування структуризованих ІП досягається певний рівень захисту від несанкціонованого доступу.

Досліджені системні характеристики кодування та опрацювання ІП на основі ТЧБ Радемахера, який породжує двійкову систему числення. Показано переваги застосування ТЧБ Крестенсона для структуризації ІП та їх опрацювання на основі модульних математичних операцій. Систематизовані аналітичні моделі прямих та зворотних перетворень ТЧБ Крестенсона: цілочисельного, нормалізованого, досконалого та в розмежованій формі. Оцінена часова складність реалізації модульних арифметичних операцій в базисах Радемахера та Крестенсона в залежності від розрядності процесорів.

Розроблена класифікація сучасних методів криптографії, що базуються на застосуванні ЕК, та проведено аналіз стійкості, який дозволяє встановити ефективність застосування алгоритму Шуфа для їх реалізації.

Проаналізовано різні удосконалення алгоритму Шуфа та на основі оцінки їх часових складностей встановлено, що він забезпечує точніший пошук порядку ЕК, але в той же час характеризується найбільшою часовою складністю. Даний

алгоритм в існуючих системах традиційно реалізується на основі використання математичного апарату опрацювання двійкових чисел базису Радемахера, що призводить до експоненційної складності його реалізації програмно-апаратними засобами і обмежує можливості застосування для забезпечення необхідного рівня захисту у відповідності із зростаючими вимогами криптостійкості ІП в КМ.

Розроблено систему показників та критеріїв ефективності функціонування алгоритмів шифрування на ЕК та оцінки їх стійкості до атак, що дозволило сформулювати вимоги необхідного рівня вдосконалення алгоритмів захисту ІП за умови застосування ЕК та їх реалізації на основі математичного апарату ТЧБ Крестенсона-Радемахера.

Теоретичне обґрунтування дослідження, моделювання та оцінка ефективності запропонованих методів захисту ІП за умови застосування ЕК, які відповідають сформульованим критеріям та показникам ефективності алгоритмів на основі теоретичних засад базисів Радемахера-Крестенсона, є постановкою задачі та предметом її дослідження.

У другому розділі проведені теоретичні та експериментальні дослідження розроблених методів та критеріїв ефективності опрацювання ІП за умови застосування ЕК на основі математичного апарату базису Крестенсона-Радемахера. Обгрунтована доцільність застосування цілочисельних перетворень системи залишкових класів, згідно аналітичних виразів:

1. Пряме перетворення :

$$N_k = (b_1 b_2 ... b_i ... b_k)_{(p_1 p_2 ... p_i ... p_k)}; N_k = b_i (\mathrm{mod}\, p_i), N_k = a_i p_i + b_i, P = \prod_{i=1}^{k} p_i ; 0 \le N_k \le P. \quad (1)$$

2. Зворотне:

$$b_i = res N_k (\mathrm{mod}\, p_i), \; N_k = res \sum_{i=1}^{k} b_i \cdot B_i (\mathrm{mod}\, P), \; B_i = \frac{P}{p_i} \cdot m_i \equiv 1 (\mathrm{mod}\, P_i), \quad (2)$$

де $p_1, p_2, \ldots, p_j, \ldots, p_k$ система взаємно простих модулів; $0 \le N_k \le P-1$ - код числа в базисі Радемахера; P- діапазон кодування чисел, в якому однозначно виконується пряме та зворотне перетворення базису Крестенсона; $0 \le b_i \le P_i - 1$- найменший невід'ємний залишок числа N_k по модулю P_i; B_i- базисне число системи залишкових класів (СЗК) заданої набором модулів $p_1, p_2, \ldots, p_j, \ldots, p_k$; $0 \le m_i \le P_i - 1$- коефіцієнт досконалості СЗК; $(b_1 b_2 ... b_i ... b_k)_{(p_1 p_2 ... p_i ... p_k)}$- код числа в базисі Крестенсона.

Розроблено метод матрично-модулярного множення n–розрядних чисел $a=a_{n-1}2^{n-1}+\ldots+ +a_i 2^i+\ldots+ a_1 2+a_0$ та $b=b_{n-1}2^{n-1}+\ldots+ +b_i 2^j+\ldots+ b_1 2+b_0$, де a_i, $b_j=0, 1$, n–розрядність модуля p. Для знаходження результату їх множення за модулем p побудована матриця $\left\| c_{ij} \right\| = 2^{i+j} \bmod p$. Добуток чисел a та b знаходиться згідно формули:

$$a \cdot b = \left(\sum_{i=1}^{n-1} \sum_{j=1}^{n-1} a_i b_j 2^{i+j} \right) \mathrm{mod} \;\; p, \quad (3)$$

де a_i, $b_j=1$, тобто c_{ij} знаходиться на перетині стовпця та рядка, для яких відповідні a_i та b_j дорівнюють 1.

Таким чином, отримано новий алгоритм заміни операції множення операцією додавання з часовою складністю $O2(n)=\begin{cases}\log n, \textit{ якщо } n\le 64\\ \frac{n}{2}\cdot\log n, \textit{ в інших випадках}\end{cases}$, в порівнянні з відомими: $O1(n)=n^2$ - звичайний метод множення, $O(n)=n\cdot\log n\cdot\log(\log n)$ - алгоритм Шонхаге-Штрасена, або $O3(n)=n^{1,585}$, $O4(n)=n^{1,465}$ - алгоритми Каратсуби та Тома-Кука відповідно.

Результати дослідження часової складності запропонованого алгоритму наведені на рис. 1. Ефективність запропонованого алгоритму модулярного множення (рис.2). $E3(n)=\begin{cases}n\cdot\log(\log n), \textit{ якщо } n<64\\ \log(\log n), \textit{ в інших випадках.}\end{cases}$

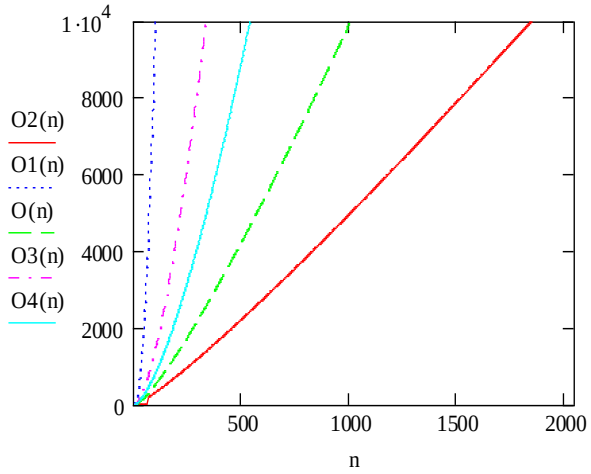

Рис. 1 – Часові складності операції модулярного множення

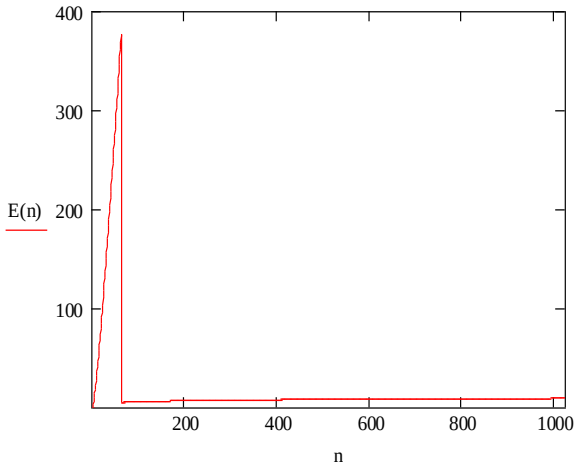

Рис. 2 – Ефективність розробленого методу модулярного множення розрядності n.

Результати чисельного експерименту показують, що при розрядності чисел до 64 бітів ефективність операції модулярного множення стрімко зростає на 1 порядок за рахунок заміни багатотактної операції множення у базисі Радемахера матрично-модульною операцією сумування в базисі Крестенсона.

Отже, використання базису Крестенсона суттєво зменшує часову складність алгоритму модулярного множення, що визначає перспективи щодо розробки високопродуктивних програмно-апаратних засобів із забезпеченням високого рівня захисту ІП в КМ.

Автором розроблено метод модулярного експоненціювання $a^x mod\ p$ (причому $x\le\varphi(p)$, $\varphi(p)$ – значення функції Ейлера від модуля p) в базисі Крестенсона-Радемахера та досліджена його ефективність в порівнянні з реалізацією в базисі Радемахера на основі матрично-модульних операцій множення згідно аналітичного виразу:

$$a^x \bmod p = \left(\prod_{i=0}^{n-1} a^{x_i 2^i} \right) \bmod p = \prod_{k=0}^{n-1} \left(\sum_{j=0}^{n-1} \left(\sum_{i=0}^{n-1} a_i \cdot a_j \cdot 2^{i+j} \right) \bmod p \right)^{x_k 2^k} \bmod p. \qquad (4)$$

Основними перевагами такого методу є здійснення операцій множення над малорозрядними залишками, що дозволяє зменшити часову складність алгоритму.

Побудований метод піднесення до степеня двійкового числа великої розрядності за модулем p дозволяє зменшити часову складність за рахунок заміни операції множення модулярним сумуванням, підвищити швидкодію на 1–2 порядки для чисел розрядності менше 64 біт, а в діапазоні від 64 до 1024 біт на 30% (рис. 3). Чисельний експеримент показав, що розроблений метод піднесення до степеня двійкового числа за модулем p в базисі Радемахера–Крестенсона дозволяє зменшити часову складність з $O2 = n^3$, або $O1(n) = n^2 \log n$ - Монтгомері метод до $O(n) = \begin{cases} n \log_2 n, \textit{якщо } n < 64 \\ \frac{n^2}{2} \log_2 n \cdot, n \geq 64 \end{cases}$ в $E2(n) = \begin{cases} n, \textit{для } n < 64 \\ \log_2 n, n \geq 64 \end{cases}$ разів (рис. 4).

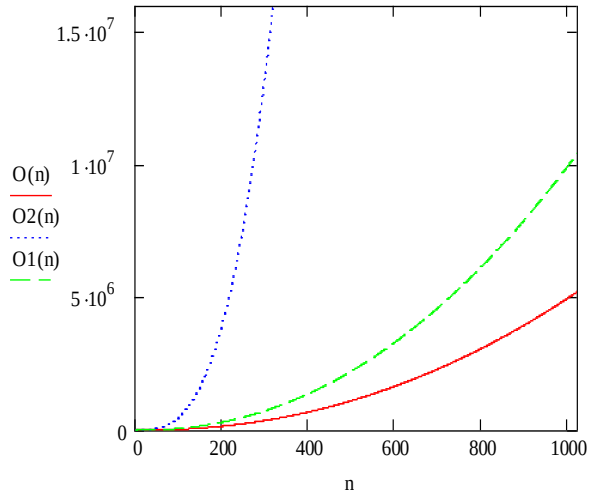

Рис. 3 – Часова складність операції модулярного експоненціювання класичних та запропонованого методу.

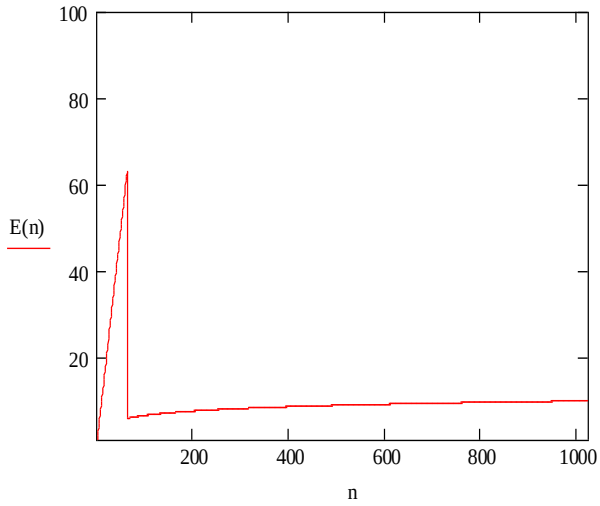

Рис.4 – Ефективність запропонованого алгоритму модулярного експоненціювання розмірності n.

Операція модулярного експоненціювання є базовою в найбільш поширених системах захисту інформаційних потоків з відкритими ключами (RSA, Ель–Гамаля тощо), тому розроблений метод доцільно використовувати для реалізації найбільш ефективного алгоритму Шуфа визначення стійкості ЕК, що дозволить реалізувати можливості підвищення рівня захисту проектованих КМ.

В роботі досліджено ефективність застосування розроблених алгоритмічних обчислень у базисі Крестенсона-Радемахера в існуючих криптоалгоритмах RSA і Ель–Гамаля, в результаті чого отримані характеристики їх часових складностей

згідно аналітичних виразів: $O5(n)=\begin{cases}\log_2 n\left(3\log_2 n+\dfrac{n}{2}\right), n<64\\ n\cdot\left(3\log_2 n+\dfrac{n}{2}\right), n\geq 64.\end{cases}$ і

$O6(n)=\begin{cases}\log_2 n\cdot\left(\log_2 n+\dfrac{n}{2}\log_2 n+1\right), n<64\\ n\cdot\left(\log_2 n+\dfrac{n}{2}\log_2 n+1\right), 64\leq n\leq 1024\end{cases}$ відповідно.

Таким чином, використання розроблених алгоритмів дозволяє зменшити часові складності існуючих алгоритмів на 1–2 порядки для параметрів, менших 64 біт, і на порядок при параметрах від 64 до 1024 біт.

У **третьому розділі** розроблена теоретична основа алгоритму Шуфа знаходження порядку ЕК з застосуванням ТЧБ Крестенсона-Радемахера.

Розроблено метод пошуку залишків $X\,(\mathrm{mod}Y)$ чисел великої розрядності з використанням ТЧБ Крестенсона-Радемахера, в якому операція ділення замінюється операцією додавання залишків степеневих коефіцієнтів по заданому модулю (табл. 1) та виразу (6).

Таблиця 1–Знаходження залишків степенів двійки

2^{n-1}	2^{n-2}	…	2^{i}	…	2	1
x_{n-1}	x_{n-2}	…	x_i	…	x_1	x_0
y_{n-1}	y_{n-2}	…	y_i	…	y_1	y_0

Щоб знайти елемент y_i, необхідно попередній елемент y_{i-1} помножити на 2 (дописати в кінці 0 у двійковому записі) і порівняти з модулем p_1 та $X\,(\mathrm{mod}Y)$ знаходити згідно виразів:

$$y_i=\begin{cases}2\cdot y_{i-1},\ 2\cdot y_{i-1}<Y\\ 2\cdot y_{i-1}-y_i,\ 2\cdot y_{i-1}\geq Y\end{cases}; \tag{5}$$

$$X\bmod Y=\left(\sum_{i=1}^{n-1}y_i\right)\bmod Y,\ x_i=1. \tag{6}$$

Вперше розроблені методи пошуку найбільшого спільного дільника з використанням математичних основ ТЧБ Радемахера-Крестенсона. Суть першого методу полягає у вдосконаленні реалізації алгоритму Евкліда, тобто знаходження значень $r_1=res(X\bmod(Y))$, $r_2=res(Y\bmod(r_1))$,…, $r_{n-1}=res(r_{n-1}\bmod(r_n))$ з використанням алгоритму пошуку залишків великорозрядних чисел в розмежованій системі числення Радемахера-Крестенсона.

Другий метод полягає в застосуванні ТЧБ Крестенсона, тобто поданні чисел X і Y у цілочисельній формі системи залишкових класів по простих модулях, які

не перевищують половину розрядності більшого з X, Y. Згідно виразу $z = \prod_{j=1}^{k} p_j$,

де $p_j = \begin{cases} p_j, a_j = b_j = 0 \\ 1, a_j \neq b_j \end{cases}$ знаходиться найбільший мультиплікативний дільник z.

Після перевірки степенів $p_j^{\,m}$, де m - показник степеня, при якому залишки $a_j = b_j = 0$, отримується остаточна формула знаходження НСД $Z = \prod_{j=1}^{k} p_j^{\,m_j}$.

Третій метод полягає у вдосконаленні методу з використанням ТЧБ Крестенсона за рахунок вилучення кроку пошуку найбільшого мультиплікативного дільника.

У порівнянні з відомим алгоритмом Евкліда, часова складність якого рівна $O1(17{,}5n(n+1)^2)$, запропонований алгоритм знаходження НСД характеризується наступними перевагами:

1. Обчислення матриць $a_j^{\,m}, b_j^{\,m}$ двох векторів по модулях $p_j^{\,m}$ виконується паралельно з використанням двох процесорів.

2. Паралельно порівнюється $X^{(n)}$ і $Y^{(n)}$, та отримується $Z = \prod_{j=1}^{k} p_j^{\,m_j}$.

У табл. 2 подано оцінки часової складності основних операцій алгоритму з використанням ТЧБ Крестенсона-Радемахера, що дозволяє зробити порівняльний аналіз вищенаведених алгоритмів пошуку найбільшого спільного дільника, а на рис. 5 показані відповідно часові складності існуючого та розроблених алгоритмів

$O(n) = \left(\log_2 n \cdot \left(\log_2 n + \frac{n}{2} + k \cdot \log_2 n \right) + n \cdot \log_2 n/2 \right)$, $O2(n) = \left(17{,}5n \cdot \left(\log_2 \frac{n}{2} \right) \right)$ і

$O3(n) = \left(\log_2 n \left(\log_2 n + k \cdot \log_2 n + \frac{n}{2} \right) + \frac{n}{2} \cdot \log_2 \frac{n}{2} \right)$.

Таблиця 2 – Часова складність основних операцій алгоритму з використанням ТЧБ Крестенсона - Радемахера

№	Основні операції	Часова складність
1.	$p_j^{\,m_j}$	$O\left(\log_2 n \cdot \left(\log_2 n + \frac{n}{2} \right) \right)$
2.	$a_j^{(n)} = res\left(\sum_{i=1}^{n-1} a_{ij} (\mathrm{mod}\ p_j^{\,m}) \right)$ $b_j^{(n)} = res\left(\sum_{i=1}^{n-1} b_{ij} (\mathrm{mod}\ p_j^{\,m}) \right)$	$O(\log_2 n/2)$
3.	$Z = \prod_{j=1}^{k} p_j^{\,m_j}$	$O(\cdot \log_2 n)$

Чисельний експеримент оцінки складностей розроблених методів пошуку НСД показує, що в діапазоні двійкових розрядів від 8 до 40 бітів, слід використовувати удосконалення реалізації алгоритму Евкліда в розмежованій системі числення Радемахера-Крестенсона, а при збільшенні розрядності чисел потрібно застосовувати метод з використанням ТЧБ Крестенсона або його удосконалення. З використанням СЗК, розроблено високопродуктивний алгоритм пошуку оберненого значення за модулем $M_i = N_i^{-1} \bmod n_i$, який є однією з основних операцій Китайської теореми про залишки (КТЗ). Суть даного алгоритму полягає в наступному: шукаємо залишок $n_i \bmod N_i = b_i$ в розмежованій системі числення Крестенсона-Радемахера. Оскільки $b_i \neq 0$, то далі виконується наступна послідовність кроків: $(n_i+1) mod\, N_i = (b_i+1) mod\, N_i = b_{i1}, (2n_i+1) mod\, N_i = (b_{i1}+1) mod\, N_i = b_{i2}, \ldots,$ $(kn_i+1) mod\, N_i = (b_{ik-1}+1) mod\, N_i = b_{ik}$ і т.д. Описана послідовність продовжується до тих пір, поки b_{ik} не стане рівним нулю. Слід зазначити, що процедура знаходження b_{ik} аналогічна визначенню залишку b_i.

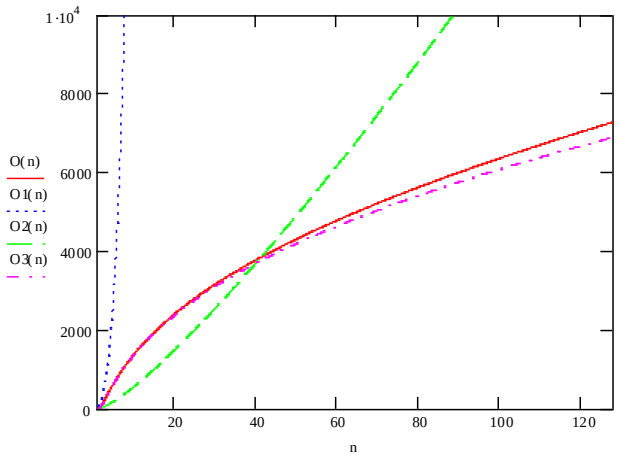

Рис. 5 – Складності існуючого та розроблених методів пошукуНСД (X, Y).

Обернений елемент $M_i = N_i^{-1} \bmod n_i$ обчислюється з результату ділення (kn_i+1) на b_i. Для уникнення цієї громіздкої операції потрібно описаним вище методом знайти залишки $S_i=(kn_i+1)\ mod\ b_i\ q_i^s$, де q_i пробігає послідовність простих чисел, $b_i\ q_i^s < (kn_i+1)$, $s=1, 2, \ldots$, причому s збільшується на 1, коли $S_i=0$. Шукане обернене число $M_i = N_i^{-1} \bmod n_i$ буде дорівнювати добутку тих q_i^s, для яких відповідні $S_i=0$.

Часову складність КТЗ визначено, як суму складностей основних трудомістких операцій пошуку залишків чисел великої розрядності, оберненого елемента за модулем та знаходження значення $x = \sum_{i=1}^{k} a_i N_i M_i \bmod n$, де k – кількість взаємно простих модулів.

Вперше побудовані аналітичні вирази характеристик часової складності відомого $O1(37k \cdot n^2 + 53{,}5k \cdot n + 17{,}5k + n^2 + 3n + 1))$ та розробленого алгоритмів КТЗ $O\left(\log_2 k \cdot (2 \cdot \log_2{}^2 n + n) + \frac{n^2 \cdot k}{2} + \log_2 n/2\right)$ (рис. 6), які складають теоретичну основу зменшення складності алгоритму Шуфа. Таким чином теоретично та експериментально доведена ефективність розроблених алгоритмів для зменшення часової складності та опрацювання інформаційних потоків в комп'ютерних мережах та системах за умови застосування ЕК.

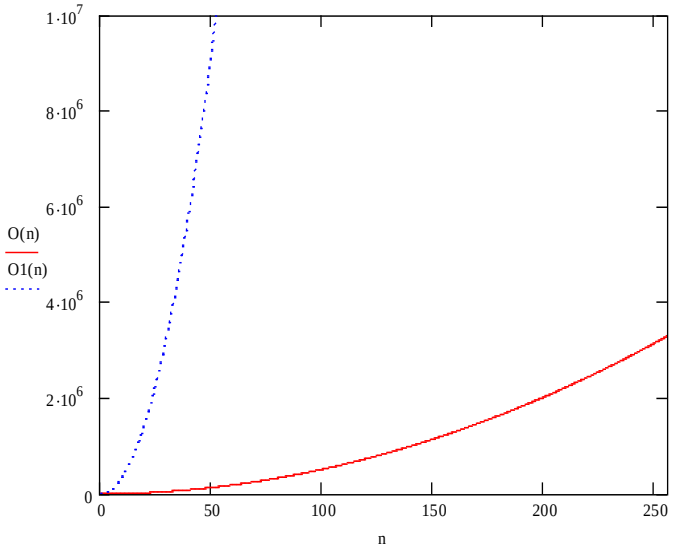

Рис. 6 – Складності розрахунку компонентів Китайської теореми про залишки.

У четвертому розділі розроблено програмні засоби пошуку параметрів ЕК, НСД двох чисел, простих та взаємно простих чисел великої розрядності, алгоритмів модулярного множення та експоненціювання, а також досліджено вплив часової складності на характеристики розроблених методів.

Побудована функціональна структура високопродуктивного спецпроцесора пошуку залишків чисел великої розрядності у розмежованій СЗК базису Крестенсона по заданому модулю.

Спецпроцесор складається з двох регістрів: RP, в який заносять модуль простого числа в доповнюючому коді $\overline{P_\partial}$, та регістра RB, де формують поточні значення залишків b_i по модулю p. В модульному блоці $\overline{P_\partial} < b_i$ виконується порозрядне порівняння коду простого числа та поточного залишку. Суматор Σ виконує функції додавання доповнюючого коду $\overline{P_\partial}$ і поточного залишку b_i. Блок управління (БУ) формує синхронізуючі сигнали snx, які тактують зсуви зчитування інформації з регістрів RP і RB. Модуль $\overline{P_\partial} = b_i$ виконує порівняння доповнюючого коду простого числа $\overline{P_\partial} - 1 = \overline{P}$ з поточним значенням b_i (рис. 7). Блок управління формує управління окремими модулями спецпроцесора, які мають наступну інтерпретацію:

(start)
y_s) RP:=0, RB:=0, $Z_i = 0$;
y_0) RP:= $P_{(0)}$;
y_1) $Z_i = Z_{i+1}$, $P_{(0)} > b_i$;
y_2) $\Sigma := P_{(0)} + b_i$;
y_3) stop:=1, $\overline{P} := b_i$.
y_4) RB:= b_i +.
stop.

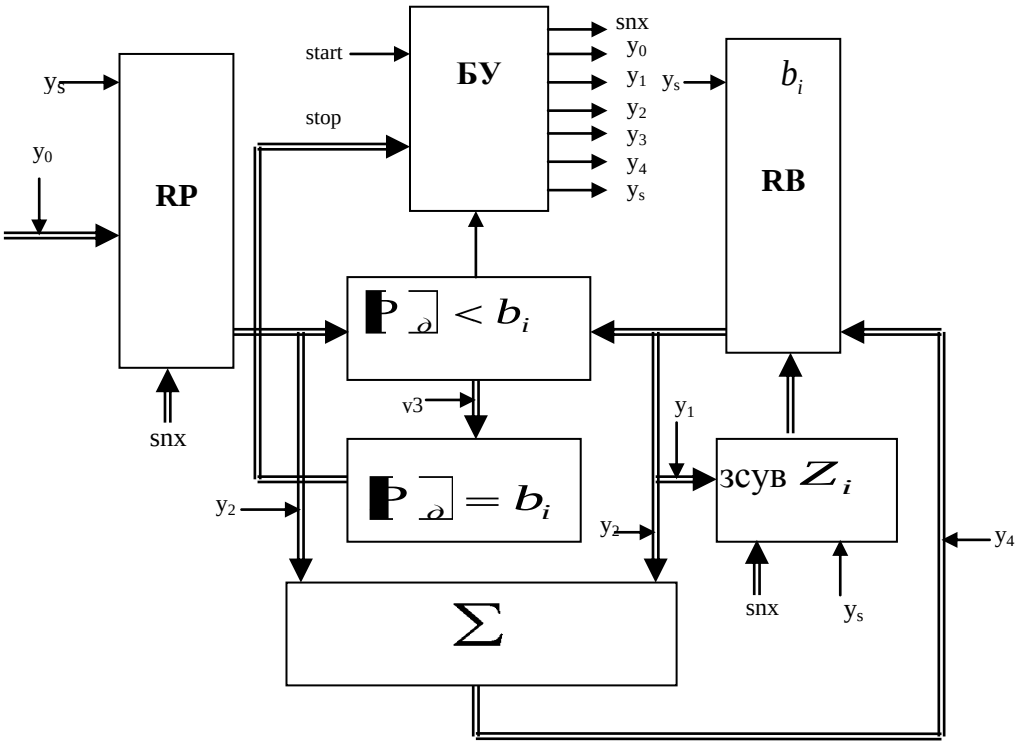

Рис. 7 – Структура спецпроцесора пошуку залишків чисел великої розрядності по заданому модулю

Розроблений спецпроцесор призначено для виконання операцій над великорозрядними двійковими числами $n > 2^{10} - 2^{32}$, його реалізацію доцільно виконати на основі регістрів кристалів флеш-пам'яті, яка характеризується високою частотою зчитування 1-2 ГГц та достатнім об'ємом пам'яті порядку 128-256 Гбайт. Отримано аналітичні вирази швидкодії $V(n)$, $V1(n)$ та $V2(n)$ (кількість залишків з розрядністю n за 1 с) спецпроцесорів, реалізованих відповідно в унітарному базисі, базисах Радемахера та Крестенсона-Радемахера: $V(n) = 1/n$, $V1(n) = 2^{\log_2 p - n}$, $V2(n) = 2^{40-2n}$ (рис.8), де p - модуль.

Отже, апаратна складність буде обчислюватися згідно наступного співвідношення:

$$P(n) = F(Ф + ЦК + \Sigma + РЗ + БУ), \qquad (7)$$

де $Ф$ - апаратна складність флеш-пам'яті, $ЦК$ - апаратна складність цифрового компаратора; Σ - апаратна складність суматора; $РЗ$ – апаратна складність регістру зсуву; $БУ$ – апаратна складність блоку управління.

Оскільки, $ЦК+\Sigma+РЗ+БУ= C_A=const$, тоді загальна апаратна складність з врахуванням коефіцієнту апаратної складності флеш-памяті буде:

$$P(n) = F \cdot \log_2 n + C_A, \qquad (8)$$

де n - розрядність числа (рис.9).

Реалізація спецпроцесора пошуку залишків великорозрядних чисел по модулю виконана на базі платформи, яка оснащена модулем інтерфейсу PCI, що дозволяє імплементовувати її в існуючі обчислювальні системи, як окремий

елемент. Особливістю даної платформи є сумісне використання ПЛІС XilinxSpartanIII та AlteraCyclone, які мають доступ до спільної оперативної пам'яті SRAM розміром 16 Мбайт, що дозволяє провести дослідження та аналіз системних характеристик спецпроцесора на різних кристалах.

Результати дослідження показали, що розроблений спецпроцесор забезпечує підвищення швидкодії пошуку залишків великорозрядних чисел на 2-3 порядки. На структуру розробленого спецпроцесора подана заявка на патент.

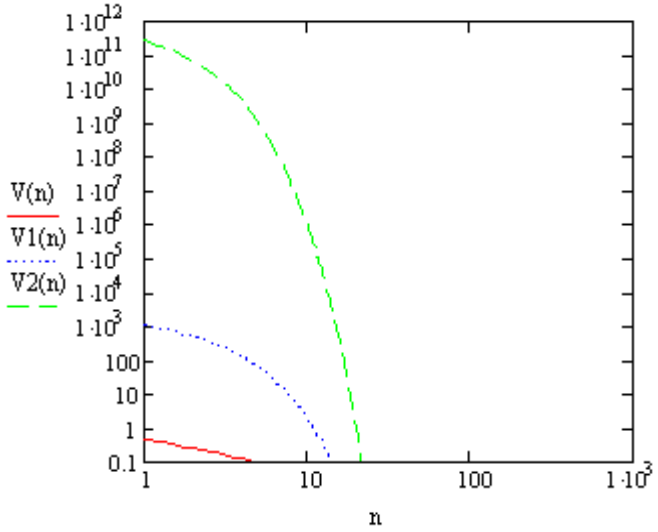

Рис. 8 – Швидкодія розглянутих пристроїв пошуку залишків по модулю

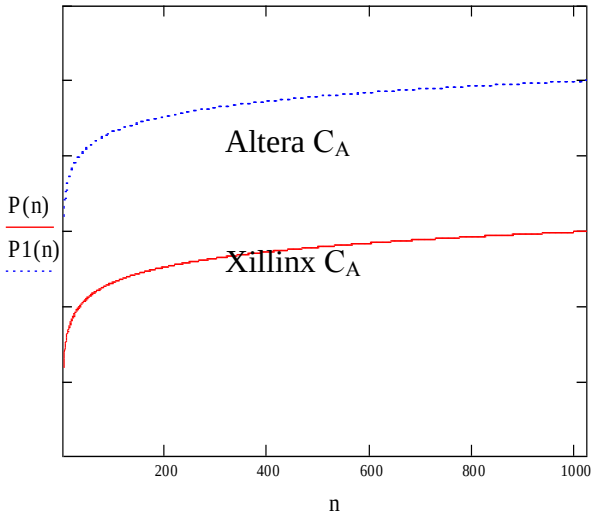

Рис. 9 – Апаратна складність спец процесора.

Експериментальний зразок високопродуктивного спецпроцесора визначення залишків чисел великої розрядності реалізовано на платі XilinxSpartanIII та AlteraCyclone і передано ТОВ ТКБР «Стріла» в якості компоненти процесу шифрування та дешифрування інформаційних потоків дистрибутивних та корпоративних комп'ютерних мереж.

У додатках наведено лістинг програмних модулів для генерування параметрів та базових точок ЕК згідно розроблених алгоритмів та схеми основних компонентів спеціалізованого процесора пошуку залишків великорозрядних чисел по заданому модулю в середовищі ISIS Professional. Подані документи про використання результатів дисертаційної роботи.

ВИСНОВКИ

У дисертаційній роботі розв'язано наукову задачу розробки методів та алгоритмів опрацювання інформаційних потоків у КМ за умови використання ЕК. При цьому отримані наступні результати:

1. Проаналізовані і досліджені архітектури та трафіки КМ на основі оцінки їх емерджентності. Показано, що найбільш перспективною архітектурою мережевих технологій опрацювання інформаційних потоків є зірково-магістральна.

2. Виконано систематизацію системних об'єктів та аналітичних моделей комп'ютерних систем. Обґрунтовано ефективність застосування ТЧБ Радемахера

та Крестенсона для зменшення часової складності формування ІП та захисту від несанкціонованого доступу.

3. Розроблено метод модулярного множення та експоненціювання з використанням матрично-модульних перетворень ТЧБ Радемахера-Крестенсона. На відміну від відомих, які побудовані на швидкому перетворенні Фур'є та на основі десяткової системи числення, ефективність запропонованого методу при розрядності чисел до 64 бітів стрімко зростає на 1 порядок за рахунок заміни багататактної операції множення у базисі Радемахера матрично-модульною операцією сумування в базисі Крестенсона і на 20% при n>64біт.

4. Розроблено метод та теоретичні основи матрично-модульних перетворень з використанням системи числення залишкових класів Крестенсона, ТЧБ Крестенсона-Радемахера та критерії їх ефективного застосування в алгоритмі Шуфа.

5. Отримано аналітичні вирази характеристик складності формування та опрацювання ІП за умови застосування ЕК, які склали теоретичну основу спрощення часових компонентів алгоритму Шуфа та дозволили експоненційну складність привести до лінійної або квадратичної складності.

6. Побудовано та досліджено нові швидкі перетворення базису Радемахера в базис Крестенсона, на основі застосування системи числення залишкових класів, ТЧБ Крестенсона-Радемахера та розмежованої системи числення Крестенсона-Радемахера розроблено алгоритми пошуку НСД двох чисел, простого числа, елементів Китайської теореми про залишки, які забезпечують підвищення швидкодії та зниження часової складності на 1-2 порядки.

7. Розроблено та реалізовано програмно-апаратні засоби опрацювання біторієнтованих ІП, які характеризуються великою розрядністю та лінійно-квадратичною складністю в порівнянні з експоненційною для існуючих алгоритмів.

СПИСОК ОПУБЛІКОВАНИХ ПРАЦЬ ЗА ТЕМОЮ ДИСЕРТАЦІЇ

1. Касянчук М. М. Теорія алгоритмів перетворень китайської теореми про залишки в матрично-розмежованому базисі Радемахера-Крестенсона / М. М. Касянчук, Я. М. Николайчук, І. З. Якименко // Вісник національного університету «Львівська політехніка». – 2011. – № 688. – С. 118–124.

2. Касянчук М. М. Теорія алгоритмів пошуку найбільшого спільного дільника у базисі Крестенсона / Касянчук М., Якименко І., Николайчук Я. // Вісник ТНТУ. — 2011. – Том 16. – № 1. – С. 154–161.

3. Касянчук М. М. Теорія алгоритмів RSA та Ель-Гамаля в розмежованій систмі числення Радемахера-Крестенсона// М. М. Касянчук, І. З. Якименко, О. І. Волинський, І.Р. Пітух / Вісник Хмельницького національного університету. – 2011. – № 3. – С. 265–273.

4. Касянчук М. М. Теорія та оптимізація алгоритмів опрацювання

великорозрядних чисел у базисі Крестенсона / М. М. Касянчук, І. З. Якименко, С. В. Івасьєв// Вісник Хмельницького національного університету. – 2011. – № 3. – С. 265–273.

5. Якименко І. З. Порівняння часових характеристик виконання базових криптографічних операцій на еліптичній та гіпереліптичній кривих/ Якименко І. З.// Праці Луганського відділення Міжнародної Академії інформатизації. – 2008. – № 1 (16). – С. 127–134.

6. Якименко І. З. Фундаментальні основи структуризації та опрацювання інформаційних потоків в комп'ютерних мережах / Якименко І. З. // Вісник Хмельницького національного університету. – 2011. – № 2. – С. 131–138.

7. Карпінський М. Метод генерування параметрів еліптичних кривих / М. Карпінський, І. Васильцов, І. Якименко, Я. Кінах // Правове, нормативне, та метрологічне забезпечення системи захисту інформації в Україні, Київ. – 2003. – Випуск 6. – С. 74–77.

8. Карпінський М. П. Показники оцінки ефективності алгоритмів шифрування на еліптичних кривих. /Карпінський М. П., Васильцов І. В., Якименко І. З.// Правове, нормативне, та метрологічне забезпечення системи захисту інформації в Україні, Київ. – 2004. – Випуск 8. – С. 121–124.

9. Карпінський М. П. Оцінка продуктивності та стійкості до часового аналізу алгоритмів експоненціювання точки еліптичної кривої / Карпінський М. П., Якименко І. З., Гіжицкі М.// Вісник Хмельницького національного університету. – 2006. – № 5. – С. 23–30.

10. Карпінський М. Використання технології паралельних обчислень для рахування кількості точок еліптичної кривої / М. П. Карпінський, І. З. Якименко, А. А. Хомінчук // Вісник Східноукраїнського національного університету імені Володимира Даля. – 2008. – № 8 (126), Частина 1. – С. 207–210.

11. Кінах Я. І Удосконалення мережевих криптоаналітичних алгоритмів на еліптичних кривих / Я. І. Кінах, І. З. Якименко //Вісник Східноукраїнського національного університету імені Володимира Даля. – № 6(136), Т. 1. – 2009.– С. 48–51.

12. Карпінський М. П. Використання символів Якобі в криптографії ЕК / М. П. Карпінський, І. З. Якименко, А. А. Хомінчук // Матеріали III Міжнародної науково-технічної конференції: Світ інформації та телекомунікацій-2006, Україна. – Київ: ДУІКТ, 2006. – С. 208.

13. Kinakh I. Reliability of Schoof Algorithm and its Computational Complexity. /Kinakh Y., Yakymenko I. // Proceedings of the Xth International Conference: The Experience of Designing and Application of CAD Systems in Microelectronics. – Lviv-Polyana. – 2009. – С. 107.

14. Якименко І. З. Апаратна імплементація помножувачів для криптографії еліптичних кривих / І. З. Якименко, Ю. М. Чайківська // Міжнародний науково-технічний журнал «Інформаційні технології та комп'ютерна інженерія, Вінниця.–

2009. – С. 18–24.

15. Кінах Я. І. Оцінка ефективності інформаційної стійкості алгоритмів шифрування на еліптичних кривих / Я. І. Кінах, І. З. Якименко, У. Яциковська // Матеріали VII Міжнародної науково-практичної конференції: Проблеми впровадження інформаційних технологій в економіці. – Ірпінь: НУДПС України, 2009. – С. 249–252.

16. Kasyanchuk M. Matrix Algorithm of Processing of the Information Flow in Computer Systems Based on Theoretical and Numerical Krestenson's Based / M. Kasyanchuk, I. Iakymenko, Y. Nykolajchuk // Modern Problems of Radio Engineering, Telecommunications and Computer Science. Proceedings of the International Conference. TCSET'2010. – Lviv-Slavsko, Ukraine. – 2010. – P. 241.

17. Касянчук М. М. Теоретичні основи аналітики та алгоритми оптимізації обчислень простих чисел / М. М. Касянчук, І. З. Якименко, О. І. Волинський, С. В. Івасьєв // Поступ в науку: зб. наук. праць за матеріалами міжнародної проблемно-наукової міжгалузевої конференції [«Інформаційні проблеми комп'ютерних систем, юриспруденції, енергетики, економіки, моделювання та управління», (ПНМК–2010)], (Бучач – Яремча, 01–04 червня 2010 р.) / НАН України, Академія правових наук України [та ін.]. – Бучач: Бучацький інститут менеджменту і аудиту. – 2010. – С. 33–37.

18. Волинський О. І. Розмежована система числення залишкових класів та спецпроцесори на її основі / О. І. Волинський, І. З. Якименко // Поступ в науку: зб. наук. праць за матеріалами міжнародної проблемно-наукової міжгалузевої конференції [«Інформаційні проблеми комп'ютерних систем, юриспруденції, енергетики, економіки, моделювання та управління», (ПНМК–2010)], (Бучач – Яремча, 01–04 червня 2010 р.) / НАН України, Академія правових наук України [та ін.]. – Бучач: Бучацький інститут менеджменту і аудиту. – 2010. – С. 80–84.

АНОТАЦІЯ

Якименко І. З. Методи та алгоритми опрацювання інформаційних потоків в комп'ютерних мережах за умови застосування еліптичних кривих. – Рукопис.

Дисертація на здобуття наукового ступеня кандидата технічних наук за спеціальністю 05.13.05 – комп'ютерні системи та компоненти. – Тернопільський національний економічний університет, Тернопіль, 2012.

В дисертаційній роботі вперше розроблено методи, отримано аналітичні вирази характеристик часової складності та розроблено високопродуктивні алгоритми опрацювання ІП у КМ за умови застосування ЕК на основі модульно-матричних операцій в ТЧБ Радемахера-Крестенсона, які склали теоретичну основу зменшення часової складності компонентів алгоритму Шуфа, що на відмінно від існуючих дозволили зменшити часову складність з експоненційної до лінійної або лінійно-логарифмічної.

Отримали подальший розвиток методи захисту ІП з використанням ЕК на основі генерування їх параметрів, що дозволило зменшити часову складність алгоритмів пошуку залишків чисел великої розрядності, знаходження НСД, модулярного множення, експоненціювання та пошуку оберненого елементу за модулем за рахунок використання ТЧБ Радемахера – Крестенсона, що дозволило зменшити на 1-2 порядки часову складність базових операцій алгоритму Шуфа.

Розроблено високопродуктивні програмно-апаратні засоби реалізації модульних операцій над числами великої розрядності та розроблено схемотехнічні рішення відповідних спеціалізованих процесорів.

Результати досліджень використані в навчальному процесі на кафедрах комп'ютерної інженерії та спеціалізованих комп'ютерних систем при викладанні дисциплін: «Комп'ютерні системи», «Захист інформації в комп'ютерних системах», «Проектування спеціалізованих комп'ютерних систем», а також впроваджені на ТОВ ТКБР «Стріла» для захисту інформаційних потоків в дистрибутивних та корпоративних комп'ютерних мережах.

Ключові слова: часова складність, теоретико-числові базиси Радемахера-Крестенсона, еліптична крива, алгоритм Шуфа, модулярне множення, модулярне експоненціювання, найбільший спільний дільник, обернений елемент за модулем.

АННОТАЦИЯ

Якименко И. З. Методы и алгоритмы обработки информационных потоков в компьютерных сетях при условии применения эллиптических кривых. – Рукопись.

Диссертация на соискание ученой степени кандидата технических наук по специальности 05.13.05 – компьютерные системы и компоненты. – Тернопольский национальный экономический университет, Тернополь, 2012.

В диссертационной работе представлены теоретические обоснования и новые решения научной задачи разработки и усовершенствования методов повышения эффективности и уменьшения временной сложности программно-аппаратной реализации алгоритмов обработки информационных потоков при условии применения эллиптических кривых.

Впервые предложены методы обработки информационных потоков в компьютерных сетях при условии применения эллиптических кривых на основе матричных спецпроцесорных программно-аппаратных средств, что в отличии от существующих позволяют путем применения теоретико-числового базиса Радемахера-Крестенсона уменьшить временную сложность с полиномиальной к линейной или линейно-логарифмической.

Полученные аналитические выражения характеристик временной сложности формирования и обработки информационных потоков при условии применения ЭК с использованием системы счисления остаточных классов Радемахера-Крестенсона, которые составили теоретическую основу уменьшения временной

сложности компонентов алгоритма Шуфа, что создало возможности повышения уровня защиты ИП в современных и проектируемых компьютерных сетей. Разработаны теоретические основы матрично-модульных операций модулярного умножения и экспоненцирования путем использования ТЧБ Рademахера-Крестенсона, что позволило уменьшить временную сложность алгоритма поиска порядка эллиптической кривой.

Получил дальнейшее развитие метод защиты информационных потоков в компьютерных сетях с использованием эллиптических кривых на основе генерирования их параметров, что позволило уменьшить временную сложность алгоритмов поиска остатков чисел большой разрядности, нахождения наибольшего общего делителя, модулярного умножения, экспоненцирования и поиска обратного элемента по модулю за счет использования ТЧБ Крестенсона и Рademахера.

Разработаны методы модулярного умножения и экспоненцирования, поиска наибольшего общего делителя и обратного элемента по модулю, путем использования разработанного математического аппарата матрично-модульных операций в базисе Крестенсона-Рademахера, что позволило уменьшить на 1–2 порядка временную сложность базовых операций алгоритма Шуфа.

Предложены аппаратные средства реализации модульных операций над числами большой разрядности и разработаны схемотехнические решения соответствующих специализированных процессоров.

Разработаны алгоритмы, программные пакеты формирования параметров на основе генетического алгоритма и алгоритма с использованием символов Якоби, базовых точек эллиптических кривых и специализированные высокопроизводительные программно-аппаратные средства обработки информационных потоков в компьютерных сетях, а также алгоритмы распараллеливания задач обработки информационных потоков компьютерными средствами на основе ТЧБ Крестенсона. Результаты исследований использованы в учебном процессе кафедр компьютерной инженерии и специализированных компьютерных систем при преподавании дисциплин: «Компьютерные системы», «Проектирование специализированных компьютерных систем», «Защита информации в компьютерных системах», а также внедрены на ООО ТКБР "Стрела" для защиты информационных потоков в дистрибутивных и корпоративных компьютерных сетях.

Ключевые слова: временная сложность, теоретико-числовые базисы Рademахера-Крестенсона, эллиптическая кривая, алгоритм Шуфа, модулярное умножение, модулярное экспоненцирование, наибольший общий делитель, обратный элемент по модулю.

ANNOTATION

Yakymenko I. Z. Methods and Algorithms for Processing of Information Flow in Computer Networks with using Elliptic curves. – Manuscript.

Thesis for the Candidate's degree of engineering science in specialty 05.13.05 – computer systems and components. – Ternopil National Economic University, Ternopil, 2012.

In the dissertation paper presents theoretical justification and new solutions of development and improvement scientific problems of efficiency increasing methods and time complexity reducing of software and hardware implementation of processing data flows algorithms in case, when used EC.

In first proposed methods, derived analytical expressions of temporal characteristics of complexity and processing algorithms, which developed high information flow in computer networks, in case of elliptic curves using based on modular-matrix operations in TDB Rademacher-Krestenson, which passed the theoretical basis for reducing time complexity of Schoof algorithm components and allowed to reduce the time complexity from exponential to linear or quadratic.

Information providing of computerized system for the stability measurement of EC Schoof algorithm, based on parallelization process subtasks optimization had been improved, thus improving the assessment accuracy of resistance level of information flow in existing and created computer networks.

The methods of protecting information flows using the EC, based on generation of their parameters, received further development, thus allowing to reduce the time complexity of search algorithms remains large numbers, finding the greatest common divisor, modular multiplication, exponentiation and finding the inverse element for the module by using TDB Rademacher–Krestenson which allowed to reduce by 1–2 orders of time complexity of Schoof algorithm basic operations.

A high-performance software and hardware implementations of modular operations realisation on large numbers had been developed and designed circuit solution of the corresponding processors.

Results of the research used in the educational process at Department of Computer Engineering and Specialized Computer System at teaching subjects: "Computer Systems", "Research and design of computer systems and networks", "Information protection in computer systems", "Design of specialized computer systems and implemented on Ltd. TKBR "Strila" for the information flow protecting in distributed and corporate computer networks.

Keywords: time complexity, theoretical and numerical bases of Rademacher-Krestenson, elliptic curve, Schoof algorithm, modular multiplication, modular exponentiation, the greatest common divisor, inverse element for the module.