МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ТЕРНОПІЛЬСЬКИЙ НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ
ІМЕНІ ІВАНА ПУЛЮЯ

Літава Гжегож Владислав

УДК 004.9:004.056:681.51

МОДЕЛІ ТА ЗАСОБИ ПІДВИЩЕННЯ ЖИВУЧОСТІ ІНФОРМАЦІЙНО-УПРАВЛЯЮЧИХ СИСТЕМ НА ОСНОВІ ЕЛІПТИЧНИХ КРИВИХ

05.13.06 – інформаційні технології

Автореферат
дисертації на здобуття наукового ступеня
кандидата технічних наук

Тернопіль – 2015

Дисертацією є рукопис.
Робота виконана в Тернопільському національному технічному університеті імені Івана Пулюя Міністерства освіти і науки України

Наукові керівники — доктор технічних наук, професор **Карпінський Микола Петрович,** професор кафедри комп'ютерних наук Тернопільського національного технічного університету імені Івана Пулюя (м. Тернопіль, Україна);

кандидат технічних наук **Алєксандер Марек Богуслав** директор технічного інституту Державної вищої професійної школи у Новому Сончі (м. Новий Сонч, Польща).

Офіційні опоненти: д.т.н., професор **Козлюк Ірина Олексіївна,** професор кафедри телекомунікаційних систем Інституту аеронавігації Національного авіаційного університету (м. Київ, Україна);

д.т.н, професор **Петров Олександр Степанович**, професор кафедри прикладної інформатики Краківської гірничо-металургійної академії ім. С. Сташіца (м. Краків, Польща).

Захист відбудеться 31 березня 2015р. о 13 год., ауд. 79, на засіданні спеціалізованої вченої ради К 58.052.06 в Тернопільському національному технічному університеті імені Івана Пулюя, 46001, м.Тернопіль, вул. Руська, 56.

З дисертацією можна ознайомитись у бібліотеці Тернопільського національного технічного університету імені Івана Пулюя, 46001, м.Тернопіль, вул. Руська, 56.

Автореферат розісланий “26” лютого 2015 р.

Учений секретар
кандидат технічних наук, доцент Фриз М. Є.

ЗАГАЛЬНА ХАРАКТЕРИСТИКА РОБОТИ

Актуальність теми. Розвиток економічного потенціалу кожної країни нерозривно пов'язаний з техногенною безпекою. Для її забезпечення одним з ключових чинників являються інформаційні технології (ІТ), як інструмент для розробки та впровадження систем управління гарантоздатності критично важливої інфраструктури. На сьогоднішній день щораз більше уваги приділяється захисту інформації та конфіденційності. Нехтування додатковими дефіцитами гарантоздатності, такими як інформаційно-управляючі системи (ІУС), може призвести до що п’ятої відмови атомного енергетичного обладнання і що п'ятої аварії космічно-ракетної техніки, з тенденцією їх зростання за останні роки. Цій темі притаманний міжнародний характер та її розгляду присвячено низку міжнародних конференцій, пов’язаних з гарантоздатністю, зокрема з її складовими – живучістю та функціональною безпекою ІТ: DESSERT, DSN, EDCC, ESREL, SAM, SAFECOMP, тощо. Важливим питанням є дослідження спеціальних режимів функціонування ІУС з точки зору їх живучості, які, у поєднанні з розвитком комплексних інтегрованих дистанційних сенсорів, належать до одного з провідних наукових напрямів найбільших інженерних викликів XXI століття, визначених науковим фондом NSF, а також передбачених до виконання згідно з Постановою Президії НАН України. Доцільно виділити окремий клас ІУС, що базуються на еліптичних кривих (ІУСЕК), тобто ІУС, в пристроях яких застосовуються обчислювальні операції на еліптичних кривих (ЕК), включаючи Elliptic Curve Cryptography Device (ECCD або криптографічні пристрої на ЕК), що веде до необхідності удосконалення, опрацювання і впровадження відповідних моделей живучості ІУСЕК.

Істотним завданням постає оцінювання та підвищення живучості ІУСЕК, а також самих алгоритмів шифрування. Від криптографічних пристроїв вимагається також можливість шифрування та розшифрування в реальному часі. Крім цього, не слід скидати з рахунків одну з основних проблем безпеки, яка зводиться до розв’язання задачі дискретного логарифмування. Кожне збільшення швидкості виконання основних обчислень на ЕК зумовлює скорочення часу, необхідного для знаходження цього логарифму. Одним з основних факторів, який визначає ефективність обчислювальних методів, моделей та технологій не тільки щодо швидкості шифрування/розшифрування, а також непрямо рівень гарантоздатності ECCD і відповідно параметри живучості ІУСЕК, є швидкодія додавання точок на ЕК, від якої безпосередньо залежить час, необхідний для розв’язання дискретного логарифма. З огляду на це, удосконалення моделей та засобів ІУС, що базуються на пристроях для виконання криптографічних операцій на ЕК, для підвищення живучості цих систем є актуальною науковою задачею, що має важливе наукове та практичне значення.

Зв’язок роботи з програмами, планами, науковими темами. Дисертаційна робота виконувалася у Тернопільському національному технічному університеті імені Івана Пулюя (ТНТУ ім. І. Пулюя) за держбюджетним договором на виконання науково-дослідних робіт за темою "Розробка, дослідження та впровадження методів і засобів контролю та управління якістю програмних продуктів" (ДР № 0113U000258) (2012-2013 рр., виконавець).

Мета і задачі дослідження. Метою дисертації є удосконалення моделей та засобів для підвищення живучості інформаційно-управляючих систем на основі еліптичних кривих.

Досягнення цієї мети вимагає розв’язання наступних завдань:

1. Провести аналіз моделей живучості, засад побудови та технологічних рішень ІУСЕК з точки зору їх адекватності та можливого використання для розв’язання поставленої задачі.

2. Здійснити вибір обчислювальних платформ і розробити, ґрунтуючись на ефективних методах розв'язання дискретного логарифма, моделі засобів та технології обчислень на ЕК *GF(p)* у пристроях ІУСЕК з врахуванням дефектів зовнішніх впливів.

3. Створити апаратно-програмні засоби для виконання обчислень на ЕК *GF(p)* і розв’язання дискретного логарифма вищої швидкодії для живучих ІУСЕК.

4. Дослідити вплив методів виконання основних операцій на ЕК над скінченним полем вищих порядків *GF(p)* на параметри живучості ІУСЕК для кожної з опрацьованих моделей та обчислювальних технологій.

5. Провести симуляційні дослідження (імітаційне моделювання) для верифікації отриманих теоретичних залежностей щодо живучості ІУСЕК та реалізувати імплементацію запропонованих рішень в практиці.

Об'єкт дослідження – процеси моделювання оцінки живучості інформаційно-управляючих систем на основі еліптичних кривих.

Предмет дослідження – моделі та засоби забезпечення живучості інформаційно-управляючих систем на основі еліптичних кривих.

Методи досліджень. Теорія ЕК, теорія математичного моделювання, теорія алгебри та теорія криптографії для створення технологій обчислень й побудови моделей пристроїв ІУСЕК на основі ЕК над полем вищих порядків, оцінювання рівня живучості таких систем, розроблення апаратно-програмних засобів для ефективних обчислень на ЕК і розв’язання задачі дискретного логарифмування для визначення рівня живучості ІТ, що забезпечується пристроями захисту на основі ЕК.

Наукова новизна дисертації.

1. Удосконалено структурну модель підвищення живучості ІУСЕК з врахуванням дефектів зовнішніх впливів за ознаками ймовірності та детермінованості, що дало змогу створити підґрунтя для проектування ефективних засобів цих систем.

2. Удосконалено технології обчислень на ЕК шляхом заміни множення за модулем в алгоритмі Крестенсона, що дало змогу звести множення до операції додавання, яка відрізняється від відомих новою архітектурою і меншою складністю у порівнянні з підходом, який ґрунтується на традиційному множенні, завдяки чому збільшено швидкість обчислень і прискорено дію алгоритму розв’язання задачі дискретного логарифмування у пристроях ІУСЕК.

3. Вперше одержано модифіковані моделі засобів обчислень на ЕК у пристроях ІУСЕК з врахуванням дефектів зовнішніх впливів на них, що дозволило по-новому визначити розмір кривих, які застосовуються в інтегрованих інформаційних системах, і забезпечити підвищену ефективність засобів протидії потенційним впливам.

4. Вперше, ґрунтуючись на алгоритмі модульного множення в теоретико-числових базисах (ТЧБ) Радемахера-Крестенсона щодо розв’язання дискретного логарифму, розроблено моделі, технології та структури засобів обчислень на ЕК в ІУСЕК для виконання криптографічних операцій, завдяки чому здійснено верифікацію параметрів живучості ІУСЕК та доведення збільшення його рівня.

Практичне значення отриманих результатів. На підставі отриманих теоретичних результатів розроблено математичні моделі, технології і засоби обчислень на ЕК вищих порядків, які можуть використовуватися для підвищення живучості ІУСЕК, а також вибору відповідних ЕК, які забезпечують функціонування ІУСЕК в аномальних умовах, викликаних дефектами зовнішніх впливів на неї.

На основі запропонованих моделей та технологій обчислень створено, з імплементацією в середовищі програмованих користувачем вентильних матриць FPGA (Field Programmable Gate Array), апаратні засоби для реалізації стежок блукання ро-алгоритму Полларда, які використано складовою частиною комплексної апаратно-програмної системи розв’язання дискретного логарифма на ЕК, що дало змогу отримати відомості про параметри живучості засобів ІУСЕК.

Практична цінність роботи полягає в тому, що на отриманій експериментальній базі модельованої атаки на ІУСЕК визначено час захисту засобів в залежності від розміру застосованих кривих, завдяки чому оцінено максимальне зростання ризику в короткостроковій перспективі, ґрунтуючись на особливостях симульованих дефектів впливу і даних щодо підвищення продуктивності нових апаратних рішень. Це також забезпечило вибір оптимальних розмірів ЕК в спеціалізованих рішеннях, де важливим є компроміс між обчислювальною потужністю та рівнем захисту з врахуванням часу, протягом якого даний засіб повинен бути живучим.

Додатковим фактором практичної цінності роботи є здійснення додавання точок та реалізації ро-алгоритму Полларда за допомогою створеної системи, побудованої на основі програмованих матриць FPGA типу Stratix III, завдяки чому забезпечено високу швидкодію і втричі зменшено час, необхідний для розв’язання дискретного логарифма на тій самій кривій, в порівнянні з програмною системою, яка працює на процесорі типу Itanium2. Побудовано паралельну систему, в якій швидкість зростає пропорційно до кількості застосованих програмованих матриць FPGA, здійснено також перенесення і симуляцію функціонування заімплементованої моделі на кластері FPGA (120 компонентів), який базується на програмованій матриці серії Virtex-4.

Теоретичні та практичні результати дисертаційної роботи використані та впроваджені: при виконанні науково-дослідної роботи "Розробка, дослідження та впровадження методів і засобів контролю та управління якістю програмних продуктів" (ДР № 0113U000258), що виконувалася в ТНТУ ім. І. Пулюя, ТОВ “Шредер” для повноцінного функціонування ІУС із збереженням їх живучості за наявності потенційних загроз, захисту ІУС від несанкціонованого доступу і підвищення відмовостійкості та продуктивності ІУС, а також у навчальному процесі ТНТУ ім. І. Пулюя в курсах „Технології захисту інформації”, “Інформаційна безпека” та Державної вищої професійної школи у Новому Сончі, Польща (ДВПШ)

при викладанні дисциплін “Безпека інформаційних технологій”, “Криптографія і теорія кодів” та “Мережеві технології”, згідно з Договором про співпрацю між ДВПШ і ТНТУ ім. І. Пулюя.

Особистий внесок здобувача. Основний зміст роботи, всі основні наукові положення, теоретичні та практичні розробки, висновки та рекомендації виконані автором особисто. В друкованих працях, опублікованих в співавторстві, здобувачеві належать: [1] – побудовано і впроваджено структуру, виконано функціональну симуляцію і проведено верифікацію живучості ІУСЕК за допомогою системи, яка реалізує розв’язання дискретного логарифма на ЕК вищих рядів *GF(p)*, ґрунтуючись на паралельному ро-алгоритмі Полларда із застосуванням модульного множення на підставі ТЧБ Радемахера-Крестенсона, реалізованого на програмованих матрицях типу Stratix III, [2] – удосконалено модель обчислень на ЕК вищих порядків шляхом введення в основні операції на ЕК вищих порядків модульного множення, що ґрунтується на ТЧБ Радемахера-Крестенсона, та паралельного додавання, [3] – одержано модифіковані моделі живучості ІУСЕК з врахуванням атак на них, [5] – проведено тестування системи безпечної передачі даних в телекомунікаційній мережі та виконано аналіз отриманих результатів, [6] – сформульовано та обґрунтовано підхід з використанням паралельного додавання і ТЧБ Крестенсона до виконання основних операцій на ЕК *GF(p)* та застосування їх у реалізації паралельного ро-алгоритму Полларда за допомогою програмованих матриць FPGA, [7] – розроблено моделі та технології обчислень на ЕК у пристроях ІУСЕК для виконання криптографічних операцій, [8] – виконано симуляційні дослідження для верифікації отриманих теоретичних залежностей щодо живучості ІУСЕК, [9] – проаналізовано безпеку передавання інформації в комп'ютерних мережах, під час якого застосовано методи шифрування на базі ЕК, [11] – доведено доцільність застосування моделі, в якій використано гаусівські нормальні базиси, для виконання обчислень на ЕК в апаратних рішеннях, базованих на програмованих матрицях FPGA, для дослідження живучості ІУС, що ґрунтуються на ЕК другого порядку *GF(2^m)*, [13] – розроблено паралельні розподілені системи на основі бібліотек MPI2 і MIRACL для оцінювання часу розв’язування задачі дискретного логарифмування на ЕК в багатопроцесорних середовищах.

Апробація результатів дисертації. Основні положення і результати дисертаційної роботи доповідалися та обговорювалися на: Дванадцятій науковій конференції ТНТУ ім. І. Пулюя (14-15 травня 2008, Тернопіль), 9th International Workshop “Computational Problems of Electrical Engineering” (CPEE’08) (September 16-20, 2008, Alushta (Crimea), Ukraine), ІІІ Міжнародній Науковій Конференції з циклу Інформатика в XXI столітті. Інформаційні технології в науці, техніці та інформатиці (Радом, Польща, 2009 р.), Xth International Conference “The Experience of Designing and Application of CAD Systems in Microelectronics” (CADSM 2009) (Львів-Поляна, 2009), International Science-Practical Conference «Information Technologies and Security in Administration» (ITSM’2008-ITSM’2012) (Crimea, 2008-2012), Науковому семінарі НАН України «Технічні засоби захисту інформації» (Одеське відділення) (2013), ІІІ Міжнародній науково-технічній конференції «Захист інформації і безпека інформаційних систем» (05-06 червня 2014 р., Львів, Україна).

Наукові результати дисертаційної роботи розглядалися та обговорювалися в Державному технологічному університеті (м. Черкаси), Університеті в Бєльську-Бялій (Польща), ДВПШ у Новому Сончі. В цілому роботу апробовано у ТНТУ ім. І. Пулюя, Східноукраїнському національному університеті ім. В. Даля (м. Луганськ), Державному економічному університеті (м. Одеса).

Публікації. Основні результати дисертаційних досліджень опубліковані у 14 наукових роботах: 8 із них – наукові статті, серед яких 6 ([1-3, 6, 7, 11]) – статті у наукових фахових виданнях України, 2 наукові статті ([8, 14]) – у провідних закордонних журналах, які входять до міжнародних наукометричних баз (IEEE, Inspec, Scopus, UlrichsWeb, Index Copernicus, Google Scholar, Baztech, ISI Master Journal List тощо), 2 розділи у закордонній монографії ([4, 5]), а також 4 публікації в матеріалах конференцій.

Структура та обсяг дисертації. Дисертаційна робота складається із вступу, чотирьох розділів, висновків, списку використаних джерел із 119 найменувань і додатків. Загальний обсяг дисертації становить 142 сторінки, з яких основний зміст викладений на 133 сторінках, містить 39 рисунків, 28 таблиць.

ОСНОВНИЙ ЗМІСТ

У вступі обгрунтовано актуальність обраної теми дисертації, відзначено зв’язок роботи з науковими темами, сформульовано мету і задачі дослідження, визначено об’єкт, предмет і методи дослідження, показано наукову новизну отриманих результатів та їх практичне значення, а також розкрито питання апробації результатів дисертації на конференціях, семінарах та їх висвітлення у друкованих працях.

У першому розділі на основі аналітичного огляду літературних джерел розкрито стан досліджуваної проблеми. Проведено аналіз математичних моделей оцінювання живучості ІУС з точки зору ймовірності та детермінованості, побудованих на основі засобів для виконання обчислювальних операцій на ЕК, який дозволив сформулювати відповідні технічні і наукові дані, що лежать в основі дисертаційних завдань для розв’язання. Зроблено огляд основних типів ЕК криптографічних систем, що використовуються в засобах ІУС. Показано важливість дискретного логарифма для живучості ІУС, в яких складовими елементами виступають криптографічні засоби. Піддано аналізу ефективні методи розв’язання дискретного логарифма. Обґрунтовано необхідність досліджувати нові, ефективніші моделі і технології обчислень та їх вплив на живучість ІУС.

Під ІУС на основі ЕК розуміється клас ІУС, у засобах яких застосовуються обчислювальні операції на ЕК, включно із криптографічними пристроями на ЕК ECCD. Проаналізовано аспекти живучості ІУСЕК за ознаками множини дефектів, поділених на три групи, – розроблення або проектування, фізичних впливів і зовнішніх впливів (ДВ), – причому в роботі увагу зосереджено на третій групі ДВ, яка притаманна розглянутим в роботі ІУСЕК та є наслідком несанкціонованого втручання або інформаційних атак включно з хакерськими і кракерськими та спамом, помилковими діями персоналу, екстремальних впливів фізичного характеру, які можуть призводити до кратних відмов апаратних і програмних

засобів ІУС. Виділено групи показників оцінювання живучості: а) за ознакою ймовірності – показники за станом системи (тобто зберігання працездатності після ДВ) та показники за результатами виконання завдання (тобто здатність не тільки протистояти ДВ, але й надалі, незважаючи на ДВ, успішно виконати встановлене завдання); б) за ознакою детермінованості – адитивні та мінімаксні показники, які відрізняються один від одного за способом зведення векторного показника до скалярного. Для оцінювання живучості проаналізовано такі показники: а) за станом системи – умовний закон уразливості, виживаність ІУС для k-кратного ДВ, запаси живучості (d-живучість, інакше критична кількість ДВ, зменшена на одиницю, та m_d-живучість, інакше максимальна кількість ДВ, яку ще може видержати ІУС без втрати працездатності), середня кількість ДВ, що призводять до втрати працездатності, середній запас живучості, причому перший, другий, п’ятий і шостий показники є ймовірнісними, тоді як третій і четвертий – детермінованими; б) за результатами виконання завдання протягом часу t базової S_0 та нової S_i структур ІУС – умовна функція живучості, функція виживаності ІУС для k-кратного ДВ, безумовна функція живучості, причому передостанні два показники відносяться до класу адитивних і забезпечують згортку векторного показника в скалярний. За відсутності впевненої інформації про ймовірності їх можна замінити на відповідні вагові коефіцієнти, призначені експертно. Якщо ж і це зробити складно, то необхідно переходити до мінімаксних показників. Представлено огляд основних типів ЕК та їх застосування в криптографії з точки зору живучості ІУС, що дало змогу проаналізувати обчислювальну складність для різних представлень кривої. Показано важливість дискретного логарифма для живучості криптографічних систем. Визначено зв'язок дискретного логарифма на ЕК з живучістю ІУС. Проаналізовано методи розв’язання дискретного логарифма та обґрунтовано вибір найефективнішого методу для розв’язку дискретного логарифму підвищеної швидкодії.

На підставі аналізу ДВ на системи, які базуються на ЕК, та стійкості до них виявлено, що завдяки методам прискорення виконання основних операцій на ЕК, а також введенню до обчислень спеціально побудованих засобів, зростає ймовірність забезпечення підвищеного рівня живучості ІУСЕК внаслідок суттєвого скорочення часу, необхідного на проведення атаки. Це дало змогу довести необхідність верифікації та покращення оцінювання живучості даних систем, обґрунтувати необхідність дослідження нових, ефективніших обчислювальних методів та їх вплив на живучість ІУСЕК. Крім цього, на підставі аналітичного огляду літературних джерел, врахувавши стан досліджуваної проблеми, а саме специфіку поставлених задач та відомі підходи до їх розв’язання, сформульовано основні завдання дослідження.

У другому розділі представлено представлено структурну модель підвищення живучості ІУС з врахуванням ДВ, обчислювальні платформи та компоненти, за допомогою яких здійснюються основні обчислення на ЕК і цілих числах великої розрядності на потреби створення живучих ІУС. Розглянуто питання розпалелювання операцій, що виконуються як на числах великої розрядності, так і на кривих. Висвітлено способи побудови апаратних та апаратно-програмних систем, що реалізують паралельний ро-метод Полларда. Подано моделі та технології

обчислень для випадку сумування і множення чисел великої розрядності та реалізації основних операцій на ЕК. Доведено, що вибір відповідно швидких обчислювальних алгоритмів та ефективна імплементація в специфічних умовах можуть помножити швидкість розв'язання дискретного логарифма, а отже призвести до порушення безпеки ІУСЕК. Обґрунтовано, що для визначення живучості ІУСЕК слід змодифікувати алгоритми та імплементаційні рішення в обчислювальних середовищах, а також оцінити швидкість розв'язання логарифму.

Модель живучості ІУС, зокрема ІУСЕК можна представити сукупністю відповідної кількості часткових моделей різного призначення, в яких для опису процесів застосовуються як детерміновані, так і імовірнісні методи. Ґрунтуючись на рекомендованому стандартом підході оцінювання гарантоздатності на підставі створення та аналізування структурних моделей і схем живучості ІУСЕК, із врахуванням наявності криптографічних елементів на ЕК, і беручи до уваги множину *MS* інформаційно-технічних станів системи та результати виконання нею завдання, а саме – працездатний стан (*ПС*), частково працездатний стан (*ЧП*), працездатний безпечний стан (*НБС*), небезпечний стан (*НС*), – розроблено структурні моделі живучості ІУСЕК для вихідних станів $MS_{ПС}$ і $MS_{ЧП}$ (рисунок 1). Схему живучості для працездатного вихідного стану $MS_{ПС}$

$$E_{ПС} = E_{ПС,ПС} \cup E_{ПС,ЧП} \cup E_{ПС,НБС} \cup E_{ПС,НС} \quad (1)$$

утворено елементами підмножин елементів, відмови яких призводять до її переходу в: а) інший працездатний стан $E_{ПС,ПС}$ і частково працездатний стан $E_{ПС,ЧП}$ з можливим паралельним ввімкненням, б) непрацездатний безпечний стан $E_{ПС,НБС}$ і небезпечний стан $E_{ПС,НС}$ з послідовним ввімкненням, модулем 1 оцінювання живучості ІУСЕК за її станом, модулем 2 оцінювання живучості ІУСЕК за результатами виконання нею завдання, моделлю прийняття рішення (ІІР) про способи підвищення живучості (включно із змінами структури та параметрів ІУСЕК, а також додатковим удосконаленням пасивних та активних засобів забезпечення живучості), якщо оцінки вказують на її незадовільний рівень (рисунок 1,а). Схему живучості для частково працездатного вихідного стану

$$E_{ЧП} = E_{ЧП,ЧП} \cup E_{ЧП,НБС} \cup E_{ЧП,НС} \quad (2)$$

побудовано аналогічним чином. В наведених на рисунку 1 моделях дефекти ДВ можна подати у вигляді точкової та просторової моделі, якщо класифікувати їх за областю дії, особливості чого й відображено в роботі. Для оцінювання та підвищення живучості ІУСЕК доцільно: а) провести аналіз відмов елементів та оцінити вплив їхніх наслідків на працездатність ІУСЕК і сформулювати множини інформаційно-технічних станів $MS_{ПС}$, $MS_{ЧП}$, $MS_{НБС}$ і $MS_{НС}$; б) в залежності від наслідків відмов здійснити розбиття множини елементів E на підмножини $E_{ПС}$ ($E_{ПС,ПС}$, $E_{ПС,ЧП}$, $E_{ПС,НБС}$, $E_{ПС,НС}$), $E_{ЧП}$ ($E_{ЧП,ЧП}$, $E_{ЧП,НБС}$, $E_{ЧП,НС}$) і $E_{НБС}$ ($E_{НБС,НБС}$, $E_{НБС,НС}$); в) побудувати структурну модель живучості ІУСЕК для всіх груп інформаційно-технічних станів; г) одержати відповідно до цих моделей вирази для обчислення показників живучості.

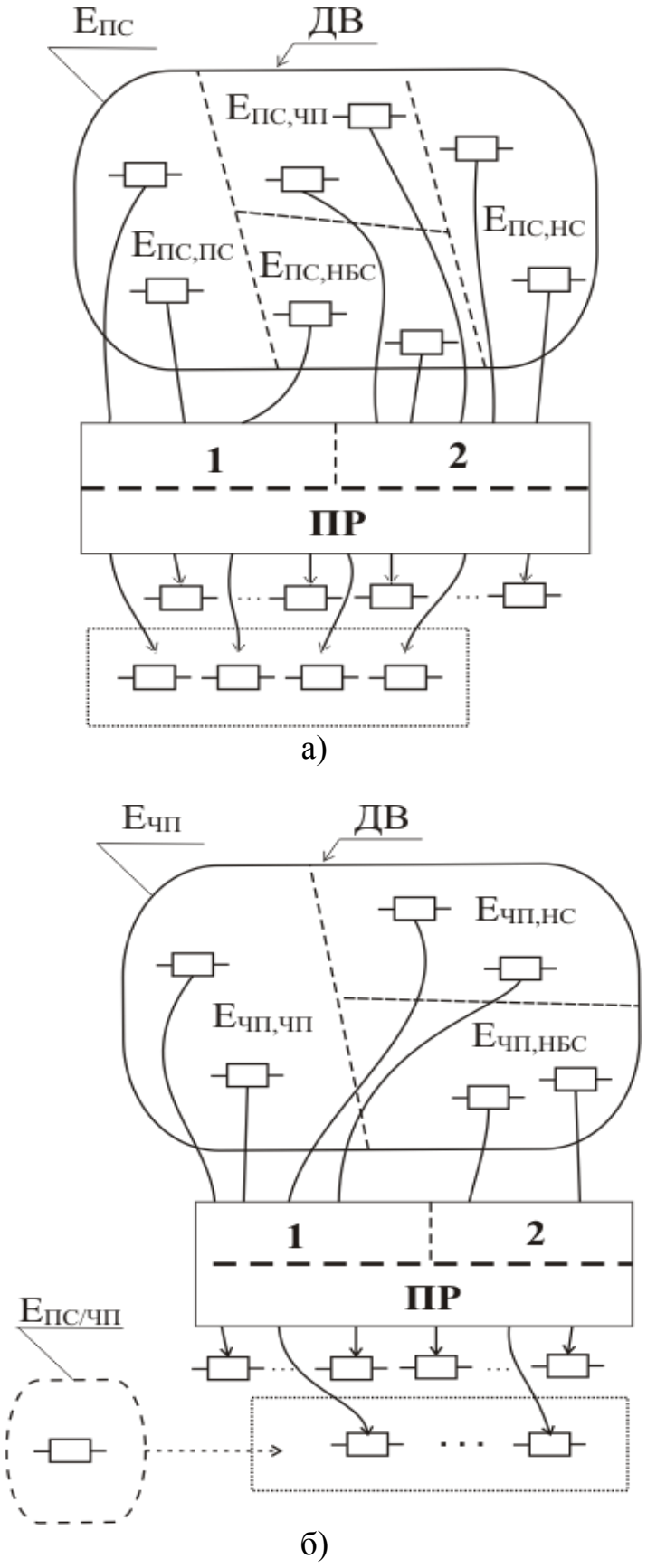

Рисунок 1 – Структурні моделі живучості ІУСЕК для вихідних станів $MS_{ПС}$ (а) і $MS_{ЧП}$ (б)

До найскладніших із цих задач, як свідчать результати досліджень, належать етапи а) та б). Їх можна виконати за допомогою відповідної методики аналізу. В наведених на рисунку 1 моделях дефекти ДВ можна подати у вигляді точкової та просторової моделі, якщо класифікувати їх за областю дії, особливості чого й відображено в роботі. Для оцінювання та підвищення живучості ІУСЕК доцільно: а) провести аналіз відмов елементів та оцінити вплив їхніх наслідків на працездатність ІУСЕК і сформулювати множини інформаційно-технічних станів $MS_{ПС}$, $MS_{ЧП}$, $MS_{НБС}$ і $MS_{НС}$; б) в залежності від наслідків відмов здійснити розбиття множини елементів E на підмножини $E_{ПС}$ ($E_{ПС,\ ПС}$, $E_{ПС,ЧП}$, $E_{ПС,НБС}$, $E_{ПС,НС}$), $E_{ЧП}$ ($E_{ЧП,ЧП}$, $E_{ЧП,НБС}$, $E_{ЧП,НС}$) і $E_{НБС}$ ($E_{НБС,НБС}$, $E_{НБС,НС}$); в) побудувати структурну модель живучості ІУСЕК для всіх груп інформаційно-технічних станів; г) одержати відповідно до цих моделей вирази для обчислення показників живучості. До найскладніших із цих задач, як свідчать результати досліджень, належать етапи а) та б). Їх можна виконати за допомогою відповідної методики аналізу.

Для виконання множення чисел великої розрядності у пристроях виконання криптографічних перетворень ІУСЕК застосовано рішення на основі ТЧБ Радемахера-Крестенсона. Використання моделі модулярного множення Крестенсона уможливлює зведення множення до операції додавання, яка реалізовується в інформаційних системах на основі попередньо згенерованих таблиць. Проведені автором теоретичні дослідження вказують на те, що використання ТЧБ Крестенсона для здійснення обчислень на числах великої розрядності забезпечить ефективне виконання операцій множення не тільки в програмній версії, але також дозволить реалізувати множення чисел великої розрядності у апаратних компонентах, наприклад, програмованих матрицях FPGA. Обгрунтовано, що створюючи апаратні або програмні системи, які функціонують паралельно, слід використати методи розпаралелювання математичних операцій, що дає змогу поділити числа великої розрядності на сегменти розміром, який дозволяє побудувати апаратні компоненти для їх обслуговування. Розглянуто алгоритми, завдяки яким можна здійснити паралельну операцію додавання та віднімання чисел, записаних у вигляді попередньо створених слів. Розглянуто технологію обчислень за допомогою паралельної системи, що реалізує ро-метод Полларда розв’язування дискретного логарифма. Така система складається з сервера, функцією якого є надання доступу до параметрів ЕК, та під’єднаними до сервера незалежними засобами, необхідними для реалізації стежки блукання. Узагальнюючи теоретичний розгляд, можна передбачати, що перспективним є підхід, який ґрунтується на застосуванні кластера програмованих матриць FPGA до обчислень на ЕК, де основне завдання полягає у знаходженні дискретного логарифма. Кластер побудований на програмованих матрицях FPGA типу Copacobana. Кластер складається з контролера USB, який дає змогу під’єднати до комп'ютера і контролера FPGA, що взаємодіє з окремими компонентами, максимально 120 програмованих матриць FPGA, зібраних у модулі. Застосовано відповідні моделі, методи та алгоритми з метою обчислення дискретного логарифма на ЕК вищих порядків *GF(p)*. Засобами також передбачено здійснення розрахунків на ЕК над полем другого порядку $GF(2^m)$.

Методи прискорення обчислень на ЕК для підвищення живучості ІУСЕК базуються на підході, що відноситься до створення засобів, які допомагають здійснити криптоаналіз шифрів на основі ЕК в репрограмованих структурах. Наявна можливість побудувати структурну одиницю – операційний пристрій, який виконує ро-метод Полларда для ЕК над полем другого порядку $GF(2^m)$. Застосування відповідно підібраних представлень, а також подання точок на ЕК у відповідних координатах призвело до того, що отримано кращі результати, ніж ті, які наведені в більш ранніх працях.

Результати проведеного теоретичного дослідження свідчать про те, що перспективною вбачається реалізація технології обчислень для прискореного виконання основних операцій на ЕК над полем вищих порядків *GF(p)* на базі вбудованих модулів VIRTEX (FPGA). При цьому точки на ЕК ще перед початком виконання операції додавання записано у проективних координатах, що дало змогу уникнути необхідності обчислення оберненого елемента в полі.

У третьому розділі представлено моделі обчислювальних платформ, за допомогою яких у пристроях ІУСЕК виконуються основні операції на ЕК із

застосуванням розроблених автором перемножувачів, що грунтуються на ТЧБ Радемахера-Крестенсона, і суматорів, базованих на паралельному сумуванні чисел великої розрядності, наприклад, довжини 100 і більше бітів. Побудовано і проаналізовано моделі та апаратні імплементації для виконання основних операцій на ЕК. Розроблено операційні пристрої для здійснення обчислень на ЕК. Реалізовано апаратний засіб, який виконує поодиноку стежку ро-методу Полларда, а також його паралельну версію. Проведено аналіз та виконано оцінювання особливостей функціонування та застосування побудованих засобів і удосконалених методів щодо живучості ІУСЕК, здійснюваної шляхом розв'язання дискретного логарифма. Показано придатність розроблених моделей та алгоритмів в шифруванні і розшифруванні.

В основу моделі для виконання основних операцій на ЕК покладено продуктивність P для оцінювання стану ІУСЕК, базованих на пристроях, що реалізують криптографічні операції на ЕК, та введено наступні позначення: p_{wwf} – імовірність безвідмовної роботи ІУСЕК; f_s – функція живучості, тобто мінімальна підмножина функцій ІУСЕК з найвищим пріоритетом, виконання яких необхідно для того, щоб система не перейшла до небезпечного стану; P_s – продуктивність ІУСЕК, необхідна для виконання функцій живучості та нижче за яку виникає аварія; m – загальна кількість функцій живучості; p_{ds} – ймовірність переходу ІУСЕК на часовому інтервалі t до небезпечного стану; n – загальна кількість процесорних пристроїв в ІУСЕК; n_{ECCD} – кількість пристроїв ECCD у системі, що виконують криптографічні операції на ЕК; x – вектор стану ІУСЕК; X_{ds} – множина, яка відповідає небезпечним станам ІУСЕК; x_i та x_j – компоненти вектора x, які відповідають стану i-гопроцесорного пристрою та j-го ECCD ($x_i = x_j = 0$ – для відмови; $x_i = x_j = 1$– для працездатності); P_i та P_j – продуктивність i-го процесорного пристрою та j-го ECCD; P_x – продуктивність ІУСЕК в стані, що відповідає вектору x.

У результаті отримано модель живучості ІУСЕК, представлену формулами:

$$P_x = \sum_{i=1}^{n-n_{ECCD}} \alpha_i \, P_i + \sum_{j=1}^{n_{ECCD}} \alpha_j \, P_j \,, \tag{3}$$

$$p_{ds}(t) = \sum_{x \in X_{ds}} p_x(t)\Big|_{\forall x \in X_{ds}} \,, \tag{4}$$

де

$$p_x(t)\Big|_{\forall x \in X_{ds}} = \prod_{i=1}^{n} p_i^{x_i}(t)\big(1 - p_i(t)\big)^{1-x_i} - \prod_{j=1}^{n-n_{ECCD}} p_j^{x_j}(t)\big(1 - p_j(t)\big)^{1-x_j} \,, \tag{5}$$

причому $p_{wwf} = p\left(P_x \geq P_s\right),\ P_s = \sum_{f=1}^{m} P_{s.f}$.

Звідси можна обчислити ймовірність переходу ІУСЕК в часовому інтервалі t до небезпечного стану, викликаного зниженням її продуктивності внаслідок відмов пристроїв ECCD.

Основна особливість моделі полягає в заміні операції модулярного множення цілих чисел великої розрядності додаванням за модулем, яке проводиться за допомогою ТЧБ Крестенсона, а також застосуванням паралельного додавання чисел, що дає змогу прискорити виконання операції на відміну від традиційного підходу.

Паралельне сумування полягає на поділі цих чисел великої розрядності на слова (довжина слова відповідає розміру регістра процесора), розмір яких дає змогу безпосередньо виконати операцію додавання за допомогою вбудованих в процесори суматорів з використанням стандартних типів даних. Віднімання чисел також виконується паралельним способом.

Розглянемо два числа *X* та *Y* і модуль *n*: $Z = X*Y \bmod n$.
Модель передбачає подання чисел *X* і *Y* у вигляді двійкових послідовностей:

$$X = x_{r-1}2^{r-1} + x_{r-2}2^{r-2} + x_i 2^i + \ldots + x_1 2^1 + x_0 2^0, \quad (6)$$

$$Y = y_{r-1}2^{r-1} + y_{r-2}2^{r-2} + y_j 2^j + \ldots + y_1 2^1 + y_0 2^0. \quad (7)$$

Для визначення результату їх множення побудовано матрицю Крестенсона, у якій вмістиме комірок обчислено згідно з виразом $m_{ij} = 2^{i+j} \bmod n$. Добуток чисел *X* та *Y* можна отримано за формулою:

$$X \cdot Y \bmod n = \sum_{s,k=0}^{r-1} m_{sk} \bmod n, \quad (8)$$

де $x_s, y_k = 1$, тобто m_{sk} знаходиться на перетині стовпця і рядка, для яких відповідні x_i та y_j дорівнють 1.

Числа, які записано в таблицю, є меншими, ніж заданий модуль *n*. Сума чисел рядка або стовпця є меншою від подвійного модуля, тому для обчислення за модулем достатньо порівняння та віднімання за модулем. Виходячи з цього, надалі створено модель, за допомогою якої проводяться обчислення із використанням стандартних типів даних, що обслуговуються безпосередньо даним процесором.

Алгоритм обчислень зводиться до наступного (рисунок 2):

1. Генерування матриці Крестенсона та її запис у тривимірному масиві, де третій вимір залежить від кількості слів, на які було поділено числа. Таким чином побудовано третій вимір масиву.

2. Додавання за модулем вмістимого кожного з *n* рядків матриці Крестенсона відповідно до виразу $\sum_{i;j=1}^{j=r-1} m_{sk} \bmod n$. Додавання вмістимого рядків відбувається в паралельному режимі. Розглянуте додавання відповідає методу, описаному в попередньому розділі. Єдина модифікація полягає у додаванні на першому кроці не двох слів, а *r-1* слів.

Рисунок 3 ілюструє концепцію додавання вмістимого рядків матриці. Результатом цієї операції є вектор розміру *r* сум для кожного рядка.

3.Додавання елементів вектора суми вмістимого рядків матриці Крестенсона здійснюється згідно зі способом, подібним до додавання вмістимого рядка, представленого вище. Єдиною відмінністю є те, що додаються всі елементи вектора (рисунок 4). В результаті виконання цієї операції одержується добуток чисел *X* та *Y* за модулем *n*.

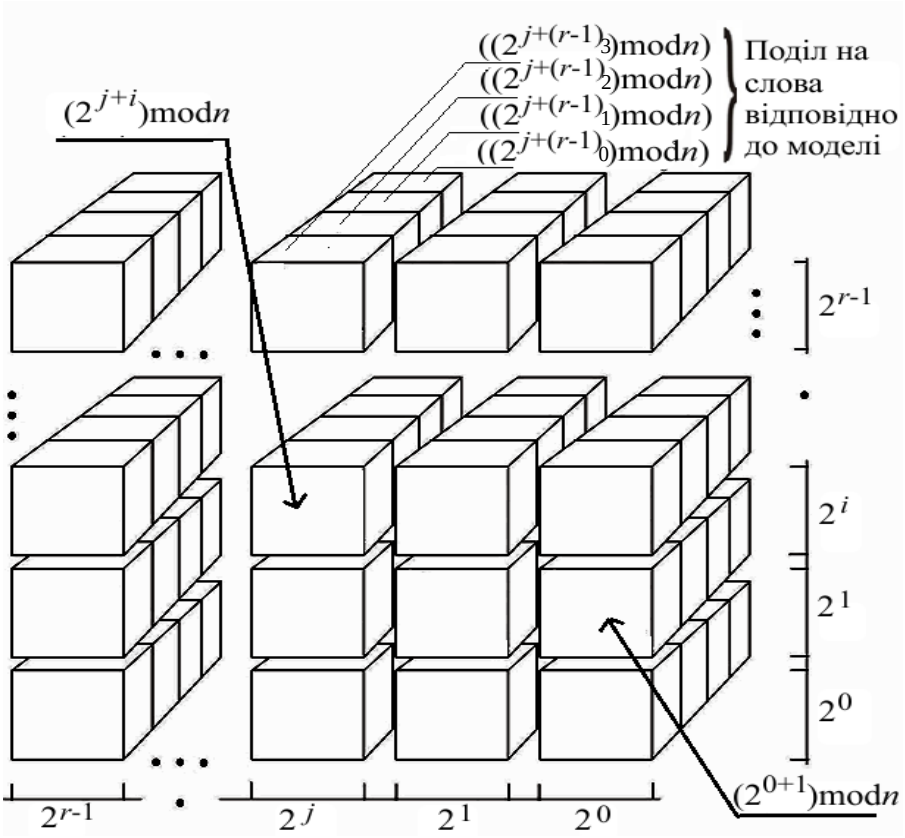

Рисунок 2 – Алгоритм запису матриці Крестенсона та обчислення для рядків моделі

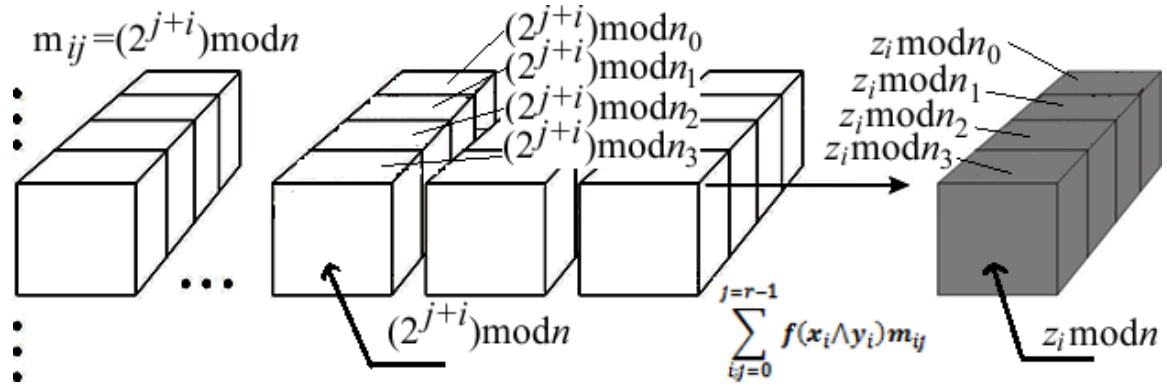

Рисунок 3 – Концепція додавання вмістимого рядків матриці Крестенсона

Створено апаратний засіб, який виконує поодиноку стежку випадкового блукання з модифікацією трьох стартових сталих у реалізації ро-методу Полларда, а також його паралельної версії. Проведено аналіз впливу змодифікованих моделей та технологій обчислень, реалізованих на основі ТЧБ Радемахера-Крестенсона, на живучість ІУСЕК шляхом розв’язання дискретного логарифма на ЕК, що дало змогу визначити мінімальні розміри ЕК, які можуть бути застосовані для забезпечення необхідного рівня живучості криптографічних компонетів системи.

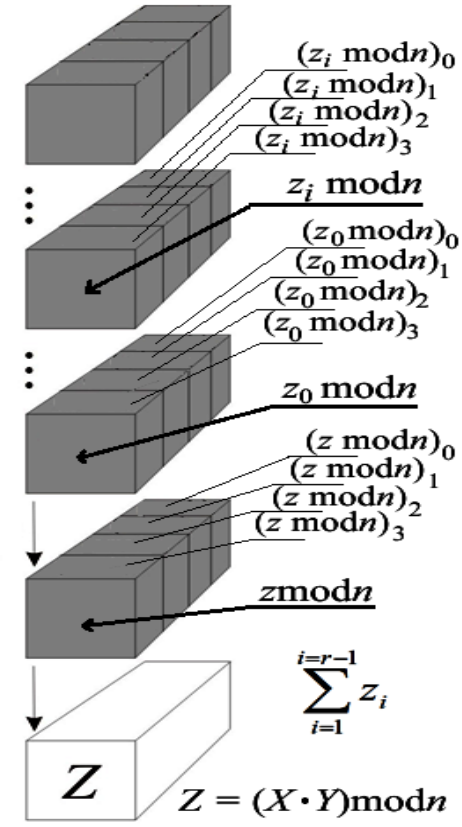

Рисунок 4 – Додавання елементів вектора

Реалізовано створені моделі та апаратні імплементації, основані на базисах Крестенсона і паралельному додаванні та за допомогою яких виконано ро-метод Полларда розв’язання дискретного логарифма, завдяки чому забезпечено ефективність його розв’язання. Визначено області і технології, в яких застосування розроблених моделей, алгоритмів та методик зумовлює підвищення ефективності обчислень на кривих *GF(p)*. Такими середовищами є структури програмованих матриць FPGA, комп’ютерні системи з багатоядерними процесорами чи багатопроцесорні сервери та комп’ютерні кластери, а також системи з архітектурою CUDA NVIDIA.

У четвертому розділі здійснено симуляцію роботи моделей та технологій обчислень, запропонованих в попередньому розділі. Проведено аналіз симуляції роботи апаратно-програмних систем для розв’язування дискретного логарифма, який є підставою для підвищення живучості ІУСЕК. На основі результатів розв’язування дискретного логарифма для кривих різних розмірів здійснено оцінювання живучості ІУСЕК.

Схему алгоритму додавання чисел *X* та *Y* за модулем *n* наведено на рисунку 5. Обчислення суми двох чисел, яке складається з чотирьох слів, вимагає виконання семи кроків. Під час додавання проводиться також операція паралельного віднімання. При цьому слід відзначити, що порівнюється не ціле число, а окремі слова, щоб на підставі порівняння всіх слів здійснити порівняння чисел. Паралельне сумування чисел в поєднанні з відніманням за модулем дозволяє зменшити кількість кроків, які повинні бути виконані для того, щоб додати числа за модулем. Проаналізовано випадок зміни складності обчислень для більших чисел, які поділено не на чотири, а на п'ять, шість і т.д. слів. Доведено, що якщо в алгоритм ввести додатково одне слово, то тоді потрібно збільшити кількість кроків на два, модифікуючи п'ятий крок, і після нього додати додатково два кроки. Звідси випливає, що для випадку поділу числа на п’ять слів кількість необхідних кроків потрібно збільшити до дев'яти.

Аналіз роботи суматора, реалізованого в програмованих структурах системи, здійснено на підставі результатів досліджень обчислювальних засобів, побудованих на програмованих матрицях FPGA. Логічний синтез апаратної моделі, виконаної на програмованій матриці фірми Altera типу Stratix III, дав змогу забезпечити робочу частоту на рівні 366 МГц. Робота на такій частоті дозволила виконати 45,75 млн. додавань за секунду для чисел, які складаються з чотирьох слів.

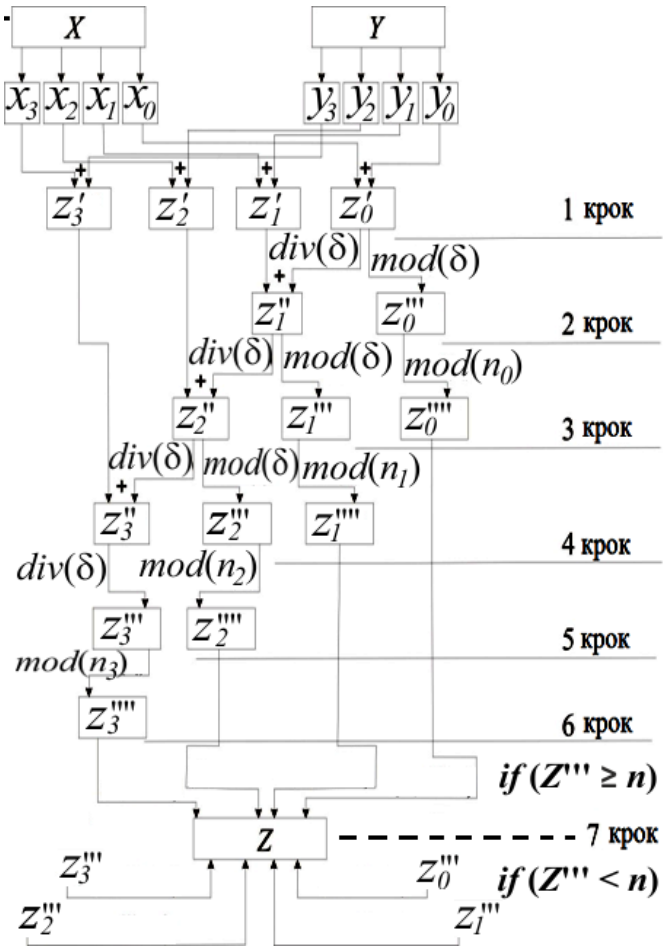

Рисунок 5 – Схема алгоритму додавання двох чисел за модулем *n*

Швидкодія сумування для числа, яке складається з п'яти слів, становить 35 млн. додавань за секунду для частоти 350 МГц, а для шести слів – 27,9 млн. додавань. Можна зауважити майже лінійне зменшення швидкості обчислень в залежності від збільшення кількості слів, що є важливим для забезпечення живучості ІУСЕК. Піддано тестуванню побудовану в третьому розділі модель перемноження чисел великої розрядності. Схема алгоритму виконання операції множення в ТЧБ Крестенсона, передбачає дії, необхідні для обчислення добутку двох чисел за модулем, виконуючи відповідні сумування елементів матриці Крестенсона. Проведено симуляцію для апаратної моделі, яку передбачено для обчислень, що здійснюються на числах великої розрядності. Відповідне генерування і синтез операційного пристрою проведено для програмованої матриці FPGA типу Stratix III. При цьому отримано тактову частоту на рівні 44 МГц. Додавання значень всіх рядків матриці здійснюється паралельним способом, причому обчислення суми рядків отримується протягом виконання семи кроків. Сумування рядка здійснюється аналогічно тому, що описано попередньо для випадку суматора, проте єдиним винятком є сумування на першому кроці багатьох чисел. На наступному кроці виконано сумування вектора, також аналогічним чином протягом 7 кроків. Для того щоб обчислити добуток двох чисел, поділених на чотири слова, потрібно виконати 14 кроків.

Проведено аналіз роботи суматора точок на ЕК із застосуванням обчислень в ТЧБ Радемахера-Крестенсона та паралельного додавання. Додавання точок у суматорі складається із виконання операцій додавання та множення чисел. Сумування точок у змішаному поданні зводиться до виконання наступних операцій над числами: 11-ти множень, 2-ох додавань, 5-ти віднімань та 2- ох бітових зсувів. Вся операція сумування точок змішаним способом може бути здійнена протягом 11 кроків, застосовуючи відповідний підхід до вибору порядку обчислень. Симуляцію процесів здійснено на апаратній моделі суматора точок *GF(p)*. Симуляцію проведено для програмованої матриці FPGA типу Stratix III EP3SL150F1152I4SL. Результати симуляції дозволили отримати тактову частоту на рівні 44 МГц. Проведено аналіз функціональних характеристик суматора точок на ЕК при реалізації алгоритму шифрування Ель-Гамаля в компонентах ІУСЕК для файлу інформаційним обсягом 1024 кБ (таблиця 1).

Таблиця 1

Швидкість шифрування файлу методом Ель-Гамаля в компонентах ІУСЕК

Крива $GF(p)$		89	97	109	131	163	191
Час, с	для стандартного алгоритму	104	131	145	243	339	440
	на основі ТЧК Радемахера-Крестенсона	37	40	43	79	111	127

З аналізу даних таблиці 1 можна зробити висновок, що введення додавання на основі ТЧБ Крестенсона у відповідному середовищі ІУСЕК збільшує швидкість шифрування приблизно вдвічі порівняно з традиційним підходом.

Здійснено аналіз живучості ІУСЕК, базуючись на розв'язанні дискретного логарифма змодифікованим ро-методом Полларда. Симуляцію роботи здійснено на базі програмованої матриці FPGA типу Stratix III EP3SL150F1152I4SL (таблиця 2).

Для визначення середнього очікуваного часу знаходження дискретного логарифма за допомогою ро-методу Полларда використано оцінку за формулою $\sqrt{\pi n}/2$, де n – порядок ЕК (таблиця 2,а).

Таблиця 2

Результати дослідження процесів, які протікають у апаратно-програмних моделях для ЕК *GF(p)* різного розміру

ЕК *GF(p)*		*GF*(69)	*GF*(92)	*GF*(115)	*GF*(138)	*GF*(161)	*GF*(184)
Кіль-кість ітера-цій / с	Itanium2	109169	67142	53791	47921	42052	32543
	Pentium IV	117496	73157	56045	48659	41274	31235
	FPGA	321678	235294	186147	149091	125392	107438
	Кластер	38601398	28235294	22337662	17890909	15047022	12892562
Час, дні	а)	0,84	3295	$12*10^6$	$4{,}2*10^{10}$	$1{,}7*10^{14}$	$5{,}8*10^{17}$
	б)	0,007	27	100790	$3{,}5*10^8$	$1{,}4*10^{12}$	$4{,}9*10^{15}$

Проведено дослідження процесів в апаратній моделі реалізації ро-методу Полларада для підтримки системи криптоаналізу, спрямованого на відповідні компоненти ІУСЕК. Цю модель застосовано складовим компонентом для підтримки функціонування криптографічної системи, що ґрунтується на програмному рішенні. Процеси як у апаратно-програмній, так і програмній моделях симульовано в різних середовищах. Одні з них – процесорами Itanium 2 тактової частоти 1,5 ГГц, інші – на основі мікропроцесора Pentium IV 2,8 ГГц. Результати роботи, які ілюструють наведені в таблиці 2 дані, відносяться до кількості ітерацій, необхідних для реалізації одної стежки випадкового блукання. Як випливає з даних, наведених в таблиці 2, швидкість обчислення на заданій ЕК при застосуванні апаратно-програмної моделі збільшується принаймні втричі в порівнянні з обчисленнями, виконаними в програмній моделі. Застосування апаратної моделі обчислень з використанням ТЧБ Крестенсона дає реальне збільшення швидкості обчислень на ЕК і значно пришвидшує продуктивність ро-методу Полларда.

Реалізація алгоритму паралельного блукання полягає на створенні компонентів, за допомогою яких реалізуються окремі стежки випадкового блукання. Для випадку впровадження до обчислень більшої кількості компонентів ІУСЕК, що реалізують шляхи випадковго блукання, кількість ітерацій алгоритму збільшується

пропорційно до кількості впроваджених компонентів. Розглянемо випадок заімплементування моделі, яка дає змогу реалізувати паралельний ро-метод Полларда, на кластері програмованих матриць FPGA типу COPACOBANA. В результаті аналізу проведених досліджень отримано, що для застосованих 120 стежок випадкового блукання, які виконуються паралельно, отримані результати досліджень дали змогу оцінити час, необхідний для розв'язку дискретного логарифма для кривих *GF(p)* різного розміру. Продуктивність обчислювальної системи, виражена в кількості ітерацій за секунду, для такого рішення зростає до значень, наведених в таблиці 2.

Отримані результати досліджень дали змогу оцінити час, який необхідний для розв'язку дискретного логарифма для кривих *GF(p)* різного розміру при використанні 120 стежок блукання (таблиця 2,б). Беручи до уваги атаку на алгоритм, забезпечення живучості інтегрованих ІУС на основі ЕК *GF(p)* залежить від розміру застосованої ЕК. Мінімальний час, протягом якого системі забезпечено живучість і цілісність даних під час дефекту ДВ, наведено в таблиці 2.

ВИСНОВКИ

У дисертації отримано науково-обґрунтовані результати розв'язання актуального наукового завдання – побудови моделей та засобів підвищення живучості інформаційно-управляючих систем на основі еліптичних кривих, базованих на полях більш високого порядку, що має істотне значення для визначення гарантоздатності систем, вибору потрібних розмірів і типів кривих, збільшення стійкості до дефектів зовнішніх впливів. Найважливіші наукові результати, висновки та рекомендації такі:

1. Базуючись на результатах аналізу принципів побудови, технологічних рішень і напрямів розвитку інформаційно-управляючих систем, доведено необхідність створення моделей та засобів ІУСЕК, що дає змогу забезпечити високі продуктивність і живучість їх функціонування.

2. На підставі ефективних методів розв'язання дискретного логарифма на ЕК розроблено моделі підвищення живучості ІУСЕК з врахуванням дефектів зовнішніх впливів за ознаками ймовірності та детермінованості та технології обчислень у ТЧБ Крестенсона на ЕК *GF(p)* у пристроях для виконання криптографічних операцій із реалізацією ро-методу Полларда, що дало змогу забезпечити низьку тривалість факторизації, верифікацію та визначення розміру ЕК в залежності від часу, протягом якого інформація повинна бути конфіденційною, і в той же мінімізацію обчислювальних затрат та ефективну протидію потенційним загрозам.

3. Виконано оцінювання часу, потрібного для одержання розв'язання дискретного логарифма ро-методом Полларда при застосуванні запропонованих моделей та технологій обчислення, а також визначено середовища, в яких можна використовувати ці підходи, завдяки чому можна вибрати оптимальний розмір ЕК для засобів підвищення живучості ІУСЕК.

4. Удосконалено технологію обчислення добутку за модулем багатобітних чисел з використанням ТЧБ Радемахера-Крестенсона, що дає змогу позбутися операції множення в традиційній формі шляхом заміни операцією додавання та, на

підставі поділу чисел на слова потрібної довжини, усунути обмеження щодо максимальної довжини чисел, які додаються, у засобах підвищення живучості ІУСЕК.

5. Модифіковано модель обчислення точок на ЕК *GF*(p), впроваджуючи удосконалену технологію обчислення добутку та сумування чисел, змішане представлення точок, що дозволило кількість необхідних операцій обчислення добутку зменшити до значення 11, уникаючи додатково потреби знаходження оберненого елемента в полі у засобах підвищення живучості ІУСЕК.

6. Удосконалено технологію обчислень для реалізації паралельного ро-методу Полларда для ЕК вищих порядків *GF*(p) на основі модифікованої моделі суматора точок в ІУСЕК, що забезпечило суттєве зменшення часу, необхідного для розв'язання дискретного логарифма.

7. Створено дві апаратно-програмні системи для ІУСЕК:

а) перша з них працює на програмованих матрицях FPGA та комп'ютерах класу ПК, дія якої ґрунтується на основі модифікованої моделі обчислень, причому на підставі досліджень побудованого суматора точок на програмованих матрицях FPGA Stratix III EP3SL150F1152I4SL одержано збільшення швидкості шифрування методом Ель-Гамаля приблизно втричі в порівнянні до традиційного підходу сумування точок;

б) друга з них реалізує ро-алгоритм Полларда, використовуючи технологію обчислень на ТЧБ Крестенсона, та ґрунтується на аналогічних апаратних засобах. За результатами дослідження роботи паралельної системи на декількох програмованих матрицях FPGA, дослідження її роботи для розв'язання логарифма для ЕК різного розміру та проведених вимірювань визначено, що застосування поодинокої стежки алгоритму, який реалізовано на одній програмованій матриці FPGA, зумовлює трикратне збільшення швидкості роботи алгоритму в порівнянні з системою, побудованою на базі процесора Itanium 2.

СПИСОК ПРАЦЬ ЗА ТЕМОЮ ДИСЕРТАЦІЇ

1. Aleksander M. Functional safety and survivability of information control elliptic-curve-based systems: models and methods / M. Aleksander, M. Karpinski, G. Litawa // Безпека інформації. – 2013. – Том 19, № 1. – С. 51-56. – ISSN 2225-5036.

2. Aleksander M. Implementation in FPGA of Computations on Elliptic Curves GF(p) based on Rademacher–Krestenson's Bases / M. Aleksander, M. Karpinski, G. Litawa // Інформаційна безпека. – 2012. – № 1 (7). – С. 12-17. – ISSN 2224-9613.

3. Litawa G. An Elliptic Curve Points Calculation Method with Rademacher–Krestenson's Bases / G. Litawa // Вісник Тернопільського національного технічного університету. – 2012. – Том 66, № 2. – С. 207-213.

4. Bezpieczeństwo bezprzewodowych sieci spontanicznych i sensorowych / M. Aleksander, J. Kinach, G. Litawa [et al.] // Bezpieczeństwo informacji / M. Karpiński. – Warszawa: Wydawnictwo Pomiary Automatyka Kontrola. – 2012. – Rozd. 2. – S. 82-129. – ISBN 978-83-930505-3-6. – Розділ в монографії. [Information Security.– Warsaw: Measurements, Automation and Monitoring.– 280 p.] (Chapter in monograph, in Polish).

5. Aleksander M. Bezpieczeństwo kryptosystemów opartych na krzywych eliptycznych / M. Aleksander, G. Litawa // Bezpieczeństwo informacji / M. Karpiński. – Warszawa:

Wydawnictwo Pomiary Automatyka Kontrola. – 2012. – Rozd. 5. – S. 183-196. – ISBN 978-83-930505-3-6. – Розділ в монографії. [Information Security. – Warsaw: Measurements, Automation and Monitoring. – 280 p.] (Chapter in monograph, in Polish).
6. Aleksander M. Calculation of GF (p) Elliptic Curves in FPGA / M. Aleksander, M. Karpinskyy, G. Litawa // Computing. – 2011. – Vol. 10. – Issue 2. – Pp. 91-96. – ISSN 1727-6209.
7. Aleksander M. Implementation and testing of methods parallel computation on elliptic curves GF(p) / M. Aleksander, M. Karpinski, G. Litawa // Вісник Східноукраїнського національного університету імені Володимира Даля. – 2011. – № 7 [161], Частина 1. – С. 304-310.
8. The security of data transmission over telecommunication networks based on advanced data encryption methods / M. Karpinski, M. Aleksander, G. Litawa, V. Karpinskyi // Electrical Review. – 2009. – No 4. – P. 19-21. – ISSN 0033-2097.
9. Karpiński M. Bezpieczeństwo przekazu informacji w sieciach oparte na metodach szyfrowania bazujących na krzywych eliptycznych / M. Karpiński, M. Aleksander, G. Litawa G // III Międzynarodowa Konferencja Naukowa z cyklu "Informatyka w dobie XXI wieku" na temat "Technologie informatyczne w nauce, technice i edukacji", 2009.
10. Aleksander M. Distributed computing system which solve an elliptic curve discrete logarithm problem / M. Aleksander, G. Litawa, V. Karpinskyi // The Experience of Designing and Application of CAD Systems in Microelectronics : Xth International Conference CADSM 2009, 24-28 February 2009 : Proceedings of the Conference. – Lviv-Polyana, Ukraine: Publishing House Vezha&Co, 2009. – P. 378-380. – ISBN 978-966-2191-05-9.
11. Cryptographic system security level based on elliptic curves / M. Karpinski, M. Aleksander, G. Litawa, V. Karpinskyi // Вісник Східноукраїнського національного університету імені Володимира Даля. – 2008. – № 8 (126), Том 1. – С. 94-98.
12. The Security of Data Transmission over Telecommunication Networks Based on Advanced Data Encryption Methods / M. Karpinski, M. Aleksander, G. Litawa, V. Karpinskyi // Proceedings of the 9th International Workshop “Computational Problems of Electrical Engineering” (CPEE’08) (September 16-20, 2008, Alushta (Crimea), Ukraine). – P. 71-73. [CPEE’08. Program & Abstracts. – Pp. 38-39].
13. Карпінський В. Розв’язання проблеми дискретного логарифму паралельним методом Ро-Поларда на підставі бібліотек MPI2 і MIRACL / В. Карпінський, Г. Літава, І. Якименко // Матеріали дванадцятої наукової конференції Тернопільського державного технічного університету імені І. Пулюя (14-15 травня 2008, Тернопіль). – Тернопіль: ТДТУ. – 2008. – С. 93.
14. Litawa G. Zaawansowana kryptoanaliza szyfrów opartych na krzywych eliptycznych z zastosowaniem układów programowalnych FPGA / G. Litawa, W. Karpiński // Prace naukowe Instytutu Technicznego Państwowej Wyższej Szkoły Zawodowej w Nowym Sączu. – Praca zbiorowa pod red. dr inż. Marka Aleksandra. – Nowy Sącz: Wydawca Państwowa Wyższa Szkoła Zawodowa w Nowym Sączu. – 2007. – S. 175-185.

АНОТАЦІЇ

Літава Г. В. Моделі та засоби підвищення живучості інформаційно-управляючих систем на основі еліптичних кривих. – *Рукопис*.

*Дисертація на здобуття наукового ступеня кандидата технічних наук за спеціальністю 05.13.06 – **інформаційні технології** (технічні науки)*. – *Тернопільський національний технічний університет імені Івана. Пулюя, Тернопіль, 2014 р.*

Дисертація стосується удосконалення моделей та засобів підвищення живучості інформаційно-управляючих систем на основі еліптичних кривих (ІУСЕК) з врахуванням дефектів зовнішніх впливів за ознаками ймовірності та детермінованості. Розроблено моделі засобів та технології обчислень на еліптичних кривих (ЕК) із використанням теоретико-числових базисів Радемахера-Крестенсона для підвищення продуктивності обчислювальних методик здійснення основних операцій на ЕК у пристроях ІУСЕК.

Створено апаратно-програмні засоби для виконання обчислень на ЕК і розв'язання дискретного логарифма вищої швидкодії із реалізацією паралельного ро-методу Полларда для живучих ІУСЕК. Заімплементовано побудовані теоретичні моделі помножувача цілих чисел великої розрядності за модулем та блоків для виконання операцій на ЕК у апаратних структурах. Проведено верифікацію параметрів живучості ІУСЕК для розроблених моделей, технологій та структур засобів обчислень на ЕК.

Здійснено симуляційні дослідження та проаналізовано вплив методів виконання основних операцій на ЕК над скінченним полем вищих порядків на параметри живучості ІУСЕК для кожної з опрацьованих моделей та обчислювальних технологій. Застосування обчислень, реалізованих апаратно, уможливило щонайменше у 3 рази скоротити час обчислень дискретного логарифма порівняно з відомими алгоритмами.

Ключові слова: модель, живучість, інформаційно-управляюча система, дефект зовнішніх впливів, еліптична крива, криптографічна система, дискретний логарифм, теоретико-числовий базис Радемахера-Крестенсона, паралельний ро-метод Полларда.

Литава Г. В. Модели и средства повышения живучести информационно-управляющих систем на основании элиптических кривых. – *Рукопись*.

*Диссертация на соискание ученой степени кандидата технических наук по специальности 05.13.06 – **информационные технологии** (технические науки)*. – *Тернопольский национальный технический университет имени Ивана Пулюя, Тернополь, 2014 г.*

Диссертация касается усовершенствования моделей и средств повышения живучести информационно-управляющих систем на основе эллиптических кривых (ИУСЭК) с учетом дефектов внешних воздействий по признакам вероятности и детерминированности. Разработаны модели средств и технологии вычислений на эллиптических кривых (ЭК) с использованием теоретико-числовых базисов Радемахера-Крестенсона для повышения производительности вычислительных методик осуществления основных операций на ЭК в устройствах ИУСЭК.

Создано аппаратно-программные средства для выполнения вычислений на ЭК и решения дискретного логарифма высшей быстродействия с реализацией параллельного ро-метода Полларда для живучих ИУСЭК. Заимплементовано построенные теоретические модели умножителя целых чисел большой разрядности по модулю и блоков для выполнения операций на ЭК в аппаратных структурах. Проведено верификацию параметров живучести ИУСЭК для разработанных моделей, технологий и структур средств вычислений на ЭК.

Осуществлено симуляционные исследования и проанализировано влияние методов выполнения основных операций на ЭК над конечным полем высших порядков на параметры живучести ИУСЭК для каждой из разработанных моделей и вычислительных технологий. Применение вычислений, реализованных аппаратно, дало возможность не менее в 3 раза сократить время вычислений дискретного логарифма по сравнению с известными алгоритмами.

Ключевые слова: модель, живучесть, информационно-управляющая система, дефект внешних воздействий, эллиптическая кривая, криптографическая система, дискретный логарифм, теоретико-числовой базис Радемахера-Крестенсона, параллельный ро-метод Полларда.

Litawa G. W. Models and devices of improving survivability of the information control systems based on elliptic curves. – *Manuscript*.

The thesis is submitted to get a degree of Kandidat of Technical Sciences in ***Information Technology*** *(Technical Sciences) - 05.13.06; Ivan Pul'uj Ternopil National Technical University, Ternopil, 2014.*

The thesis focuses on the perfection of models and devices of improving survivability information control systems based on elliptic curves (ICSEC) considering the interaction faults based on probability and determinism. Works on research and evaluation of survivability of ICSEC, based on the constructed models, which only increases the speed of basic calculations on elliptic curve (EC).

Presents an analysis of evaluation models of survivability of ICSEC. Gives an overview of the main EC types in cryptography systems used in ICSEC. Shown the importance of the speed of solving the discrete logarithm for survivability of cryptographic systems.

Model survivability ICS, including IUSEK can introduce a set of partial models corresponding number of different purposes, which are used to describe the process as deterministic and probabilistic methods. Based on the recommended standard for dependability assessment approach based on the creation and analysis of structural models and schemes survivability ICSEC, taking into account the availability of cryptographic items on EC and taking into account the set of MS Information Technology states of the system and the results of its task.

Analyzes the techniques and computing algorithms by witch using basic calculations on EC. Designed summing units exploiting parallel summing and calculation models, which realize basic operations on elliptic curves, making use of multiplicators (devised by the author) relying on Rademacher-Krestenson bases. A hardware realization of units responsible for basic calculations on elliptic curves was accomplished. Describes

a specially designed theoretical model of a big integer modulo multiplicator based on Rademacher-Krestenson bases.

Furthermore it describes a specially designed theoretical model of units realizing basic calculations on elliptic curves. These were implemented in FPGA matrices. As a result proposed non-standard solution witch consist in using Rademacher-Krestenson's algorithm to increase performance of computing techniques adding points on EC. Determine the survivability of ICSEC using EC should evaluate solving speed of discrete logarithm. Presents the computational models, by which basic operations performed on EC, which using author's multipliers. They are based on the Rademacher-Krestenson bases and adders, based on parallel algorithms for addition.

Conducted a simulation and analysis of models and computational methods that have an impact on survivability. Work of the software and hardware of solving the discrete logarithm, which is the basis for evaluating the survivability ICSEC, was analysed. Using of computing implemented in hardware, allowing a minimum 3 times reducing of the computation time compared with the discrete logarithm computations that performed on previously proposed solutions of this problem. Past studies have allowed to determine the time inside which ICSEC is able to properly perform tasks regarding anticipated attack.

In this dissertation was received new science-based results of solving actual scientific task – creating improved models and technologes of computing based on EC based on the fields of higher order, which have essential value to determine the survivability of cryptographic systems and allows choose the appropriate size and types of curves used in systems that allow better resistance to faults.

Key words: model, survivability, information control system, interaction fault, elliptic curve, cryptographic system, discrete logarithm, theoretical and numerical Rademacher-Krestenson's basis, parallel Pollard's rho method.