УДК 004.432; 621.391
№ держ.реєстрації
Інв. № _____

Міністерство освіти і науки України
Запорізький національний технічний університет (ЗНТУ)
69063, м.Запоріжжя, вул.Жуковського, 64;
тел (0612) 224-42-36

ЗАТВЕРДЖУЮ:
Проректор з НР
д-р техн. наук, проф.
_____ Ю.М.Внуков
“___” _____ 2015 р.

М.П.

З В І Т
ПРО НАУКОВО-ДОСЛІДНУ РОБОТУ

МЕТОДИ ТА ЗАСОБИ ПОБУДОВИ ЗАХИЩЕНИХ ІНФОРМАЦІЙНИХ ТА КОМУНІКАЦІЙНИХ СИСТЕМ

(заключний)

Шифр роботи шифр 04512

Завідувач каф., керівник НДР
д-р техн. наук, проф. Л.М. Карпуков

2015

СПИСОК АВТОРІВ

Керівник НДР д-р техн. наук, проф., зав. каф. доцент, канд. техн. наук	Л.М. Карпуков (вступ, 3.1, висновки) С.І. Лізунов (1.2, 3.3)
доцент, канд. техн. наук	В.О. Воскобойник (1.2, 3.2)
доцент, канд. фіз.-мат. наук	Г.Л. Козіна (1.1, 2.1)
доцент, канд. техн. наук	Г.В. Неласа (2.2, 2.3)
доцент, канд. техн. наук	О.В. Щекотихін (3.1, 3.2, 3.3)
старший викладач	Д.В. Бєліков (1.2, 3.1)
старший викладач	А.О. Говоров (1.2, 3.2)
старший викладач	Р.Ю. Корольков (1.2, 3.3)
старший викладач	Г.І. Нікуліщев (1.1, 2.1)

РЕФЕРАТ

Звіт: 66 стор., 10 рис., 7 табл., 65 джерел.

Мета роботи – дослідження та побудова нових ефективних моделей математичного та технічного захисту інформації.

Об’єкт дослідження – інформаційні та комунікаційні системи і мережі, системи передачі інформації.

В результаті НДР створено нові методи захисту цифрових зображень, протоколи сліпого електронного цифрового підпису на еліптичних та гіпереліптичних кривих, проведено дослідження анонімності алгоритмів сліпого підпису, розроблена бібліотека криптоперетворень на графічних процесорах, запропоновано засоби оптимізації параметрів волоконно-оптичних ліній зв'язку, організаційно-технічні методи захисту інформації від несанкціонованого доступу.

ЦИФРОВИЙ ВОДЯНИЙ ЗНАК, ЕЛЕКТРОННИЙ ЦИФРОВИЙ ПІДПИС, СКІНЧЕНЕ ВЕКТОРНЕ ПОЛЕ, СЛІПИЙ ЦИФРОВИЙ ПІДПИС, ЕЛІПТИЧНА КРИВА, ГІПЕРЕЛІПТИЧНА КРИВА, АНОНІМІСТЬ, ГРАФІЧНИЙ ПРОЦЕСОР, CUDA, ОПТИЧНЕ ВОЛОКНО, ПЕРВИННЕ ЗАХИСНЕ ПОКРИТТЯ.

ЗМІСТ

ПЕРЕЛІК СКОРОЧЕНЬ ТА ПОЗНАЧЕНЬ

АРМ	Автоматизоване робоче місце
ВОК	Волоконно-оптичний кабель
ДКП	Дискретне косинусне перетворення
ЕЦП	Електронний цифровий підпис
ЕК	Еліптична крива
МБ	Мегабайт
ОВ	Оптичне волокно
ОК	Оптичний кабель
ПЗП	Первинне захисне покриття
ПК	Персональний комп’ютер
ПМД	Поляризаційна модова дисперсія
СВП	Скінчене векторне поле
ЦВЗ	Цифровий водяний знак
DSF	Зміщена дисперсія
GPU	Графічний процесор
NZDSF	Ненульова зміщена дисперсія
SF	Незміщена дисперсія
WDM	Багатоканальне хвильове мультиплексування

ВСТУП

Розвиток інформаційних технологій, поширення інформації в сучасних захищених інформаційних та комунікаційних системах і мережах потребує дослідження та розробку нових ефективних методів захисту інформації.

Цифрове зображення, як продукт діяльності висококваліфікованих фахівців у всьому технологічно та економічно розвиненому світі, часто створюється в комерційних цілях і характеризується великою трудомісткістю та цінністю. Тому несанкціоноване використання зображень найчастіше несе збитки його правовласнику.

Захист авторських прав на цифрові зображення розглядається в роботах [1]-[4], захист програмних продуктів – в роботах [5], [6]. Авторами розроблено дві комп'ютерні програми – "Комп'ютерна програма для захисту цифрових зображень", Комп'ютерна програма "Захист програмних продуктів" – та отримано патент на корисну модель «Спосіб захисту авторського права на цифрові зображення». Метод захисту авторського права на цифрові зображення призначений для створення перешкод порушенню авторського та суміжних прав при розповсюдженні цифрових зображень, а само для виявлення факту порушення авторських або суміжних прав. Програма може бути використана у випадку, коли при передачі твору підписується ліцензійна угода між ліцензіаром та ліцензіатом.

Організаційно-технічні способи захисту інформації розглядаються в роботах [7–14]. Досліджено проблеми витоку інформації в каналах мобільного зв'язку та запропонована комплексна система захисту мовної інформації в приміщенні. Розглянуто організація доступу до інформації засобами біометричної аутентифікації та можливості використання ДНК-чипів в системах контролю та доступу. Досліджено та проаналізовано застосування сучасних технічних засобів захисту інформації в інформаційних мережах та методів апаратного захисту програмного забезпечення.

Розробка математичних методів захисту інформаційних систем розглядається в роботах [15]-[19].

Запропоновано новий протокол сліпого цифрового підпису на еліптичних кривих над скінченим векторним полем. Сліпий підпис вирішує специфічну задачу підтвердження справжності документів без розкриття їхнього авторства і, завдяки цьому, може використовуватись в схемах електронного голосування. В алгоритмі сліпого підпису один учасник формує документ, а інший підписує його всліпу без можливості ознайомитися із вмістом. При цьому важливо, щоб навіть підписувач не зміг встановити автора документа. Через це до інших критеріїв захищеності схем підпису у випадку сліпого підпису додається критерій анонімності. Він показує неможливість визначити автора документа з боку підписувача, якщо він

використовуватиме всі відомі йому параметри, які використовувались при постановці підпису.

Пропонується реалізація протоколу сліпого цифрового підпису, що являє собою модифікацію стандарту ГОСТ Р 34.10-2001 на еліптичних кривих над скінченим векторним полем. Аналізується захищеність запропонованого протоколу за критерієм анонімності. Показано, що зміна математичного апарату не впливає на захищеність схеми сліпого підпису за критерієм анонімності.

Розглянуті математичні основи виконання криптографічних операцій на гіпереліптичних кривих та їх застосування в протоколі цифрового підпису, основаному на українському стандарті цифрового підпису ДСТУ 4145-2002.

Сучасний рівень розвитку апаратних платформ не дозволяє значно збільшити продуктивність ядер центральних процесорів, тому найбільш доступним і перспективним способом підвищення швидкості обчислень є використання паралельних обчислювальних пристроїв.

Паралельне програмування на сьогодні вже не є інноваційною технологією – існує безліч різних типів паралельних обчислювальних системи: кластера, grid-системи, хмарні обчислення, багатоядерні процесори. Однак серед них є порівняно нова і активно розвивається концепція масивно-паралельних неграфічних обчислень на графічних прискорювачах, або GPGPU.

Проблеми реалізації криптографічних алгоритмів на масивно-паралельних пристроях розглядаються в роботах [20]-[23].

В останні десятиріччя бурхливий розвиток технології виробництва систем і засобів зв'язку з практично необмеженою пропускною здатністю і дальністю передавання, а також масове їхнє використання привели до розвитку волоконно-оптичних систем передавання інформації.

В роботах [24]-[26] розглядаються основи волоконної оптики, устрій, принцип дії та характеристики оптичних волокон, конструкції і характеристики волоконно-оптичних кабелів, джерела та приймачі випромінювання, оптичні підсилювачі, з’єднання оптичних волокон, розподілювачі оптичної потужності, мультиплексори й інші компоненти та пристрої волоконно-оптичних ліній зв’язку.

Проблеми захисту від комбінованих завад розглядаються в роботах [27]-[30]. Запропоновано та отримано патент на спосіб захисту когерентно-імпульсних радіолокаційних станцій від комбінованих завад.

Проблеми теоретичних основ технічного захисту інформації розглядаються в роботах [31]-[40].

Запропоновано математичну модель каскадного з'єднання прямокутних хвилеводів. Отримано аналітичний вираз для розрахунку поверхневого імпедансу вузької стінки прямокутного хвилеводу, представлений у вигляді тригонометричного ряду Фур'є.

Запропоновано новий спосіб ідентифікації нелінійних об’єктів типу метал-окис-метал, який пропонується використовувати як перший етап, що передує поглибленому методу аналізу нелінійних об’єктів з використанням функцій та концепції динамічного насичення, які можна застосовувати: а) в нелінійній радіолокації з метою зменшення вірогідності помилкового прийняття хибного нелінійного об’єкту за справжній і навпаки; б) в нелінійній рефлектометрії для визначення дефектів в лініях передачі.

Проаналізовано причини виникнення втрат у швидкісній характеристиці радіолокаційної станції 35Д6. Виявлено неузгодженість періодів повторення імпульсів зондування з властивостями штатних вагових функцій, застосовуваних за обчислення дискретного перетворення Фур’є. Показано, що не існує вагового вікна, яке було б єдиним оптимальним для режимів випромінювання радіолокаційної станції 35Д6 з однаковою кількістю імпульсів зондування. Виконано оптимізацію вікон ДПФ за критерієм мінімуму втрат у швидкісній характеристиці. Отримано, що шляхом заміни штатних вагових функцій на оптимальні, можливе зменшення втрат на 7%..16%. За цього, для кожного режиму випромінювання треба застосовувати окрему вагову функцію.

На основі проекційного методу дається строгий розв’язок задачі дифракції основної хвилі Н10 на стику регулярного і нерегулярного прямокутних хвилеводів з діелектричної пластиною, розташованою паралельно вузьким імпедансним стінкам. Наводяться і аналізуються залежності дифракційних характеристик стику хвилеводів від його параметрів.

Розглянута можливість застосування еквівалентних граничних умов для визначення параметрів складних хвилевідних структур, що являються ключовими елементами при розробці фільтруючих систем в радіотехнічних засобах.

1 ДОСЛІДЖЕННЯ ОРГАНІЗАЦІЙНО-ТЕХНІЧНИХ ТА ПРАВОВИХ МЕТОДІВ ЗАХИСТУ ІНФОРМАЦІЇ

1.1 Дослідження методів захисту авторських прав на цифрові зображення

Цифрове зображення, як продукт діяльності висококваліфікованих фахівців у всьому технологічно та економічно розвиненому світі, часто створюється в комерційних цілях і характеризується великою трудомісткістю та цінністю. Тому несанкціоноване використання зображень найчастіше несе збитки його правовласнику.

Закон України про авторське право та суміжні права [41] свідчить, що авторське право на твір виникає в наслідок факту його створення. Для виникнення і здійснення авторського права не вимагається реєстрація авторського твору. Але внаслідок виникнення суперечок може знадобиться підтвердження факту створення фотографічного твору справжнім автором в судовому порядку або підтвердження факту підписання ліцензійного договору.

Розглядаються методи захисту інформації для підтвердження авторських прав на цифрові зображення, які представлені в растровому форматі в стеганографічних системах захисту інформації, зокрема для захисту цифрової інформації та елементів дизайну представлених як растрові зображення.

В роботі запропоновано новий метод [1,2] захисту авторського права на цифрові зображення. В зображення вбудовується цифровий водяний знак на основі дискретного косинусного перетворення точок зображення у частотні коефіцієнти шляхом зміни цих коефіцієнтів та мають змогу витягувати цифровий водяний знак на основі відповідного дискретного косинусного перетворення шляхом порівняння значень частотних коефіцієнтів для розпізнавання бітів цифрового водяного знаку залежно від значень інших високочастотних коефіцієнтів.

1.1.1 Методи захисту авторського права на цифрові зображення

Відомий спосіб та пристрій для отримання та видалення інформації відносно об’єктів цифрових прав [42], призначений для створення технологічних перешкод порушенню авторських та суміжних прав при використанні об’єктів цифрових прав, який полягає в тому, що пристрій на якому відтворюється цифровий об’єкт, отримує інформацію про наявність права у видавця прав і приймає рішення про дозвіл доступу до інформації користувачу. Недоліком цього способу є те, що несумлінний користувач, навіть при наявності прав може зловживати ними і зробити

контрафактну копію цифрового об'єкту. При цьому якщо кількість користувачів досить велика, правовласник не зможе виявити правопорушника.

В [43] розглядається метод захисту авторських прав векторних зображень цифровими водяними знаками у вигляді електронного коду. Він оснований на тому, що в зображення вбудовують цифровий водяний знак (ЦВЗ) на основі двовимірного дискретного косинусного перетворення точок векторного зображення у матриці з частотними коефіцієнтами шляхом зміни в межах матриці перетворення залежно від значень інших високочастотних коефіцієнтів цієї матриці, які визначають і величину зміни, а також мають змогу витягувати цифровий водяний знак без оригіналу векторного зображення та цифрового водяного знаку.

Недоліком такого способу є те, що він не передбачає можливості визначення правопорушника авторських прав при виявленні факту появи контрафактної копії. Крім того автори цього способу пропонують його використовувати для захисту векторних зображень, але часто необхідно захищати зображення, представлені у растровому форматі.

При створені метода захисту цифрових зображень було поставлено завдання розширення функціональних можливостей захисту авторського права на цифрові зображення та розробка більш ефективного способа, який можливо використовувати для растрових зображень та який зможе надати можливість правовласнику виявляти правопорушника при появі контрафактної копії.

В запропонованому методі в зображення вбудовують цифровий водяний знак на основі дискретного косинусного перетворення точок зображення у частотні коефіцієнти шляхом зміни цих коефіцієнтів та мають змогу витягувати цифровий водяний знак на основі відповідного дискретного косинусного перетворення шляхом порівняння значень частотних коефіцієнтів для розпізнавання бітів цифрового водяного знаку залежно від значень інших високочастотних коефіцієнтів. При цьому в процесі вбудовування цифрового водяного знаку його попередньо поділяють на дві або більше частин, які не дублюються, а узгодженні між собою діалектичними зв’язками, причому кожна з них не може бути створена окремо від інших частин, та відповідно формують два або більше ключів для витягування цих частин цифрового водяного знаку окремо кожну з них.

Наявність двох або більше частин цифрового водяного знаку в копії цифрового зображення, які не дублюються, а узгодженні між собою діалектичними зв’язками, причому так, що кожна з них не може бути створена окремо від інших частин, дозволяє власникам ключів окремо один від одного ідентифікувати копію зображення та виявляти факт порушення без знання інших ключів. Узгодження різних частин цифрового водяного знаку між собою діалектичними зв’язками та неможливість створення різних частин окремо одна від одної дозволяє власнику при виявленні факту правопорушення ідентифікувати правопорушника. Крім того цей спосіб можливо використовувати для растрових зображень.

Метод захисту реалізують наступним чином.

При передачі майнового права на об'єкт авторського права складається ліцензійна угода, яка підписується електронними цифровими підписами різних сторін. Таким чином, вони підтверджують згоду один з одним. Після того довірена особа або апаратний пристрій вбудовує цифровий водяний знак в оригінал зображення, який складається з цих електронних цифрових підписів таким чином, що біти ЦВЗ складаються по черзі з біт електронних цифрових підписів. При цьому кожен з цифрових підписів формує окрему частину ЦВЗ. Для приховування даних використовують частотну область контейнера. Зображення розбивається на блоки розмірністю 8 × 8 пікселів і до кожного блоку застосовується двовимірне дискретне косинусне перетворення (ДКП). Кожен блок придатний для запису одного біта інформації. Перед вбудовуванням ЦВЗ довільним образом вибираються стільки блоків ДКП, скільки бітів в ЦВЗ.

Далі для вбудовування кожного біту даних беруть черговий блок ДКП, що входить в обрану групу блоків. Вибираються N довільних коефіцієнтів ДКП зі смуги середніх та низьких частот, які задаються координатами (υ_1,ν_1), (υ_2,ν_2), …, (υ_N,ν_N). Також вибирають дві фіксовані величини S та P. Для передачі біта «0» коефіцієнти з координатами (υ_1,ν_1), (υ_2,ν_2), …, (υ_N,ν_N) змінюються так, щоб середнє арифметичне цих коефіцієнтів стало не нижче величини $S+P$. А для передачі біта «1» змінюються так, щоб їх середнє арифметичне стало не вище, ніж $(S-P)$. Після цього проводиться зворотне ДКП. Для вибору оптимального значення S, обчислюють математичне очікування значення середнього очікування коефіцієнтів з координатами (υ_1,ν_1), (υ_2,ν_2), …, (υ_N,ν_N) на основі вибірки з деякої кількості блоків ДКП. Поріг вбудовування P впливає на стійкість стеганосистеми, а само чим більше P, тим більша стійкість стеганосистеми до спотворень зображення, але тим більше погіршується якість зображення при вбудовуванні інформації. Для витягування i біту даних формується ключ K_{bi}, який складається з номеру блоку ДКП та координат (υ_1,ν_1), (υ_2,ν_2), …, (υ_N,ν_N).

Після вбудовування ЦВЗ кожна з сторін, що приймає участь в ліцензійній угоді, отримує ключ, який складається зі значень K_{bi}, необхідних для витягування бітів електронного цифрового підпису одного з інших учасників.

При витягуванні бітів цифрового водяного знаку з відомого блоку ДКП та відомих коефіцієнтів з координатами (υ_1,ν_1), (υ_2,ν_2), …, (υ_N,ν_N), якщо середнє арифметичне значення коефіцієнтів з координатами (υ_1,ν_1), (υ_2,ν_2), …, (υ_N,ν_N) більше ніж S, то витягується значення 0, інакше витягується значення 1.

Приклад конкретного виконання.

Нехай видавництво вирішило придбати майнові права на фотографію власником якої є фотостудія або приватний фотограф. Для цього представники обох сторін підписують ліцензійний договір, який містить зменшену копію зображення, своїми електронними цифровими підписами.

При цьому будуть згенеровані електронні коди Е1 – електронний цифровий підпис ліцензіата та Е2 – електронний цифровий підпис ліцензіара. Крім того, електроний нотаріус [44,45] створює мітку часу для підписаного ліцензійного договору та завіряє її своїм електронним цифровим підписом, тим самим отримує електронний код – Е3. Далі довірена особа Т або апаратний пристрій отримує оригінал зображення та електронні коди Е1, Е2, Е3 та вбудовує цифровий водяний знак, що представляє собою біти Е1, Е2 та Е3, які чергуються.

Для витягу цифрового водяного знаку формуються три ключі – К1, К2 та К3 так, що ключ К1 дозволяє витягувати тільки Е1, ключ К2 дозволяє витягувати тільки Е2, ключ К3 дозволяє витягувати тільки Е3.

Після вбудовування ЦВЗ ліценціат отримує ключ, який складається зі значень, необхідних для витягування бітів електронного цифрового підпису ліцензіара. А ліцензіар навпаки отримує ключ, який складається зі значень, необхідних для витягування бітів електронного цифрового підпису ліцензіата. Електронний нотаріус отримує ключ, який складається зі значень, необхідних для витягування бітів свого електронного цифрового підпису.

Таким чином після вбудовування ЦВЗ ліценціат отримує ключ К2, який дозволяє витягнути із зображення ЕЦП ліцензіара, а ліцензіар отримує ключ К1, що дозволяю витягувати ЕЦП ліцензіата. Ключ К3 отримує електронний нотаріус.

При появі суперечки стосовно порушення авторського права як стороною, що отримала ліцензію так і самим ліцензіаром, може знадобиться підтвердження факту підписання ліцензійної угоди в судовому процесі.

В такому випадку, для захисту своїх прав при легальному використанні зображення ліцензіат може пред’явити в судовому процесі ліцензійний договір разом зі своїм ключем для витягу електронного цифрового підпису ліцензіара. А для захисту прав ліцензіара у випадку виявлення правопорушення, він може пред’явити в судовому процесі ліцензійний договір разом зі своїм ключем для витягу електронного цифрового підпису ліцензіата. Крім того може бути залучено електронного нотаріуса для підтвердження мітки часу.

При випробуваннях запропонованого методу захиста цифрових зображень виявилося, що простота реалізації алгоритму дозволить використовувати його як в великих так і в невеликих програмах і не підвищує вартість розробки. Розміщення електронних цифрових підписів ліцензіата, ліцензіара та електронного нотаріуса безпосередньо в статичне зображення, у вигляді цифрового водяного знаку виключає можливість використання об’єкту авторського права окремо від ліцензійного договору. Тим самим при появі контрафактної копії зображення, правовласник може швидко ідентифікувати правопорушника, а порушення умов ліцензійного договору виявлено та доказано в судовому процесі, завдяки витягування електронного цифрового підпису ліцензіата. Крім того, невиправдане звинувачення може бути спростовано ліцензіатом завдяки витягуванню

електронного цифрового підпису ліцензіара. А при появі суперечки може бути залучено електронного нотаріуса для доказу факту підписання договору, завдяки витягуванню електронного цифрового підпису нотаріуса.

1.1.2 Комп'ютерна програма для захисту цифрових зображень

Комп'ютерна програма для захисту цифрових зображень [3] призначена для створення перешкод порушенню авторського та суміжних прав при розповсюдженні цифрових зображень, а само для виявлення факту порушення авторських або суміжних прав. Програма може бути використана у випадку, коли при передачі твору підписується ліцензійна угода між ліцензіаром та ліцензіатом.

Розміщення електронних цифрових підписів ліцензіата, ліцензіара та електронного нотаріуса безпосередньо в статичне зображення, у вигляді цифрового водяного знаку виключає можливість використання об'єкту авторського права окремо від ліцензійного договору. Тим самим при появі контрафактної копії зображення, правовласник може швидко ідентифікувати правопорушника, а порушення умов ліцензійного договору може бути виявлено та доказано в судовому процесі, завдяки витягування електронного цифрового підпису ліцензіата. З іншого боку невиправдане звинувачення може бути спростовано ліцензіатом завдяки витягуванню електронного цифрового підпису ліцензіара. А при появі суперечки може бути залучено електронного нотаріуса для доказу факту підписання договору, завдяки витягуванню електронного цифрового підпису нотаріуса.

Таким чином, програма складається з двох частин, перша з яких дозволяє вбудовувати в цифрове зображення в форматі jpg цифровий водяний знак (ЦВЗ), а друга перевіряти наявність ЦВЗ в цифровому зображенні.

Функціонування системи.

Оскільки основне призначення програми – це створення перешкод порушенню авторського та суміжних прав на цифрові зображення, загальний процес роботи у програмі можна означити наступними положеннями.

При передачі майнового права на об'єкт авторського права складається ліцензійна угода, яка підписується електронними цифровими підписами різних сторін. Таким чином вони підтверджують згоду один з одним.

Після того отримані ЦВЗ додаються в розроблену комп'ютерну програму разом з цифровим зображенням. Програма вбудовує цифровий водяний знак в оригінал зображення таким чином, що біти ЦВЗ складаються по черзі з біт електронних цифрових підписів. При цьому кожен з цифрових підписів формує окрему частину ЦВЗ. Для приховування даних використовується частотна область

контейнера. Зображення розбивається на блоки розмірністю 8 × 8 пікселів і до кожного блоку застосовується двовимірне ДКП.

Для вбудовування кожного біту даних беруть черговий блок ДКП, що входить в обрану групу блоків. Вибираються N довільних коефіцієнтів ДКП зі смуги середніх та низьких частот, які задаються координатами (υ_1,ν_1), (υ_2,ν_2), …, (υ_N,ν_N). Також вибирають дві фіксовані величини S та P. Для передачі біта «0» коефіцієнти з координатами (υ_1,ν_1), (υ_2,ν_2), …, (υ_N,ν_N) змінюються так, щоб середнє арифметичне цих коефіцієнтів стало не нижче величини $S+P$. А для передачі біта «1» змінюються так, щоб їх середнє арифметичне стало не вище, ніж $(S-P)$. Після цього проводиться зворотне ДКП. Для вибору оптимального значення S обчислюють математичне очікування значення середнього очікування коефіцієнтів з координатами (υ_1,ν_1), (υ_2,ν_2), …, (υ_N,ν_N) на основі вибірки з деякої кількості блоків ДКП. Поріг вбудовування P впливає на стійкість стеганосистеми, а саме: чим більше P, тим більша стійкість стеганосистеми до спотворень зображення, але тим більше погіршується якість зображення при вбудовуванні інформації. Для витягування i-того біту даних формується ключ K_{bi}, який складається з номеру блоку ДКП та координат (υ_1,ν_1), (υ_2,ν_2), …, (υ_N,ν_N). З ключів K_{bi} складається секретний код для кожного учасника процесу.

Витягування бітів цифрового водяного знаку з відомого блоку ДКП та відомих коефіцієнтів з координатами (υ_1,ν_1), (υ_2,ν_2), …, (υ_N,ν_N) відбувається наступним чином. Якщо середнє арифметичне значення коефіцієнтів з координатами (υ_1,ν_1), (υ_2,ν_2), …, (υ_N,ν_N) більше ніж S, то витягується значення 0, інакше витягується значення 1.

Структура та організація даних.

Програма являє собою набір класів, в роботі яких використовуються локальні змінні, приватні атрибути, а також публічні атрибути та методи.

Основний функціонал програми представлено наступними методами на мові програмування C#: public float[,][,] EmbedWatermark(float[,][,] DCT, int imax, int jmax, float Sum, float P) – метод для вбудовування ЦВЗ; public string ExtractWatermark(float[,][,] DCT_emb, int imax, int jmax, float Sum) – метод для витягування ЦВЗ; public static float[,] DirectDct(float [,] image) – метод для виконання прямого ДКП; public static float[,] InverseDct(float[,] array) – метод для виконання зворотного ДКП; public float[,] GetBrightArray() – отримання матриці пікселів зображення; public Bitmap TransformToImage(float[,][,] DCT, int DCTWidth, int DCTHeight) – збереження зображення по відомій матриці ДКП.

Вимоги до програмного та апаратного забезпечення.

Програма призначена для експлуатації на IBM-сумісних персональних комп’ютерах. Для використання програми необхідно мати таку апаратну та програмну конфігурацію: 32- або 64-розрядний процесор архітектури x86 зі швидкодією не менше 433 МГц; оперативна пам’ять – не менше 256 МБ; жорсткий

диск з обсягом вільного дискового простору не менше 130 МБ; - кольоровий графічний дисплей – 16 млн. кольорів, 800x600 або вище; пристрій для читання компакт-дисків (для встановлення програми); миша; операційна система Microsoft Windows ME, Microsoft Windows 2000 Professional/Server з пакетом оновлення 3 або вище, Microsoft Windows XP, Microsoft Windows 2003 Server, Microsoft Windows Vista або Windows 7.

Для роботи програми в операційній системі повинен бути встановлений програмний компонент «.NET Framework 3.5».

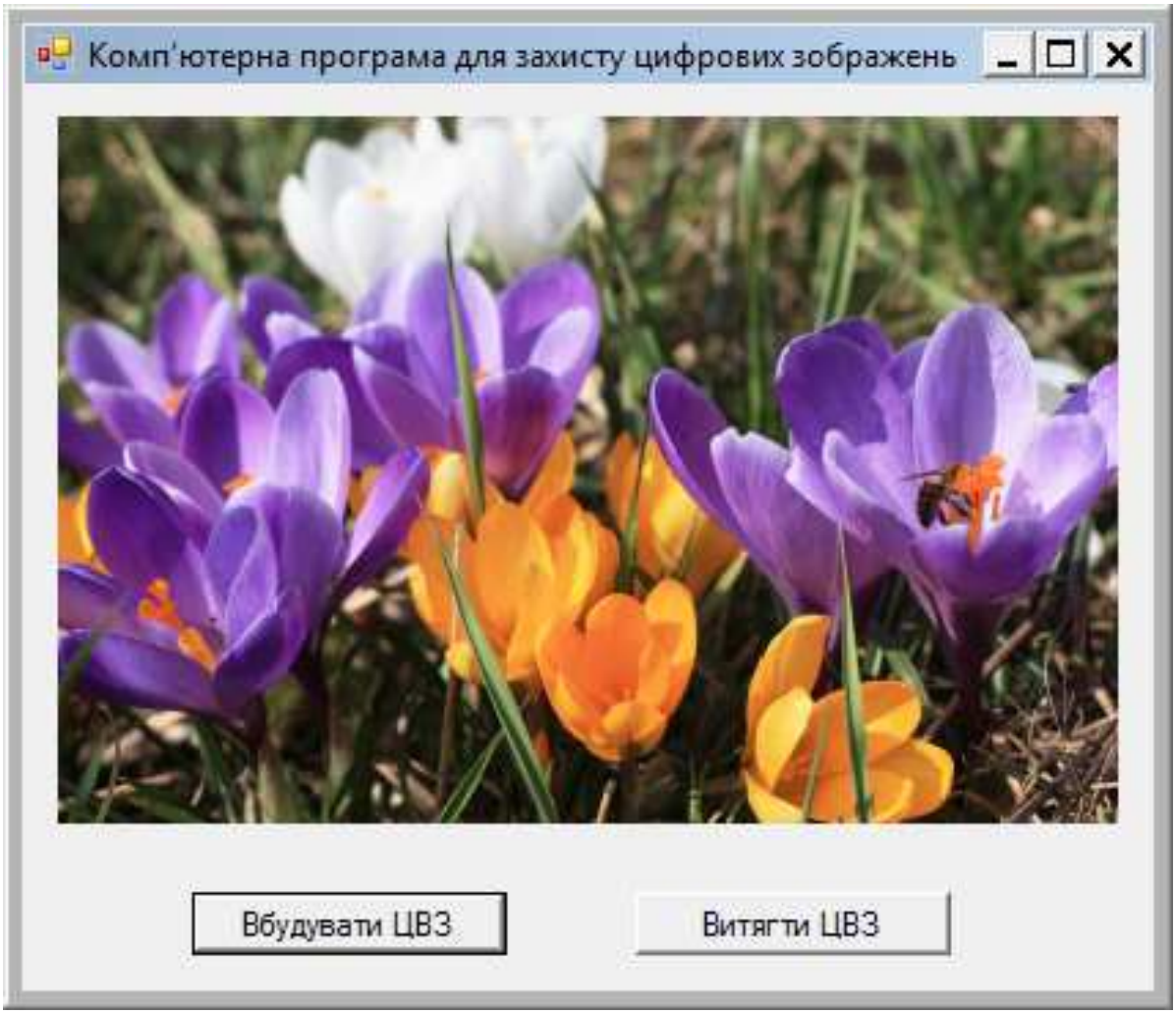


Рисунок 1.1 – Вбудовування цифрового водяного знаку в зображення

Також для коректної роботи програми в регіональних настроюваннях операційної системи повинен бути встановлений російський або український мовний стандарт.

У разі невідповідності ПК цим вимогам коректна робота АРМ не гарантується.

Методика роботи користувача з програмою.

Програма розповсюджується у вигляді вихідних кодів.

Нехай видавництво вирішило придбати майнові права на фотографію, власником якої є фотостудія або приватний фотограф. Для цього представники обох сторін підписують ліцензійний договір, який містить зменшену копію зображення, своїми електронними цифровими підписами.

При цьому будуть генеровані електронні коди Е1 – електронний цифровий підпис ліцензіата та Е2 – електронний цифровий підпис ліцензіара. Крім того, електронний нотаріус створює мітку часу для підписаного ліцензійного договору та завіряє її своїм електронним цифровим підписом. Тим самим він отримує електронний код – Е3. Далі за допомогою комп'ютерної програми необхідно вбудувати цифровий водяний знак, що представляє собою біти Е1, Е2 та Е3, що йдуть послідовно один за іншим.

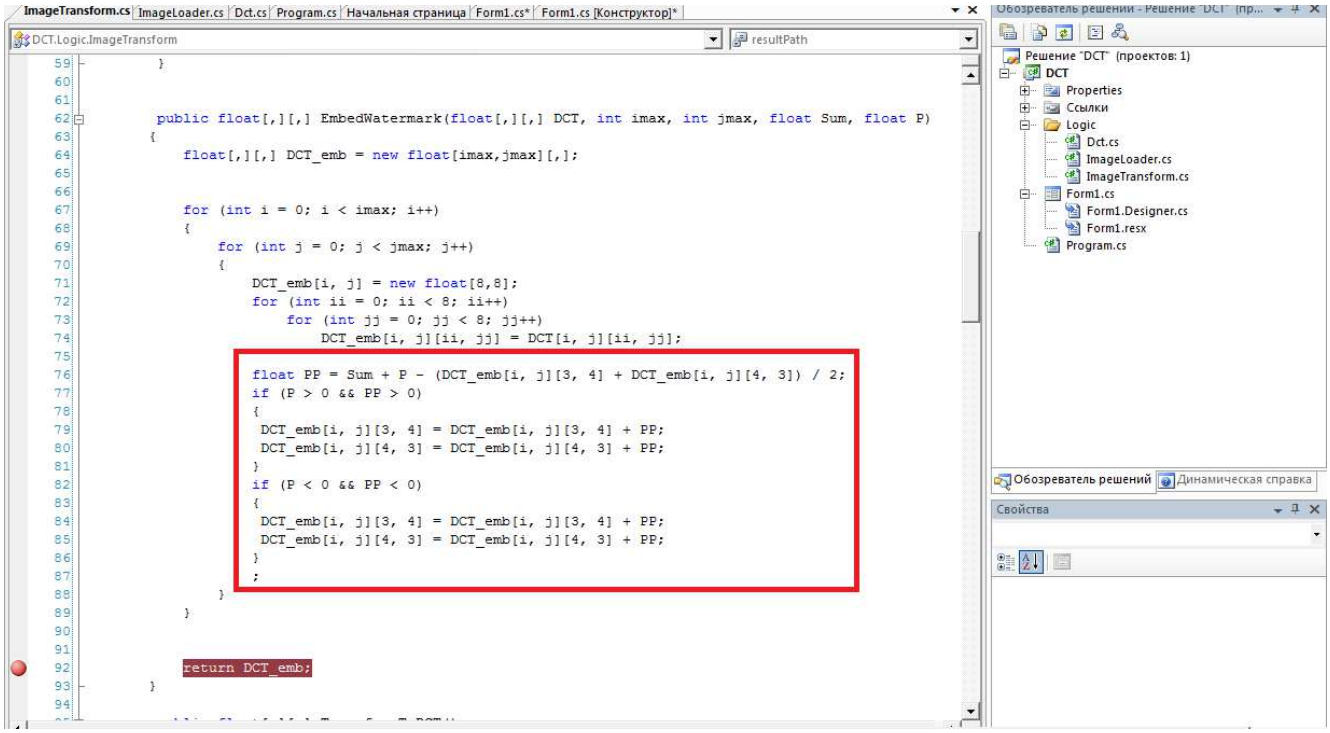


Рисунок 1.2 – Зміна коефіцієнтів для вбудовування цифрового водяного знаку

Для захисту цифрового зображення необхідно натиснути кнопку «Вбудувати ЦВЗ» (рис. 1.1). При цьому буде вбудований цифровий водяний знак в оригінал зображення.

Для витягування цифрового водяного знаку необхідно натиснути кнопку – «Витягти ЦВЗ» (рис. 1.1).

Для того щоб вибрати коефіцієнти ДКП, які використовуються для збереження ЦВЗ, необхідно змінити відповідні строки коду в методах EmbedWatermark та ExtractWatermark (рис. 1.2). Для того щоб вибрати оригінал зображення, необхідно змінити відповідні дані в методі ImageLoader (рис. 1.3).

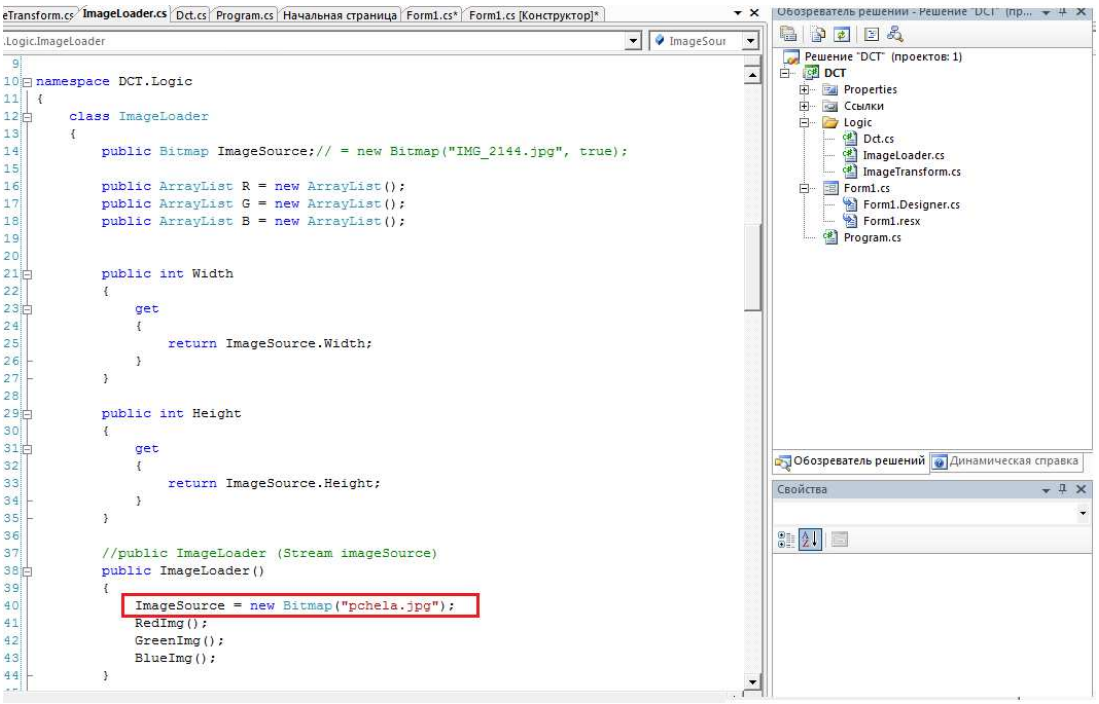
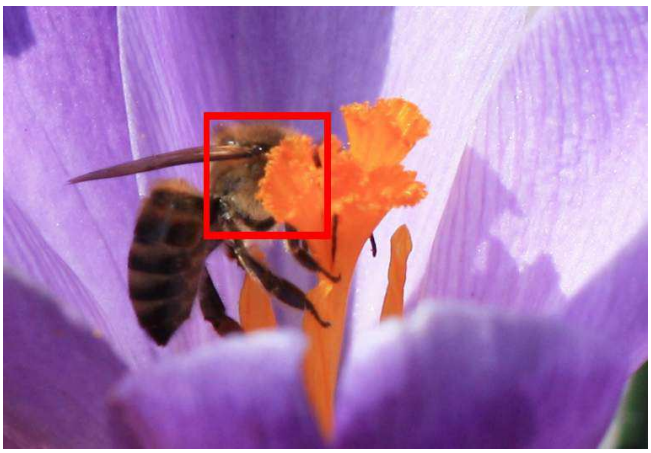


Рисунок 1.3 – Вибір зображення для вбудовування цифрового водяного знаку

Приклад роботи програми для різних значень порога вбудовування P представлено на рисунку 1.4.



\

Рисунок 1.4 – Зображення бджоли (оригінал) та обраний фрагмент для вбудовування ЦВЗ

На рисунку 1.5а) показаний фрагмент каналу синього кольору для зображення бджоли з вбудованим ЦВЗ з порогом вбудовування P = 5, на рисунку 1.5б) - ЦВЗ з порогом вбудовування P = 25 , а на рисунку 1.5в) - з порогом вбудовування P = 45.

а) P=5

б) P=25

в) P=45

Рисунок 1.5 – Канал синього кольору фрагмента зображення бджоли з вбудованим водяним знаком і порогом вбудовування

Приклади показують, що чим більше поріг вбудовування, тим сильніше погіршується якість зображення при вбудовуванні ЦВЗ.

Таким чином, використання запропонованого методу дозволяє значно знизити ризики несанкціонованого розповсюдження цифрових зображень, зокрема, для растрових зображень. У випадку, коли це сталося, програма надає можливість правовласнику як виявити правопорушника, так і захистити своє право в судовому чи адміністративному порядку.

1.2 Дослідження організаційно-технічних способів захисту інформації

Організаційно-технічні способи захисту інформації розглядаються в роботах [7–14]. Досліджено проблеми витоку інформації в каналах мобільного зв'язку та запропонована комплексна система захисту мовної інформації в приміщенні. Розглянуто організація доступу до інформації засобами біометричної аутентифікації та можливості використання ДНК-чипів в системах контролю та доступу. Досліджено та проаналізовано застосування сучасних технічних засобів захисту інформації в інформаційних мережах та методів апаратного захисту програмного забезпечення.

1.2.1 Комплексна система захисту мовної інформації в приміщенні

В даний час актуальність захисту мовної інформації від витоку по технічним каналам безперечна. Особливо це стосується обговорення конфіденційної інформації при проведенні нарад та переговорів в комерційних та державних підприємствах і установах.

Існує маса можливостей несанкціоновано зняти мовну інформацію. Один з найпростіших способів - це прослуховування розмови за допомогою радіозакладного пристрою, встановленого в офісі. Інший поширений спосіб - прослуховування приміщень за допомогою мікрофона телефонного апарату. Здається, що якщо слухавка не піднята, то і нема можливості використовувати мікрофон в якості засобу зняття інформації. Насправді це можливо з використанням високочастотного наведення. Ще один дуже поширений метод - це прослуховування звукових хвиль мовної інформації, що передаються через перегородки, стіни, вікна, батареї опалення, вентиляційні отвори, тощо. Для цього в даний час використовуються електронні стетоскопи. Для прослуховування приміщень, що

мають вікна можуть застосовуватися пристрої, що працюють в оптичному діапазоні - лазерні детектори.

Удосконалення інженерно-технічного захисту інформації в приміщенні для проведення переговорів є одним із заходів захисту інформації в організації.

В роботі [9] розглянуті активні засоби захисту мовної інформації.

На основі проведеного аналізу сучасної літератури з даного питання, авторами роботи було: проаналізовано вірогідності перехоплення конфіденційної мовної інформації залежно від конкретних вхідних даних; запропоновано заходи протидії для різних каналів, способів і засобів перехоплення мовної інформації; розглянуто основні сучасні пристрої захисту мовної інформації.

1.2.2 Дослідження можливості використання ДНК-чіпів в системах контролю і доступу

У системах контролю та доступу до конфіденційної інформації [46,47]все частіше перевагу надають біометричному способу ідентифікації та автентифікації. ДНК людини є носієм унікальної інформації про особистість, а отже, цю перевагу слід використовувати для практичного використання.

ДНК-чіпи дозволяють за короткий термін розпізнати людину по її ДНК В цілому, ДНК-чіп – це вид БІО-чіпу, що орієнтований на розпізнавання поліморфізму ДНК людини, та являє собою невелику (від декількох міліметрів) пластинку зі скла, пластику або кремнію, на яку наносяться біологічні макромолекули (ДНК, білки, у тому числі і ферменти, клітини). Ці адсорбенти здатні вибірково зв'язувати речовини, що містяться в аналізованому розчині. Використовувати такі чіпи можливо, але сам процес добування інформації зводиться до надання необхідних ферментів, а саме, крові, плазми та інших біологічно активних рідин тіла людини.

На даний час для проведення ДНК-тесту використовується мінілабораторія, яка потребує майже 10 хвилин для отримання результату. Цей термін, звичайно, не прийнятний, оскільки термін встановлення відповідності особи має бути мінімальним.

Дослідження сучасних досягнень біоінженерії дозволили зробити висновок, що ДНК-чіпи мають своє майбутнє. Зокрема, пропонується для систем контролю та доступу використовувати ДНК-чіпи, що імплантуються безпосередньо в людину. Це дає змогу встановити особу з дуже високою ймовірністю. При імплантації такий аналіз необхідно проводити постійно з метою виключення можливості пере живлення ДНК-чіпу.

Імплантація чіпів, виготовлених на базі скла, пластику або кремнію, не прийнятна. Для встановлення особистості потрібно використовувати чіпи нового покоління, виготовлених з використанням біомолекул. Ця технологія використовує біохімічні кола, а в якості носія заряду виступають хімічні сполуки. Такі чіпи можна імплантувати до артерії, чи до вени людини, що забезпечує надшвидкий ДНК-тест, а отже, і процес встановлення особи.

Для зчитування інформації з такого чіпа потрібен безконтактний зчитувач особистих даних. Сучасні компанії-виробники вже пропонують такі зчитувачі.

Використовуючи таке впровадження, процес ідентифікації та автентифікації займає декілька секунд, оскільки тест ДНК в імплантованому чіпі виконується постійно. Одним із варіантів впровадження запропонованого вирішення питання встановлення особи може бути наступний приклад (рис. 1.6).

Рисунок 1.6 – Приклад імплантації ДНК-чіпа

Запропонований підхід з питань ідентифікації/автентифікації з використанням імплантованого чіпа є найбільш точним і швидким. Це є вагома перевага для систем контролю і доступу. Але, слід зазначити, що сама процедура імплантації не для всіх людей прийнятна, оскільки велику роль грають особисті властивості особи. Використовувати таку систему пропонується лише тоді, коли інформація, що потребує захисту, має надзвичайну цінність.

1.2.3 Дослідження способів реалізації загрози типу «злом пароля»

Злом пароля – це процес відновлення пароля (або секретної фрази) в електронних системах, який звичайно супроводжується використанням спеціалізованих програмних засобів. Методи, що застосовують для виконання задачі злому пароля, вдосконалюються досить швидко. Існує велика кількість програмного забезпечення, що використовує підходи, засновані на методах підбору пароля. За декілька останніх років почастішали випадки крадіжок паролів користувачів методами соціальної інженерії.

Коли говориться про злом пароля, то найчастіше під цим розуміються несанкціоновані спроби зловмисника (хакера) отримати доступ до певної електронної або програмної системи. Поряд з цим методи злому пароля також використовуються для цілком законних задач, наприклад: відновлення втраченого (або забутого) пароля; досить часто виконання цієї операції вимагає наявності підвищених привілеїв у цільовій системі; тестування систем автентифікації та безпеки програмного забезпечення; виконується системними адміністраторами та розробниками програмних засобів під час аудиту та у процесах оцінки якості.

Однією з найпоширеніших способів злому є атака методом повного перебору (грубої сили). Цей метод схожий на атаку за словником, але з додатковими можливостями по виявленню фраз, що не містяться в словнику, перебираючи всі можливі літеро-цифрові комбінації (A-Za-z0-9), а також спеціальні символи.

Це не швидкий спосіб, особливо, якщо пароль містить комбінації різних груп символів. Проте сьогодні вже існують засоби підвищення ефективності подібних методів за допомогою можливостей апаратного забезпечення. Методи повного перебору та перебору за словником можуть бути вдосконалені за допомого сучасних графічних процесорів (GPU), розподілених обчислювальних моделей, технологій хмарних обчислень, а також зомбі-ботнетів.

Ще один спосіб злому – атака з використанням райдужних таблиць. Райдужна таблиця – це перелік попередньо обчислених хешей (числових значень зашифрованих паролів), використовуваних більшістю сучасних систем. Цей спосіб припускає, що можливим є отримання хеша пароля, а також що алгоритми хеша пароля і хеша таблиці співпадають. Таблиця включає в себе хеши всіх можливих комбінацій паролів для будь-якого виду алгоритму хешування.

Час, необхідний для злому пароля за допомогою райдужної таблиці, зводиться до того часу, який потрібен, щоб знайти захешованний пароль у списку. Тим не менше, сама таблиця величезна і для перегляду вимагає серйозних обчислювальних потужностей та ресурсів пам'яті. Також вона буде даремна, якщо хеш, який вона намагається знайти, був ускладнений додаванням випадкових символів до паролю до застосування алгоритму хешування.

В роботі виконується аналіз основних підходів до реалізації загрози типу «Злом паролю», наводиться порівняльна характеристика, а також огляд деяких програмних засобів.

1.2.4 Апаратний захист програмного забезпечення. Технологія HASP

Одними з найпоширеніших способів апаратного захисту програмного забезпечення від неліцензійного копіювання [48-50], на сьогоднішній день, є USB-

ключі. Ці пристрої забезпечують не тільки безпеку програм від незаконного використання, але і дозволяють розробникам застосовувати складні способи ліцензування.

Основним апаратним засобом для захисту ПЗ є серія електронних ключів HASP від компанії Aladdin Software Security RD. Більше 2/3 ринку пристроїв для захисту програмного забезпечення від нелегального використання належить таким ключам. Область застосування цього продукту: захист готових програм, авторизація в операційних системах, захист окремих документів, мультімедіа роликів, конфігурацій 1С.

На даний момент з'явилася можливість обходу апаратного захисту HASP це бітхак. Бітхак - це програмне емулювання як самого ключа, так і USB-шини з віртуальним ключем.

Головними недоліками системи захисту ПЗ HASP4 є можливість перехоплення викликів диспетчера введення-виведення, перехоплення шифрованих даних з подальшим дешифруванням, емулювання апаратного ключа.

Модель драйвера HASP4 описується в структурі DRIVER_OBJECT. Ця модель зберігає масив обробників повідомлень. Цей факт надає можливість перехоплювати і підміняти IRP-пакети, підставляючи ліцензійні дані. Маючи дамп ключа захисту, можна передати його програмі, яка перевіряє вірність ліцензійних даних. Так само існує також можливість розробки драйвера віртуального ключа. Для цього також потрібен дамп ключа, а підстановка даних здійснюється в режимі емуляції (рис. 1.7). Тобто драйвер захисту зможе звертатися з віртуальним ключем так само, як і з фізичним.

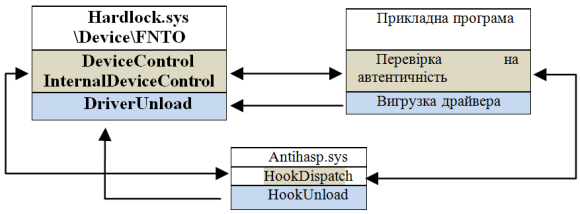


Рисунок 1.7 - Структурна схема програми емулятора

Апаратний ключ HASP має унікальний номер і містить всю необхідну для копіювання інформацію, але для доступу до нього потрібні програмні ключі. Вміст пакетів шифрується публічним симетричним алгоритмом AES (Advanced Encryption Standard). Для розшифровки повідомлень використовується перехоплення пакетів з ключем і перехват пакетів без ключа. Ключі витягуються з перехоплених пакетів методом брутфорс. Ключ використовується для зняття отриманого дампа: тип, ідентифікатор, порт підключення (рис. 1.8).

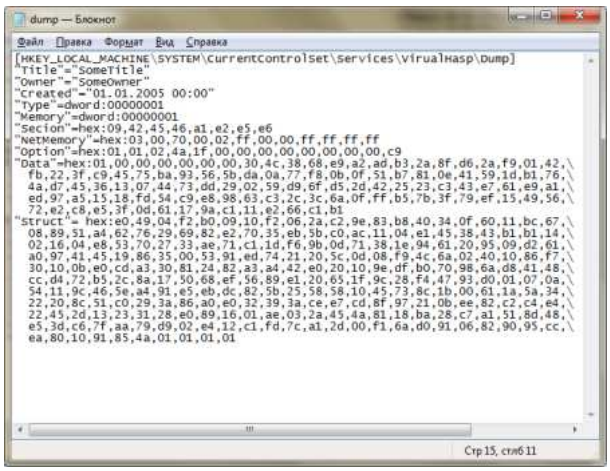


Рисунок 1.8 – Приклад дампа ключа

Рішення проблеми емуляції портів може бути таким, що якщо застосувати більш стійкі алгоритми шифрування такі як RC5 з довжиною ключа 1024, то загрозу перебору ключа шифрування для доступу до пакету можна буде нейтралізувати. Застосування динамічної генерації даних для перевірки ключа, дасть можливість захиститися від перехоплення пакетів. Також не менш важливим, є підвищення захисту коду драйвера, що дає змогу захистити драйвер від відладки після компіляції.

В роботі було описано недоліки програмно-апаратного захисту HASP4 та запропоновані рішення для їх мінізації. На сьогоднішній день компанія-розробник даної системи захисту, представила принципово новий метод захисту HASP HL. Нові модулі більше не містять в собі ключі які необхідні для запуску програм, а замість цього пристрій HASP HL використовується для зняття хеш-зліпка апаратної частини системи, необхідного для реєстрації програми в мережі Інтернет.

Запропоновані рішення щодо підвищення стійкості алгоритму до взлому, може вирішити проблему неліцензійного копіювання, та залишити вартість системи захисту на тому ж рівні. Дані рішення не дають повної гарантії від неліцензійного використання програмного забезпечення, але вони суттєво ускладнюють можливість взлому, і зводять нанівець раціональність таких дій в порівнянні з купівлею ліцензованого програмного забезпечення.

На даний час вартість системи захисту технології HASP4 становить $ 30-45, вартість системи захисту HASP HL – $ 45-250.

2 РОЗРОБКА МАТЕМАТИЧНИХ МЕТОДІВ ЗАХИСТУ ІНФОРМАЦІЙНИХ СИСТЕМ

2.1 Протокол сліпого цифрового підпису на еліптичних кривих

На часі разом із завданнями реалізації стандартних схем електронного цифрового підпису (ЕЦП) практичну актуальність і значущість мають реалізації інших схем, зокрема, сліпого підпису.

Сліпий ЕЦП дозволяє авторові документа довести його юридичну значимість, не розкриваючи власної особи. Це може знадобитися, зокрема, при проведенні електронного голосування чи розрахунку електронними грошима.

В типовій схемі сліпого підпису, як правило, приймають участь три сторони – емітент документу, підписувач та валідатор. Емітент створює документ, який має підписати підписувач. При цьому, підписувач не має знати вмісту документа та вигляду остаточного підпису, для чого емітент маскує документ за допомогою певного криптографічного перетворення. Підписувач підписує замаскований документ, а емітент на основі його підпису формує остаточний ЕЦП під документом у відкритому вигляді згідно зі схемою сліпого підпису. Валідатор перевіряє правильність підпису за допомогою відкритого ключа емітента.

Наприклад, в схемі електронного голосування в якості емітента виступає виборець, підписувача – дільнична виборча комісія, валідатора – центральна виборча комісія. Виборець заповнює бюлетень, маскує його, щоб зберегти конфіденційність голосу, і передає на підпис у дільничну виборчу комісію. Комісія, засвідчивши особу виборця, підписує його бюлетень, не знаючи, за кого той проголосував. Центральна виборча комісія отримує бюлетень у відкритому вигляді і перевіряє валідність підпису дільничної комісії, не знаючи при цьому, хто заповнив цей бюлетень.

Таким чином, у випадку сліпого ЕЦП до критеріїв захищеності схеми підпису додається анонімність – неможливість відстежити за підписаним документом його автора і однозначно їх пов’язати. Втім, в деяких схемах у підписувача може виявитись можливість порушити анонімність, оскільки в процесі формування остаточного підпису він обмінюється з емітентом документа додатковими параметрами, передбаченими схемою підпису. Якщо підписувач збереже ці параметри, пов’язавши їх з конкретним емітентом, а в подальшому зможе отримати доступ до документу із власним підписом у відкритому вигляді, то він зможе спробувати вирахувати його автора за допомогою збережених параметрів. Обчисливши маскуючі параметри, які використовував емітент, підписувач зможе однозначно пов’язати його із документом, що призведе до порушення анонімності. Наприклад, в схемі електронного голосування це означатиме, що буде відомо, за кого проголосував конкретний виборець.

Пропонується реалізація протоколу сліпого цифрового підпису, що являє собою модифікацію стандарту ГОСТ Р 34.10-2001 на еліптичних кривих над скінченим векторним полем. Аналізується захищеність запропонованого протоколу за критерієм анонімності. Показано, що зміна математичного апарату не впливає на захищеність схеми сліпого підпису за критерієм анонімності.

2.1.1 Еліптичні криві над скінченим векторним полем

Розглянемо одне з можливих розширень поля Галуа $GF(p)$ – скінчене векторне поле. В СВП входять вектори певної довжини n

$$\nu = \nu_1 \cdot e_1 + \nu_2 \cdot e_2 + ... + \nu_n \cdot e_n = (\nu_1, \nu_2, ..., \nu_n), \quad (2.1)$$

де $\nu_i \in GF(p)$,

e_i – базисні вектори, $i = 1,2,...,n$.

На множині векторів визначимо операції додавання та множення.

Додавання двох векторів $u = (u_1, u_2, ..., u_n)$ та $\nu = (\nu_1, \nu_2, ..., \nu_n)$ відбувається за формулою

$$w = u + \nu = (u_1 + \nu_1 \bmod p, u_2 + \nu_2 \bmod p, ..., u_n + \nu_n \bmod p). \quad (2.2)$$

Одиничним елементом за операцією додавання є вектор $u_0 = (0,0,...,0)$. Відповідно, вектор $u = (u_1, u_2, ..., u_n)$ називається оберненим до вектора $\nu = (\nu_1, \nu_2, ..., \nu_n)$, якщо $u + \nu = u_0$, тобто

$$\nu = -u = (-u_1 \bmod p, -u_2 \bmod p, ..., -u_n \bmod p). \quad (2.3)$$

Множення вектора ν на число k реалізується за формулою

$$k \cdot u = (k \cdot u_1 \bmod p, k \cdot u_2 \bmod p, ..., k \cdot u_n \bmod p). \quad (2.4)$$

Позначимо операцію множення двох векторів знаком «◦». Ця групова операція мультиплікативної групи СВП визначається асоціативною таблицею множення базисних векторів [51], коефіцієнти перемножуються за принципом множення многочленів. В якості одиничного елемента СВП оберемо, наприклад, вектор $v_0 = (1,0,...,0)$. Відповідно, два елементи СВП, результатом множення яких між собою є одиничний елемент, називаються взаємно оберненими.

Проілюструємо правило множення базисних векторів для довжини вектора $n=2$ за допомогою табл.2.1, для $n=3$ – табл. 2.2. Значення розтягуючих коефіцієнтів τ і μ обчислюються з системи характеристичних рівнянь, що задає існування оберненого вектора для будь-якого заданого v_0.

Таблиця 2.1. Множення базисних векторів СВП для $n=2$

$\circ$	e_1	e_2
e_1	e_1	e_2
e_2	e_2	$\tau \cdot e_2$

Відповідно до табл. 2.1 система характеристичних рівнянь для $n=2$ має вигляд

$$v_2 \cdot x + v_1 \cdot y = 0 \bmod p. \qquad (2.5)$$

Якщо визначник $\Delta = v_1^4 - \tau \cdot v_2^4 \bmod p$ системи (2.5) приймає нульове значення, то для вектора $v=(v_1,v_2)$ не існує оберненого. Звідси, τ має бути квадратичним незалишком за модулем p. Тоді всі ненульові вектори СВП будуть утворювати мультиплікативну групу порядку p^2-1.

Таблиця 2.2. Множення базисних векторів СВП для $n=3$

$\circ$	e_1	e_2	e_3
e_1	e_1	e_2	e_3
e_2	e_2	$\tau \cdot e_3$	$\tau \cdot \mu \cdot e_1$
e_3	e_3	$\tau \cdot \mu \cdot e_1$	$\mu \cdot e_2$

Відповідно до табл. 2.2 система характеристичних рівнянь для $n=3$ має вигляд

$$v_3 \cdot x + \tau \cdot v_2 \cdot y + v_1 \cdot z = 0 \bmod p. \qquad (2.6)$$

Якщо визначник системи (2.6) приймає нульове значення, то для вектора $v=(v_1,v_2,v_3)$ не існує оберненого. Величина $p-1$ має ділитися на 3, а кожен з добутків $\tau^2 \cdot \mu$ та $\tau \cdot \mu^2$ має бути кубічним незалишком за модулем p. Тоді всі ненульові вектори СВП будуть утворювати мультиплікативну групу порядку p^3-1.

Розглянемо визначення ЕК над СВП. Оскільки характеристика СВП дорівнює p, то для $p \neq 2$ та $p \neq 3$ рівняння кривої можна записувати в скороченій формі

$$y \circ y = x \circ x \circ x + a \circ x + b, \qquad (2.7)$$

де x, y, a, b – елементи СВП.

Кожна пара векторів x, y, що задовольняє рівнянню (2.7), вважається точкою ЕК. Сукупність всіх точок ЕК разом з нескінченно віддаленою точкою О складає групу точок ЕК над СВП.

Групова операція додавання точок ЕК над СВП визначається аналогічно до групової операції додавання точок ЕК над простим полем [52] з використанням операції множення векторів $\circ$. Координати точки $U = (x^U, y^U)$, яка представляє собою суму точок $S = (x^S, y^S)$ та $T = (x^T, y^T)$, визначаються за формулами

$$x^U = \lambda \circ \lambda - x^S - x^T, \tag{2.8}$$

$$y^U = \lambda \circ (x^S - x^U) - y^S. \tag{2.9}$$

Величина λ обчислюється за формулою (2.10), якщо $S \neq T$

$$\lambda = \frac{y^S - y^T}{x^S - x^T}, \tag{2.10}$$

або за формулою (2.11), якщо $S = T$

$$\lambda = \frac{3 \cdot x \circ x + a}{2 \cdot y^S}, \tag{2.11}$$

де a – коефіцієнт ЕК.

Виконання умови гладкості

$$4 \cdot a \circ a \circ a + 27 \cdot b \circ b \neq (0,0,...,0) \tag{2.12}$$

забезпечує утворення групи точками ЕК.

В криптографії застосовуються гладкі ЕК з великим простим порядком групи точок. Порядок СВП дорівнює p^n, отже оцінку порядку групи точок ЕК над СВП $ordE(p)$ за теоремою Хассе [52] можна виразити наступним співвідношенням

$$p^n + 1 - 2 \cdot \sqrt{p^n} \leq ordE(p) \leq p^n + 1 + 2 \cdot \sqrt{p^n}. \tag{2.13}$$

Згідно з нижньою границею співвідношення (2.13), для досягнення порядку групи точок ЕК величиною, наприклад, 178 біт, необхідно використовувати просте число p величиною 90 біт за довжини вектора $n = 2$.

2.1.2 Протокол сліпого підпису на еліптичних кривих над СВП

Протокол сліпого підпису базується на алгоритмі ГОСТ Р 34.10-2001, однак використовує математичний апарат ЕК над СВП.

В схемі приймають участь дві сторони: підписувач А та абонент Б. Абонент Б виступає в якості емітента документа m, який підписувач А має підписати наосліп. Валідатором може виступити будь-хто з них або третя особа. Перевірка підпису відбувається за допомогою відкритого ключа підписувача А.

Загальні параметри: скінчене векторне поле з довжиною вектора n – розширення простого поля $GF(p)$, ЕК над цим полем з групою точок простого порядку q, базова точка P, хеш-функція $H()$.

Протокол складається з трьох етапів – генерація ключів, постановка підпису, перевірка підпису.

Під час генерації ключів секретний ключ d обирається випадково з діапазону $1 < d < q$.

Відкритий ключ Q отримується з нього за формулою

$$Q = d \cdot P. \tag{2.14}$$

Оскільки ЕК задана над СВП, то при обчисленні суми двох точок в цій та подальших формулах використовуються співвідношення (2.8-2.11).

Етап постановки підпису починає підписувач А, обираючи одноразовий ключ k з діапазону $1 < k < q$, обчислюючи точку E за формулою

$$E = k \cdot P = (x^E, y^E) \tag{2.15}$$

та відправляючи цю точку абоненту Б.

Абонент Б формує хеш-образ повідомлення за співвідношенням

$$h = H(m). \tag{2.16}$$

Після цього він випадково обирає маскуючі параметри α та β з діапазону $1 < \alpha, \beta < q$ і обчислює точку C за формулою

$$C = \alpha \cdot E + \beta \cdot P = (x^C, y^C). \tag{2.17}$$

Абонент Б обчислює величини r та r' за формулами

$$r = \sum_{i=1}^{n} x_i^C \bmod q, \tag{2.18}$$

$$r' = \sum_{i=1}^{n} x_i^E \bmod q, \tag{2.19}$$

де $x^C = (x_1{}^C, x_2{}^C, ..., x_n{}^C)$, $x^E = (x_1{}^E, x_2{}^E, ..., x_n{}^E)$.

Абонент Б засліплює хеш-образ повідомлення за співвідношенням

$$h' = \frac{r'}{r} \cdot h \cdot \alpha \bmod q \tag{2.20}$$

і пересилає засліплений хеш-образ повідомлення h' підписувачу А.

Підписувач А формує засліплений підпис s' за допомогою власного секретного ключа d

$$s' = (d \cdot r' + k \cdot h') \bmod q, \tag{2.21}$$

та пересилає отримане значення абоненту Б.

Абонент Б має можливість перевірити справжність засліпленого підпису s' за допомогою співвідношення (2.22), використовуючи відкритий ключ Q підписувача А

$$s' \cdot P = r' \cdot Q + h' \cdot E. \tag{2.22}$$

Якщо засліплений підпис проходить перевірку, абонент Б формує з нього остаточний підпис

$$s = (s' \cdot \frac{r}{r'} + \beta \cdot h) \bmod q. \tag{2.23}$$

Сліпим підписом під документом m вважається пара значень $< r, s >$.

Валідатор при перевірці підпису $\{m, < r, s >\}$ обчислює точку R, використовуючи відкритий ключ Q підписувача А

$$R = \frac{s}{h} \cdot P - \frac{r}{h} \cdot Q = (x^R, y^R). \tag{2.24}$$

Якщо виконується співвідношення

$$r = \sum_{i=1}^{n} x_i^R \bmod q, \tag{2.25}$$

де $x^R = (x_1^R, x_2^R, ..., x_n^R)$, підпис вважається справжнім

2.1.3 Перевірка захищеності протоколу за критерієм анонімності

Для схем сліпого підпису, на відміну від інших різновидів ЕЦП, актуальною є атака порушення анонімності. Спроба атаки може бути здійснена підписувачем за умови, що він зберігатиме всі відомі йому параметри схеми сліпого підпису разом із ідентифікатором емітента для кожної сесії постановки підпису. Накопичена база даних може бути використана в атаці, яка полягає у спробі визначення автора відомого документа m із підписом $< r, s >$, що проходить перевірку за допомогою відкритого ключа підписувача Q.

В запропонованому протоколі атака порушення анонімності може бути здійснена наступним чином. Підписувач А для кожного рядка своєї бази даних має обчислити ймовірні засліплюючи параметри α' та β' за формулами (2.26-2.27)

$$\alpha' = \frac{r \cdot h'}{h \cdot r'} \bmod q, \tag{2.26}$$

$$\beta' = \frac{s - s' \cdot \dfrac{r}{r'}}{h} \bmod q, \tag{2.27}$$

За допомогою обчислених параметрів підписувач А для кожного рядка бази даних обчислює точку R' за формулою (2.28)

$$R' = \alpha' \cdot E + \beta' \cdot P = (x^{R'}, y^{R'}). \tag{2.28}$$

Рядок бази даних, для якого виконається співвідношення (2.29) має вказати на емітента повідомлення

$$r = \sum_{i=1}^{n} x_i^{R'} \bmod q. \tag{2.29}$$

Як доведено автором в [19], точка R' не залежить від параметрів h', r', s' і завжди збігається з перевірочною точкою R, що не дає підписувачеві можливості визначити емітента.

$$R' = \alpha' \cdot E + \beta' \cdot P = \frac{r \cdot h'}{h \cdot r'} \cdot E + \frac{s - s' \cdot \frac{r}{r'}}{h} \cdot P =$$

$$= \frac{r}{h \cdot r'} \cdot \left(s' \cdot P - r' \cdot Q \right) + \frac{s}{h} \cdot P - \frac{s' \cdot r}{h \cdot r'} \cdot P = \frac{s}{h} \cdot P - \frac{r}{h} \cdot Q = R.$$

Таким чином, розглянутий протокол вважається захищеним за критерієм анонімності.

В подальшому авторами планується оцінка виграшу в швидкодії та ресурсомісткості при використанні математичного апарату ЕК над СВП в схемах ЕЦП з рекомендованими параметрами.

2.2 Протокол цифрового підпису на гіпереліптичних кривих

Стійкість криптографічних перетворень безпосередньо залежить від розмірів значень параметрів криптосистеми, головним серед яких є довжина особистого ключа. Тому розвиток математичної бази алгоритмів асиметричної криптографії [54] спрямовано, головним чином, на пошук компромісу між показниками «швидкість-стійкість». Програмна реалізація сучасних стандартів цифрового підпису, заснованих на арифметиці в групах точок еліптичних кривих над скінченними полями, для забезпечення достатньої стійкості вимагає підключення спеціалізованих бібліотек великих чисел. Їх використання пов'язане з додатковими накладними витратами на підтримку внутрішніх механізмів представлення і обробки великих чисел у форматах спеціалізованих бібліотек довгої арифметики.

У 1989 році М. Коблицем було запропоновано використовувати в криптографії гіпереліптичні криві [55]. На відміну від еліптичних кривих, точки гіпереліптичної кривої не утворюють групи. Однак адитивну абелеву групу можна побудувати з використанням дивізорів. Порядок такої групи значно перевищує кількість точок кривої, що дозволяє досягати прийнятної стійкості при меншому розмірі основного поля. Прямі і зворотні криптографічні перетворення в цьому випадку є більш складними в порівнянні з еліптичними кривими, однак довжина елементів основного поля зменшується пропорційно роду кривої. Це дає можливість взагалі відмовитись від застосування спеціалізованих бібліотек великих чисел, що

значно прискорює виконання операцій в основному полі. Тому дослідження цього напрямку криптографії з відкритим ключем є актуальними і своєчасними [56].

В цьому розділі будуть розглянуті математичні основи виконання криптографічних операцій на гіпереліптичних кривих та їх застосування в протоколі цифрового підпису [57], основаному на ДСТУ 4145-2002 [58].

2.2.1 Групова операція на гіпереліптичних кривих

Наведемо короткий опис загальних математичних основ теорії дивізорів гіпереліптичних кривих і опис способу побудови якобіана гіпереліптичної кривої, що має структуру групи й, отже, може використовуватися в алгоритмах асиметричної криптографії [59-61].

Гіпереліптичною кривою C роду g ($g \geq 1$) над полем $GF(q), q = p^m$, (p – просте число) є рівняння виду

$$C: y^2 + h(x)y = f(x) \tag{2.30}$$

де $f(x)$ – нормований многочлен ступеня $2g+1$ над полем $GF(q)$, $x, y \in \overline{GF(q)}$, $\overline{GF(q)}$ – алгебраїчне замикання поля $GF(q)$ і не існує рішень $(x, y) \in \overline{GF(q)} \times \overline{GF(q)}$, які одночасно задовольняли б рівнянню (2.30) та рівнянням часткових похідних $2y + h(x) = 0$ і $f'(x) - h'(x)y = 0$.

Точки гіпереліптичної кривої $P = (x, y)$ і $\tilde{P} = (x, -y - h(x))$ визначимо як протилежні $\tilde{P} = -P$.

Крім скінченних точок (x, y) гіпереліптичної кривої в формуванні якобіана бере участь точка на нескінченності P_∞, $P_\infty = -P_\infty$.

Якщо характеристика основного поля $GF(q)$ відмінна від 2, то Заміною змінних $x \to x$, $y \to (y - h(x)/2)$ криву $y^2 + h(x)y = f(x)$ можна перетворити на криву $y^2 + h(x)y = f(x)$

$$C: y^2 = f(x). \tag{2.31}$$

Отже, в подальшому будемо розглядати гіпереліптичні криви в такому вигляді.

Теорема [62]. Порядок якобіану гіпереліптичної кривої роду g над полем $GF(q)$ обмежено інтервалом Хассе-Вейля

$$\left\lceil (\sqrt{q} - 1)^{2g} \right\rceil \leq \#J / GF(q) \leq \left\lfloor (\sqrt{q} + 1)^{2g} \right\rfloor. \tag{2.32}$$

Дивізором гіпереліптичної кривої C називається формальна сума скінченної кількості точок кривої:

$$D = \sum_{P_i \in C} m_i P_i , \quad m_i \in Z . \tag{2.33}$$

Порядком дивізора $D = \sum_{P_i \in C} m_i P_i$ в точці P_i є коефіцієнт m_i: $ord_{P_i}(D) = m_i$.

Дивізори $D = \sum_{P_i \in C} m_i P_i$ і $-D = \sum_{P_i \in C} m_i (-P_i)$ називаються протилежними.

Введемо правило додавання дивізорів:

$$\sum_{P_i \in C} m_i P_i + \sum_{P_i \in C} n_i P_i = \sum_{P_i \in C} (m_i + n_i) P_i . \tag{2.34}$$

Степенем дивізора $D = \sum_{P_i \in C} m_i P_i$ називається сума $\sum_{P_i \in C} m_i$ порядків точок P_i.

Будемо розглядати дивізори степеня 0:

$$D = \sum_{P_i \in C} m_i P_i - \sum_{P_i \in C} m_i P_\infty , \tag{2.35}$$

де $\sum_{P_i \in C} m_i \le g$, причому в сумі не можуть бути одночасно P_i і $-P_i$.

Такі дивізори називаються зведеними і є унікальними елементами якобіану кривої, що являє собою адитивну групу з наведеним вище правилом додавання дивізорів.

Для практичних додатків більш ефективно представлення зведених дивізорів в формі Мамфорда [63], у вигляді пар многочленів – $D = \langle u(x), v(x) \rangle$. В такому вигляді протилежним для дивізора D є дивізор $-D = \langle u(x), -v(x) \rangle$.

Якщо $D = \sum_{P_i \in C} m_i P_i - \sum_{P_i \in C} m_i P_\infty$, де $P_i = (X_i, Y_i)$ – точки гіпереліптичної кривої, то многочлени $u(x)$, $v(x)$ обчислюються за правилами (2.36)-(2.38):

$$u(x) = \prod_i (x - X_i)^{m_i} , \tag{2.36}$$

$$\deg v(x) < \deg u(x) , \tag{2.37}$$

$$v(X_i) = Y_i . \tag{2.38}$$

Введемо [64] операцію додавання двох дивізорів $D_1 = \langle u_1, v_1 \rangle$ і $D_2 = \langle u_2, v_2 \rangle$: $D = D_1 + D_2 = \langle u_3, v_3 \rangle$.

Якщо $D_1 \neq D_2$, то виконуємо наступні кроки.

Спочаку обчислимо найбільш спільний дільник многочленів u_1, u_2 і $(v_1 + v_2)$: $d = \gcd(u_1, u_2, v_1 + v_2) = s_1 u_1 + s_2 u_2 + s_3 (v_1 + v_2)$.

Потім обчислимо $u_0' = \dfrac{u_1 u_2}{d^2}$

та $v_0' = \dfrac{s_1 u_1 v_2 + s_2 u_2 v_1 + s_3 (v_1 v_2 + f)}{d} \bmod u_0'$.

Далі обчислимо в циклі $(u_k', v_k'), k = 1, 2...$, до виконанні умови $\deg u_k' \leq g$

$$u_k' = \frac{f - (v_{k-1}')^2}{u_{k-1}'},$$

$$v_k' = -v_{k-1}' \bmod u_k';$$

Якщо умова $\deg u_k' \leq g$ виконана, то обчислено сума дивізорів $D = D_1 + D_2 = \langle u_3, v_3 \rangle = \langle u_k', v_k' \rangle$.

Якщо $D_1 = D_2 = \langle u, v \rangle$, то обчислення d, u_0', v_0' виконуються за іншими формулами:

$$d = \gcd(u, 2v) = s_1 u + s_3 (2v),$$

$$u_0' = \left(\frac{u}{d} \right)^2,$$

$$v_0' = \frac{s_1 uv + s_3 (v^2 + f)}{d} \bmod u_0'.$$

Дивізор $D0 = \langle 1, 0 \rangle$ є нейтральним елементом (нулем) якобіану.

Для отримання елементів якобіану необхідно обчислити кратні базового дивізора до отримання нуля групи, тобто дивізора $D0 = \langle 1, 0 \rangle$.

Елементи якобіану кривої $y^2 = x^5 + 2x^2 + x + 3 \pmod 7$ представлені в таблиці 2.3 як кратні базового дивізора $D =< x^2 + 3x + 3, 4x + 3 >$.

Таблиця 2.3 – Елементи якобіану кривої $y^2 = x^5 + 2x^2 + x + 3 \pmod 7$

Дивізор	Представлення у формі Мамфорда	Представлення у вигляді суми точок
D	<x2+3x+3, 4x+3>	(1,0)+(3,1)
2D	<x2+x+2, 6x+4>	(3,1)+(3,1)
3D	<x2+2, 6x+1>	(1+5t, 2t)+(6+2t, 2+5t)
4D	<x2+5x+3, 5x>	(2t, 3t)+(2+5t, 3+4t)
5D	<x2+6x+3, 3x+5>	(2+4t, 4+5t)+(6+3t, 2+2t)
6D	<x2+4x+6, 6x+3>	(6+5t, 4+2t)+(4+2t, 6+5t)
7D	<x2+x+4, 5x+5>	(2+2t, 1+3t)+(4+5t, 4+4t)
8D	<x2+3x+5, x+2>	(4+3t, 6+3t)+(4t, 2+4t)
9D	<x2+x+3, 5x+6>	(1+4t, 4+6t)+(5+3t, 3+t)
10D	<x2+5x+5, 2>	(4+t, 2)+(5+6t, 2)
11D	<x2+2x+3, 5x+5>	(5t, 5+4t)+(5+2t, 2+3t)
12D	<x2+5x+2, 5x>	(3+3t, 1+t)+(6+4t, 2+6t)
13D	<x2+2x+2, x+1>	(4+4t, 5+4t)+(1+3t, 2+3t)
14D	<x2+x+6, 6x+1>	(6+t, 2+6t)+(6t, 1+t)
15D	<x2+6x+6, x>	(t, t)+(1+6t, 1+6t)
16D	<x+4, 6>	(3,6)
17D	<x+6, 0>	(1,0)
18D	<x+4, 1>	(3,1)
19D	<x2+6x+6, 6x>	(1+6t, 6+t)+(t, 6t)
20D	<x2+x+6, x+6>	(6+t, 5+t)+(6t, 6+6t)
21D	<x2+2x+2, 6x+6>	(1+3t, 5+4t)+(4+4t, 2+3t)
22D	<x2+5x+2, 2x>	(3+3t, 6+6t)+(6+4t, 5+t)
23D	<x2+2x+3, 2x+2>	(5+2t, 5+4t)+(5t, 2+3t)
24D	<x2+5x+5, 5>	(4+t, 5)+(5+6t, 5)
25D	<x2+x+3, 2x+1>	(1+4t, 3+t)+(5+3t, 4+6t)
26D	<x2+3x+5, 6x+5>	(4t, 5+3t)+(4+3t, 1+4t)
27D	<x2+x+4, 2x+2>	(2+2t, 6+4t)+(4+5t, 3+3t>
28D	<x2+4x+6, x+4>	(4+2t, 1+2t)+(6+5t, 3+5t)
29D	<x2+6x+3, 4x+2>	(6+3t, 5+5t)+(2+4t, 3+2t)
30D	<x2+5x+3, 2x>	(2t, 4t)+(2+5t,4+3t)
31D	<x2+2, x+6>	(6+2t, 5+2t)+(1+5t, 5t)
32D	<x2+x+2, x+3>	(3,6)+(3,6)
33D	<x2+3x+3, 3x+4>	(1,0)+(3,6)
34D	<1, 0>	

Дивізор $D =< x^2 + 3x + 3, 4x + 3 >$ породжує групу порядку 34 [57], яка містить нуль групи $\langle 1,0 \rangle$, один дивізор $< x + 6, 0 >$ порядку 2, 16 дивізорів порядку 17 и 16 дивізорів порядку 34.

Наявність групової структури дозволяє будувати криптографічні протоколи на основі арифметики якобіанів гіпереліптичних кривих. Групова операція, задана представленою ітераційною формулою, є достатньо громіздкою. Сучасні дослідження проводяться в напрямку пошуку більш оптимальних явних формул додавання та подвоєння дивізорів для заданого роду. Також ведеться пошук кривих спеціальних видів, для яких процедура визначення порядку якобіану не є обчислювально-складною. Зокрема, в роботі використана одна з таких кривих – крива Фурукави, для якої існує ефективний алгоритм [65] обчислення порядку якобіану.

2.2.2 Протокол цифрового підпису на гіпереліптичних кривих

Використовуючи криптографічні перетворення операції з дивізорами в якобіані гіпереліптичної кривої як базові, можна модифікувати протоколи цифрового підпису на еліптичних кривих. При цьому операції з точками еліптичної кривої замінюються на операції з дивізорами гіпереліптичної кривої.

Корекції потребують процедури генерації загальносистемних параметрів, зокрема процедура визначення порядку гіпереліптичної кривої, формули групового додавання та подвоєння (як наведено вище), а також функція $\psi(D)$ перетворення дивізора на ціле число.

Далі представлено протокол цифрового підпису на гіпереліптичних кривих, що базується на послідовності кроків сучасного українського стандарту ДСТУ 4145-2002.

Для перетворення дивізора $D = \langle u(x), v(x) \rangle$ дивізора гіпереліптичної кривої над простим полем $GF(p)$, представленого в формі Мамфорда, на ціле число введемо функцію $\psi(D)$, яку, наприклад, можна задати формулою $\psi(D) = u(p)$.

Загальні параметри:

– основне поле – скінченне поле $GF(p)$;

– гіпереліптична крива роду g ($g \geq 1$) над основним полем $y^2 = f(x)$, де $f(x)$ – нормований многочлен ступеня $2g+1$ над полем $GF(p)$;

– базовий дивізор D простого порядку n, такий що $nD = \langle 1,0 \rangle$ і $kD \neq \langle 1,0 \rangle$, $0 < k < n$;

– H – функція хешування.

Підписувач А має асиметричну пару ключів: особистий $d : 1 < d < n$, та відкритий $Q = -dD$.

Нехай підписував має підписати електронний документ M з хеш-образом $H(M)$. Молодші $|n|-1$ розряди хеш-образу $H(M)$ формують десяткове число h, яке використається при обчисленні цифрового підпису.

Підписувач обирає одноразовий випадковий секретний ключ k, $1<k<n$, обчислює дивізор $R=kD=\langle u(x),v(x)\rangle$, після чого формуються складові цифрового підпису

$$r=h\cdot\psi(R)\ \bmod n=h\cdot u(p)\bmod n, \tag{2.39}$$

$$s=(k+d\cdot r\ )\bmod n. \tag{2.40}$$

Параметр підпису s не може бути рівним 0. При $s=0$ процедура підпису повторюється.

Цифровим підписом є пара чисел $\langle r,s\rangle$.

Перевірка підпису $\langle r,s\rangle$ під електронним документом M здійснюється за допомогою відкритого ключа Q підписувача А.

Обчислюється дивізор гіпереліптичної кривої

$$\tilde{R}=sD+rQ, \tag{2.41}$$

після чого обчислюються хеш-образ документу $H(M)$, відповідне десяткове число h та формується число

$$\tilde{r}=h\cdot\psi(\tilde{R})\ \bmod n. \tag{2.42}$$

Якщо $\tilde{r}=r$, цифровий підпис електронного документу M признається справжнім.

Покажемо коректність пропонованого алгоритму формування і перевірки підпису:

$$\tilde{R}=sD+rQ=\left(k+d\cdot r\right)D+r\left(-d\cdot D\right)=kD=R. \tag{2.43}$$

Оскільки $\tilde{R}=R$, то і $\tilde{r}=r$.

У протоколі формування й перевірки цифрового підпису група точок еліптичної кривої була замінена на групу дивізорів (якобіан) гіпереліптичної кривої. На прикладах показана коректність роботи такого протоколу.

У більшості криптографічних додатків використовуються еліптичні та гіпереліптичні криві з порядком групи не менш за 2^{160}. Таким чином, для криптосистем на гіпереліптичних кривих над $GF(q)$ повинно виконуватись як мінімум $g\cdot\log_2 q\approx 160$. Зокрема, для кривої роду 2, необхідно вибрати основне поле з довжиною операндів 80 біт для забезпечення мінімального рівня секретності, що відповідає довжині особистого ключа 160 біт.

2.3 Реалізація криптографічних алгоритмів на масивно-паралельних пристроях

Сучасний етап розвитку інформаційного суспільства характеризується масовим використанням комп'ютерних комунікацій для вирішення завдань як державного рівня і великого бізнесу, так і повсякденних проблем пересічних громадян. При цьому гостро постають питання захисту інформації, які в даний час в розвинених державах вирішуються за допомогою використання інфраструктури відкритих ключів, заснованої використанні методів асиметричної криптографії в алгоритмах цифрового підпису та направленого шифрування. Основою сучасних стандартів цифрового підпису є алгоритми, засновані на криптографічних перетвореннях в групах точок еліптичних кривих, визначених над полями Галуа. Стандарти визначають алгоритми основних дій по генерації ключових пар, формуванню та верифікації цифрового підпису, а також набір рекомендованих для використання загальносистемних параметрів.

Сучасний рівень розвитку апаратних платформ не дозволяє значно збільшити продуктивність ядер центральних процесорів, тому найбільш доступним і перспективним способом підвищення швидкості обчислень є використання паралельних обчислювальних пристроїв. Паралельне програмування на сьогодні вже не є інноваційною технологією – існує безліч різних типів паралельних обчислювальних системи: кластера, grid-системи, хмарні обчислення, багатоядерні процесори. Однак серед них є порівняно нова і активно розвивається концепція масивно-паралельних неграфічних обчислень на графічних прискорювачах, або GPGPU.

Головна перевага графічних прискорювачів, як паралельних обчислювальних пристроїв, це дуже високий ступінь паралелізму: одна сучасна відеокарта може обробляти до декількох тисяч паралельних потоків. Таким чином графічні прискорювачі дають рівень паралелізму системи, порівнянний з великими кластерами і grid-системами, маючи при цьому малі габарити самого пристрою і низькі показники енергоспоживання. Другим важливим фактором, який забезпечив популярність концепції GPU, стало те, що переважна більшість сучасних робочих станцій оснащені досить потужними відеокартами.

Технології неграфічних обчислень на графічних процесорах набирають все більшої популярності. Концепція GPGPU дозволила значно знизити питому вартість високопродуктивних обчислень, зменшити габарити і енергоспоживання паралельних обчислювальних систем. На сьогодні існує декілька реалізацій даної концепції: CUDA, DirectCompute, OpenCL, AMD FireStream, C ++ AMP. Розрізняються вони набором підтримуваного устаткування, особливостями реалізації програмного інтерфейсу, підходом до ліцензування. Однією з найбільш

активно розвиваються останнім часом технологій є технологія CUDA, що розробляється компанією Nvidia. Перевагами даної технології є якісна документація, зручний програмний інтерфейс, широкі можливості. Головний же її недолік - сумісність виключно з графічними прискорювачами компанії Nvidia, що призводить до необхідності закупівлі спеціального обладнання.

У реалізації різних криптографічних примітивів використовуються такі математичні структури, як арифметика скінчених полів, поліноміальна арифметика, арифметика простих і розширених полів Галуа. Як показав аналіз існуючих розробок в області застосування концепції GPGPU для вирішення завдань криптографії та криптоаналізу, даний напрямок розвинений досить слабо. У ряді зарубіжних публікацій досліджується продуктивність паралельних алгоритмів розв'язання окремих завдань криптоаналізу і криптографії, наприклад: вирішення проблеми дискретного логарифмування на еліптичних кривих методом ро-Полларда, реалізація методів факторизації на еліптичних кривих. Однак, аналіз цих публікацій приводить до висновку про відсутність будь-якої універсальної реалізації бібліотеки кріптопрімітивів і бібліотеки довгої арифметики для GPU, використовуваної дослідниками в даній області. У пошуках відповідних бібліотек були виявлені два цікавих проекти: CUMP – бібліотека дійсних чисел довільної точності на основі технології CUDA; GMP-ECM – реалізація арифметики еліптичних кривих на основі проекту GMP , у вихідних кодах якої знайдені функції, що використовують GPU, у разі його наявності, для підвищення продуктивності обчислень.

Перший проект не був завершений: в ньому реалізовані лише 3 базові операції: додавання, віднімання і множення. Що стосується другого проекту, то він не відповідає критерію універсальності і являє собою лише реалізацію кількох окремо взятих завдань.

В результаті було прийнято рішення про необхідність і доцільність створення власної бібліотеки довгої арифметики для GPU, і заснованої на ній бібліотеки кріптопрімітивів, для проведення різнобічних досліджень щодо ефективності використання концепції GPGPU в області криптографії.

2.3.1 Вибір внутрішнього подання довгих чисел

Існує безліч різних бібліотек довгої арифметики і арифметики довільної точності для CPU: NTL, CLN, Miracl, GMP та ін. Деякі з них є також і бібліотеками кріптопрімітівов (наприклад бібліотека Miracl). У цих бібліотеках присутня реалізація всього необхідного математичного апарату для криптографічних досліджень. Вивчення досвіду і особливостей реалізації таких бібліотек, а також

теорії побудови алгоритмів довгої арифметики в цілому є необхідною умовою для створення ефективної бібліотеки довгої арифметики для GPU.

В основі будь-якої арифметичної бібліотеки лежить внутрішній формат представлення чисел. Від нього залежить як ефективність роботи з пам'яттю при вибірці і зміні цих даних, так і ефективність застосування різних алгоритмів обробки цих даних. У різних бібліотеках це питання вирішувалося по-різному. Основні три параметри, що визначають спосіб зберігання даних, це ємність розряду числа, порядок проходження розрядів, спосіб зберігання знака числа.

Наведемо короткий огляд способу зберігання даних в різних існуючих бібліотеках. Для того щоб проілюструвати запропоновані методи і підходи, буде використовуватися синтаксис мови C ++.

Першим і самим природним з точки зору людини варіантом зберігання довгих числі в пам'яті є їх зберігання в десятковій системі числення, з порядком проходження розрядів від старшого до молодшого, а знак числа зберігати у вигляді окремого прапора. У такому випадку ємність розряду такого числа - 10 значень, і для його зберігання в пам'яті може бути використаний тип char (1 байт). Такий підхід до зберігання довгих чисел застосовується в бібліотеці VeryLong:

```
class Verylong {
...
char * Mass;
bool sign;
int length;
...
}
```

До переваг такого методу можна віднести наступне: даний спосіб інтуїтивно зрозумілий і напрошується сам собою; простота реалізації операцій введення / виводу.

Недоліки: неповне використання апаратних ресурсів машини (кожен байт в поданні числа може вміщати 256 різних значень, з яких використовується лише 10); при такому порядку проходження розрядів (від старшого до молодшого) при збільшенні числа необхідно виконання операції зсуву - копіювання значень всіх розрядів в сусідні комірки пам'яті; труднощі реалізації побітових операцій (зсув, логічне і, або, не і т. д.);

У сумі всі недоліки даного методу призводять до вкрай неефективного використання пам'яті і зниження швидкодії алгоритмів, що використовують таку бібліотеку. А оскільки на операції з пам'яттю припадає основна маса накладних витрат, пов'язаних з використанням бібліотек довгої арифметики, даний спосіб подання довгих чисел не має ніякої практичної цінності. Очевидно, що простота

конструкцій і зручність сприйняття не виправдовують багаторазове зниження ефективності алгоритмів.

Альтернативний підхід до подання довгих чисел можна побачити в бібліотеці FLINT. По-перше в цій бібліотеці обраний зворотний порядок проходження розрядів: від молодшого до старшого. Такий підхід значно спрощує процес доповнення числа старшими розрядами або виділення додаткової пам'яті для його зберігання, оскільки відсутня необхідність в зміщенні значень молодших розрядів в пам'яті. Таким чином мінімізується кількість звернень до пам'яті при виконанні ряду операцій над числами. По-друге в цій бібліотеці прийнятий інший спосіб роботи з розрядами чисел, який можна назвати універсальним для архітектури сучасних обчислювальних систем.

Для найбільш ефективного використання пам'яті і апаратних можливостей процесора не можна обходити стороною поняття машинного слова. У будь-якому процесорі, будь то CPU і потоковий мультипроцесор GPU, всі операції виконуються над машинними словами, розмір яких залежить від розрядності системи. Для досягнення максимальної ефективності необхідно щоб розряд внутрішнього подання числа в бібліотеці найбільш повно використовував це машинне слово.

Проілюструємо це для випадку 32-розрядної системи. Основними операціями, які будуть виконуватися над розрядами чисел, є додавання, віднімання і множення. При додаванні і відніманні ми отримуємо число тієї ж розрядності, що і вихідні операнди, плюс прапор переносу. При множенні двох чисел результат займає в два рази більше пам'яті, ніж вихідні операнди. Виходячи з цього для 32-розрядної системи доцільно використовувати 16-бітові розряди довгих чисел. Приклад з бібліотеки FLINT:

```
...
typedef unsigned short clint;
typedef clint * CLINT;
...
```

У цьому випадку оголосити покажчик на область пам'яті для зберігання довгого числа можна як

```
...
CLINT n_l;
...
```

Питання зберігання знака числа можна вирішити, зарезервувавши нульовий розряд внутрішнього подання числа для зберігання службової інформації про це числі. Так, наприклад, в бібліотеці GMP в цьому розряді зберігається розмір пам'яті, виділений для числа. При цьому знак цього значення вказує на знак усього числа. Описаний таким чином підхід до подання довгих чисел є найбільш ефективним з точки зору архітектури сучасних обчислювальних систем, що підтверджується

використанням його у всіх сучасних бібліотеках довгої арифметики, зокрема в бібліотеці GMP.

У процесі пошуку відповідного програмного забезпечення для реалізації криптосистем на GPU був виявлений проект CUMP - бібліотека арифметики довільної точності загального призначення під технологію CUDA з GMP-подібним інтерфейсом. GMP - одна з найвідоміших бібліотек довгої арифметики для центральних процесорів, широко застосовується програмістами і дослідниками по всьому світу. В силу цього, використання програмного інтерфейсу GMP є доцільним, і полегшить подальше портування на нову платформу реалізованих раніше алгоритмів.

Всі роздуми щодо подання довгих чисел в пам'яті в рівній мірі справедливі як для CPU так і для GPU зважаючи ідентичності їх архітектури на базовому рівні. При розробці бібліотеки довгої арифметики під технологію CUDA необхідно лише враховувати особливості роботи з пам'яттю, а вірніше з різними типами пам'яті, присутніми в CUDA. Однак це більшою мірою відноситься вже до алгоритмів, використовуваним в бібліотеці, ніж до особливостей внутрішнього представлення чисел.

Як було згадано, внутрішнє подання чисел бібліотеки GMP повністю задовольняє критерію ефективності і може бути взято в якості основи нашої бібліотеки довгої арифметики для GPU, забезпечивши тим самим її сумісність на рівні формату даних з GMP. Цей шлях розвитку був підказаний творцями проекту CUMP. Крім ефективності він надає можливість використання безлічі допоміжних функцій, реалізованих в GMP, таких як функції введення / виводу, конвертація між різним системами числення, управління пам'яттю на стороні CPU.

Вибір і реалізація внутрішнього подання довгих чисел, це лише перший крок у процесі створення бібліотеки довгої арифметики для GPU. Проте він значною мірою визначать весь подальший шлях розвитку проекту, вибір алгоритмів обробки даних, способи взаємодії з іншими бібліотеками. Це завдання вимагає ретельного і продуманого рішення, оскільки надалі переглянути його буде важко. Використання внутрішнього представлення чисел бібліотеки GMP, що є на сьогоднішній день лідером за швидкістю роботи з довгими числами, представляється найбільш ефективним рішенням даної задачі.

У CUMP реалізовані лише три базові арифметичні операції: додавання, віднімання і множення; а також на рівні інтерфейсу підтримувався тільки один тип даних - дійсні числа. Однак його структура виявилася досить зручною для створення на базі CUMP повноцінного аналога GMP для графічних прискорювачів. Таким чином була розроблена бібліотека CudaMPZ, в яку на даний момент входять: реалізація базових арифметичних операцій над довгими числами; модульна арифметика; арифметика в кільцях поліномів; поліноміальна арифметика над полями Галуа характеристики 2.

2.3.2 Оцінка продуктивності бібліотеки CUDAMPZ в порівнянні з GMP

API бібліотеки CudaMPZ має три основні складові, що умовно названі CPU API, GPU API і DataTransfer API. Така структура обумовлена жорстким поділом коду і простору пам'яті, доступним GPU і CPU.

CPU API - це набір функцій, які виконуються на центральному процесорі. У першу чергу це функції введення / виведення, виділення і звільнення пам'яті під використовувані змінні, приведення типів даних для забезпечення сумісності з іншими бібліотеками та програмними комплексами. Як вже було сказано вище, в основу реалізації CudaMPZ була закладена повна сумісність з бібліотекою GMP. Завдяки цьому CPU API бібліотеки CudaMPZ ґрунтується на API бібліотеки GMP і може використовувати її стандартні функції і типи даних.

GPU API - це набір функцій, які виконуються в середовищі графічного прискорювача. Імена та параметри виклику цих функція ідентичні таким в бібліотеці GMP. Також в GPU API додані функції для роботи з поліноміальною арифметикою над полями Галуа характеристики 2.

DataTransfer API - набір типів даних і функцій, що забезпечують обмін даними між простором пам'яті CPU і GPU. Наявність цього програмного прошарку необхідно, оскільки на даному етапі розвитку технології GPGPU центральний процесор не має безпосереднього доступу до пам'яті графічного прискорювача і навпаки.

У попередніх дослідженнях бібліотека GMP була виділена, як найбільш швидка серед існуючих на даних момент бібліотек довгої арифметики. Оцінка продуктивності бібліотеки CudaMPZ був виконана на основі порівняння з продуктивністю бібліотеки GMP при виконанні різних арифметичних операцій.

У першому тесті порівнювалася швидкість виконання базових арифметичних операцій над масивом цілих чисел в однопоточному режимі. Довжина операндів становила 32768 біт.

Таблиця 2.4 – Порівняння швидкості в базових арифметичних операцій в однопоточному режимі

Операція	GMP	CudaMPZ
Додавання (106 ітерацій)	0,8 с	4,8 с
Множення (104 ітерацій)	2,2 с	10,8 с
Ділення (104 ітерацій)	3,1 с	11,3 с

З результатів першого тесту бачимо помітне відставання в продуктивності бібліотеки CudaMPZ перед GMP при роботі в однопоточном режимі, що однак є цілком очевидним, якщо порівняти технічні характеристики ядра центрального процесора і обчислювальних ядер графічного прискорювача. Виграш у продуктивності очікується при використанні можливостей паралельного програмування на GPU.

У другому тесті порівнювалася швидкість виконання базових арифметичних операцій над масивом цілих чисел в паралельному режимі. Довжина операндів становила 32768 біт. При виконанні обчислень на центральному процесорі були задіяні 2 ядра - обчислення виконувалися в 2-х потоках. Обчислення на графічному прискорювачі виконувалися в 64 потоках, що складає приблизно половину його апаратних можливостей.

Таблиця 2.5 – Порівняння швидкості в базових арифметичних операцій в паралельному режимі

Операція	GMP	CudaMPZ
Додавання (106 ітерацій)	0,5 с	0,2 с
Множення (104 ітерацій)	1,3 с	0,6 с
Ділення (104 ітерацій)	1,7 с	0,9 с

За результатами другого тесту помітний приріст продуктивності при використанні бібліотеки CudaMPZ за рахунок застосування паралельного програмування. Помітно, що особливістю технологій GPGPU є висока латентність звернень до глобальної пам'яті.

2.3.3 Особливості представлення базових елементів для алгоритмів стандарту ЕЦП ДСТУ 4145 в технології CUDA

Наступним етапом в ході реалізації алгоритмів стандарту ЕЦП ДСТУ 4145 є вибір найбільш придатних для аналізованої програмно-апаратної платформи базису представлення елементів основного поля і системи координат, що використовуються для представлення точок еліптичної кривої.

Еліптичні криві можуть бути представлені в різних системах координат, а також використовувати різні базиси для представлення елементів основного поля. Кожен з цих факторів впливає на складність виконання тих чи інших математичних операцій, а також на способи подання даних у пам'яті обчислювальної машини. Це, в свою чергу, впливає на частоту і порядок звернень до пам'яті в процесі обчислень і

на ступінь паралелізму алгоритмів, що у випадку з обчисленнями на графічних прискорювачах, може зіграти фатальну роль щодо продуктивності обчислювальної системи.

До розгляду були прийняті наступні типи базисів: поліноміальний базис, оптимальний нормальний базис, гаусові нормальні базиси; та різних систем координат для представлення точок еліптичної кривої: афінні координати, проективні координати, якобіанові координати, координати Чудновського, координати Лопеса-Дахаба.

Наступним етапом даної роботи є застосування розроблених технологій в задачах обчислення точок еліптичних.

Найбільш важливим параметром, що визначає в кінцевому підсумку криптостойкость обраної кривої, є її порядок, тобто скінчена кількість точок з координатами з основного поля, що належать кривій. При цьому порядок базової точки повинен бути великим простим дільником порядку кривої, щоб уникнути атаки Поліга-Хеллмана.

Існує ще ряд обмежень, що дозволяє вибрати стійку криву. У стандартах наводяться готові до використання криві, стійкість яких регламентується розробниками стандартів, проте з часом вимоги до стійкості неухильно ростуть і в підсумку можуть вийти за рамки стандартизованих параметрів. Отже, завдання визначення порядку еліптичних кривих не втрачає своєї актуальності.

Відомі два протилежних підходи до знаходження стійкої кривої: вибір коефіцієнтів кривої випадковим чином і підрахунок її точок відповідними методами; знаходження коефіцієнтів кривої по заздалегідь заданому порядку.

Сучасні методи вирішення обох цих здач є обчислювально складними. Тому бажано розробити їх паралельні аналоги та відповідне програмне забезпечення для GPGPU.

В ході роботи було досліджено ефективність визначення порядку еліптичної кривої, визначеною над розширеним полем Галуа характеристики 2 із застосуванням технології CUDA. Проведено порівняльний аналіз цих методів з урахуванням архітектурних особливостей масивно-паралельних пристроїв (GPU) і традиційних процесорних систем (CPU). Експериментальна частина даної роботи виконана з використанням розробленої бібліотеки криптопримітивів CudaMPZ.

Примітивний алгоритм визначення порядку еліптичної кривої засновано на повному переборі x-координат кривої (по одній на потік виконання в разі GPU) і обчисленні y-координати. Існування та значення відповідної y-координати визначається обчисленням символу Лежандра в кожному потоці та розв’язком квадратного рівняння у випадку підтвердження.

Нижче (рис. 2.1) приведена залежність часу роботи алгоритму від довжини модуля основного поля на GPU і CPU .

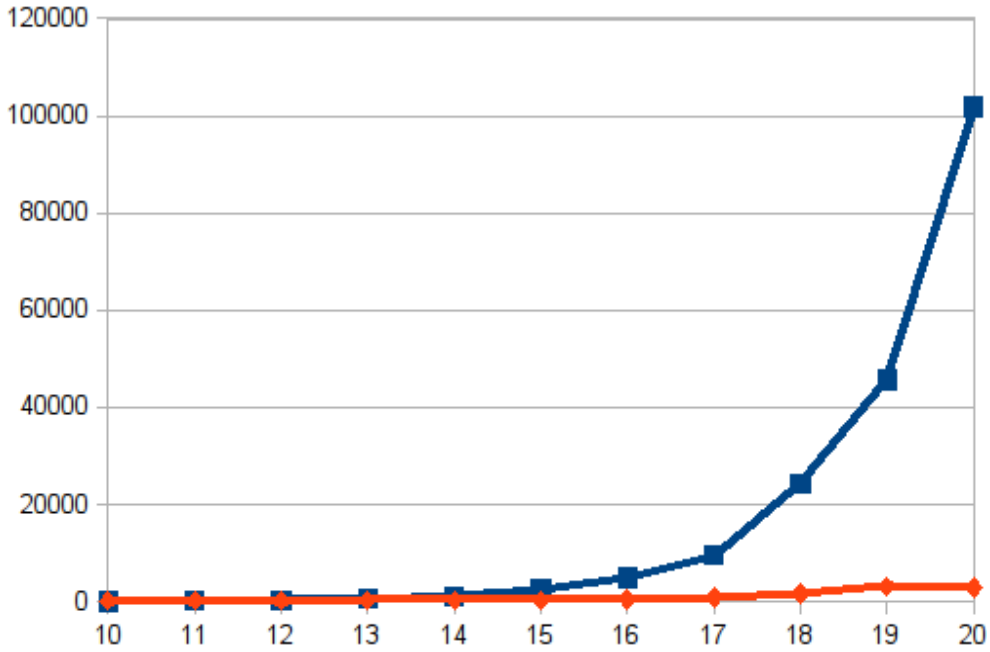


Рисунок 2.1– Порівняння продуктивності GPU і CPU

З результатів експерименту видно, що крива, яка відповідає обчисленням на GPU практично не залежить від довжини модуля. Отже, використання обчислювальних резервів графічних прискорювачів дає вагомі результати навіть при використанні алгоритмів, що базуються на повному переборі варіантів.

3 РОЗРОБКА ТЕХНІЧНИХ МЕТОДІВ ТА ЗАСОБІВ ЗАХИСТУ ІНФОРМАЦІЙНИХ І КОМУНІКАЦІЙНИХ СИСТЕМ

В останні десятиріччя бурхливий розвиток технології виробництва систем і засобів зв'язку з практично необмеженою пропускною здатністю і дальністю передавання, а також масове їхнє використання привели до інформаційно-технологічної революції і формування глобального інформаційного суспільства.

Такий розвиток подій став можливим завдяки широкому практичному використанню досягнень фундаментальных наук – насамперед фізики, хімії і математики, а також комп'ютерних технологій. Успіхи в цих областях науки дозволили досягти великих зрушень в галузі розвитку волоконно-оптичних систем передавання.

В даний час волоконно-оптичні лінії зв'язку міцно займають свої позиції й інтенсивно розвиваються. Видатні технологічні ідеї приходять саме тоді, коли в них виникає практична потреба, і це в значній мірі стосується волоконно-оптичних ліній зв’язку. Статистичні дані показують, що при числі каналів більше 10 тисяч волоконно-оптичних ліній зв’язку більш економічні за радіорелейні лінії і супутникові системи зв'язку. На частку волоконно-оптичних ліній зв’язку в системах дальнього зв'язку приходиться 60…70% каналів, а на частку супутникових і радіорелейних ліній – 30…40%.

У світі телекомунікацій відбувається стрімкий перехід від багатомодових до одномодових оптичних волокон (ОВ), збільшується число ОВ у кабелях, розширюється асортимент оптичних елементів. Лінії зв'язку працюють на довжинах хвиль 1,3 мкм та 1,55 мкм, збільшується довжина ділянок регенерації – з десятків до сотень кілометрів і швидкість передавання – до декількох гігабіт у секунду, використовується спектральне ущільнення, упроваджуються ербієві підсилювачі. Пріоритет віддається міжміським і міжнародним лініям, а також лініям абонентського зв'язку.

Стрімкими темпами йде заміна кабелів з металевими жилами на волоконно-оптичні кабелі на всіх ділянках мереж, у тому числі і на абонентських лініях міста і села. Перспективними є наземні і підводні волоконно-оптичних ліній зв’язку. Тривалий термін служби (25 років) і захищеність системи зв’язку від несанкціонованого доступу і метеорологічних умов також є перевагами волоконно-оптичних ліній зв’язку.

У глобальній мережі зв'язку 60% ліній займають наземні і підводні волоконно-оптичних ліній зв’язку.

Обсяг використання різних видів кабелів і проводів у світі збільшився за останні чотири роки на 17%, а волоконно-оптичних – на 110%.

Продовжується стрімкий розвиток волоконно-оптичних і квантово-оптичних технологій для волоконно-оптичних ліній зв’язку. Те, що сьогодні ще є наукою, завтра стає вже технікою. В останні роки для збільшення довжини регенераційних ділянок магістральних волоконно-оптичних систем передавання активно упроваджуються волоконні оптичні підсилювачі та пристрої хвильового ущільнення, проводяться інтенсивні дослідження щодо подальшого розвитку волоконно-оптичних систем передавання, впроваджуються в практику нові типи оптичних волокон і фотонних кристалів.

3.1 Функціональні властивості одномодових волокон

З огляду на дисперсію, існуючі одномодові волокна, що часто використовуються в сучасних мережах, поділяються на три основні типи: волокна із незміщеною дисперсією SF (стандартне волокно зі східчастим профілем), волокна зі зміщеною дисперсією DSF і волокна з ненульовою зміщеною дисперсією NZDSF.

Всі три типи волокон дуже близькі за загасанням у вікнах одномодового передавання 1310 і 1550 нм, але відрізняються характеристиками хроматичної дисперсії. Оскільки дисперсія впливає на максимальну допустиму довжину безретрансляційних ділянок, то на перший погляд, природно, що виникає бажання вибрати волокно з найменшою можливою дисперсією. Це справедливо для випадку передавання однієї довжини хвилі при одноканальному передаванні.

Багатоканальне хвильове мультиплексування (WDM) у вікні 1550 нм диктує інший раціоналізм. Дослідження показують, що, коли довжина хвилі нульової дисперсії попадає в зону мультиплексного сигналу, починають виявлятися небажані інтерференційні ефекти, що пришвидшують деградацію сигналу. Тому виробники пристроїв зв'язку повинні чітко бачити переваги і недоліки кожного волокна при еволюції традиційних мереж в бік повністю оптичних мереж.

Волокно SF. На початку 80-х років передавачі на довжину хвилі 1550 нм мали дуже високу ціну і низьку надійність і не могли конкурувати на ринку з передавачами на довжину хвилі 1300 нм. Тому стандартне східчасте волокно SF є першим комерційним волокном і на даний час найбільш поширене в телекомунікаційних мережах. Воно оптимізоване по дисперсії для роботи у вікні 1310 нм.

Волокно DSF. Внаслідок удосконалення систем передавання на довжині хвилі 1550 нм виникає потреба у розробці волокна з довжиною хвилі нульової дисперсії, що потрапляє в середину цього вікна. В результаті, в середині 80-х років створюється волокно зі зміщеною дисперсією DSF, яке повністю оптимізоване для роботи у вікні 1550 нм як за загасанням, так і за дисперсією.

Протягом багатьох років волокно DSF вважалося найперспективнішим з волокон. З розвитком нових технологій передавання мультиплексного оптичного сигналу суттєвого значення набувають ербієві оптичні підсилювачі типу EFDA, які можуть підсилювати багатоканальний сигнал.

На жаль, подальші дослідження на початку 90-х років показали, що саме довжина хвилі нульової дисперсії (1550 нм), яка потрапляє в середину робочого діапазону ербієвого підсилювача, є головним потенційним джерелом нелінійних ефектів (насамперед, чотирихвилевого змішування), завдяки чому різко зростає шум в умовах поширення багатоканального сигналу.

Подальші дослідження підтвердили обмежені можливості DSF при використанні в системах WDM. Щоб уникнути нелінійних ефектів при використанні DSF у WDM системах, доцільно вводити сигнал меншої потужності у волокно, збільшувати відстань між каналами й уникати передавання парних каналів (симетричних щодо λ).

Чотирихвильове змішування – це ефект, який призводить до розсіювання двох хвиль з утворенням нових небажаних довжин хвиль. Нові хвилі можуть призводити до деградації оптичного сигналу в результаті інтерференції з ним, або відсмоктувати потужність із корисного хвилевого каналу. Саме через ефект чотирихвильового змішування стало очевидним, що треба розробити новий тип волокна, у якому λ0 розташувалася б за межами (по один бік – зліва або справа) усіх можливих каналів.

3.2 Захисні оболонки оптоволокна

Значний вплив на характеристики оптоволокна має конструкція захисного полімерного покриття. Покриття повинно зберігати власну міцність ОВ для захисту його поверхні від вологи, хімічних і механічних ушкоджень, для фільтрації оболонкових мод і запобігання додаткових втрат на передачу, які обумовлюються макровигинами.

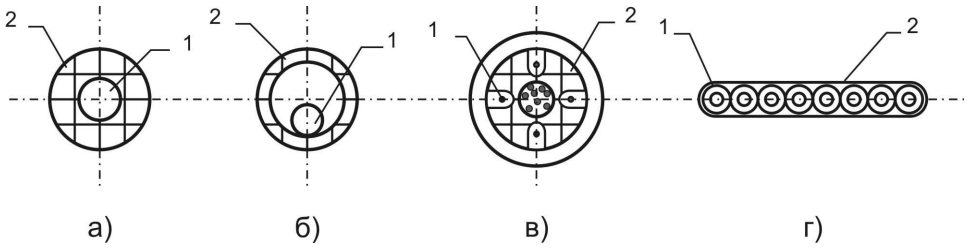
Захисна оболонка ОВ з полімерних матеріалів у загальному випадку має складну структуру і утворюється з первинного, буферного і вторинного покрить. Первинне покриття захищає оптичну оболонку ОВ. Буферне – запобігає виникненню додаткових втрат на макровигинах. Вторинне – захищає первинне і буферне покриття від механічних ушкоджень у процесі виготовлення і прокладання волоконно-оптичного кабелю (ВОК). Первинне і буферне покриття наносяться в процесі витягування ОВ, вторинне – методом екструзії при витягуванні ОВ, або виготовляється у окремій операції.

Матеріали буферного покриття повинні грати роль демпфера знижуючого зовнішнє навантаження на ОВ. Буферний слой виробляється з м’якого полімерного

матеріалу, наприклад, із СІЕЛа, уретанакрілових композицій, поліетилену, поліпропілену, фторопласту 40 та ін.

Також використовується акрилат з ультрафіолетовою обробкою. Акрилове покриття наноситься двома окремими шарами: м'який внутрішній шар та жорсткий зовнішній шар. Правильний вибір матеріалу забезпечує фізичний захист і значну міцність покриття, одночасно надає стійкості проти поперечної сили роздавлювання, абразивного зносу і стійкості до корозійного середовища.

В якості вторинного захисту ОВ можуть служити (рис. 3.1): трубки оптичних модулів чи пази профільованих серцевин оптичних кабелів (ОК); щільні покриття з полімерів; стрічково-елементне укладання.



а – щільне; б – трубчасте; в – пази профільованої серцевини;
г – стрічко-елементне укладання; 1 – ОВ; 2 – вторинне укладання

Рисунок 3.1 – Вторинне покриття оптичного волокна

Первинне захисне покриття (ПЗП) наноситься на оптичну оболонку у вигляді лаку з наступним зміцненням. Незважаючи на його невелику товщину (від одиниць до десятків мікронів), ПЗП істотно поліпшує характеристики ОВ. Так, наприклад, ПЗП із силіконового компаунда майже на 50% зменшує чутливість одномодового ОВ до впливу навантажень, які розчавлюють. Це дозволяє в багатьох випадках застосовувати звичайні одномодові ОВ для передачі сигналів з підвищеною вимогою до збереження поляризації. При впливі навантаження, яке розчавлює, на ОВ із кварцовою серцевиною і кварцовою оптичною оболонкою в ПЗП виникають мікровигини внаслідок шорсткості поверхні якогось із елементів кабельної конструкції. Частіше стали застосовуватися ОВ із двошаровим покриттям, у яких перший шар – м'який, а другий – твердий.

3.3 Останні досягнення в області розробки оптичних волокон

Перше десятиріччя нинішнього століття ознаменувалося значним проривом в області виробництва ОВ з покращеними характеристиками.

Розроблено ОВ типу All Wave ZWP з нульовим піком води, в якому усунено гідроксильні іони у складі кварцевого скла, що дозволило перейти до освоєння «повного спектру довжин хвиль» – від 1275 до 1625 нм.

Створено методи зниження поляризаційної модової дисперсії (ПМД), наявність якої обмежує дальність і швидкість передачі в протяжних високошвидкісних одномодових волоконно-оптичних системах зв'язку. Зниження ПМД досягається застосуванням технології періодичного закручування волокна в процесі його витягування із заготовки. Таке закручування волокна зменшує дію двулучезаломлення завдяки змішуванню поляризаційних компонентів мережевої хвилі. Це утримує значення ПМД на дуже малому рівні.

Проводиться розробка і створення фотонних кристалів і оптичного волокна на їх основі, що стало одним із значних досягнень оптичних технологій останніх років.

Виникла ідея використання волоконно-оптичних технологій для створення фотонних кристалів. У кварцову трубку діаметром 20 мм упаковуються капіляри діаметром близько 1 мм із направляючим стрижнем з того ж кварцового скла, і який розташовано між капілярами. Потім, із отриманої таким чином заготовки, витягується оптичне волокно. Проводиться двоступінчаста перетяжка заготовки, в процесі якої всі розміри зменшуються приблизно в 10000 разів.

Відомо два типи волоконних світловодів із структурою фотонних кристалів. Це волоконні світловоди із суцільною світловедучою жилою та волоконні світловоди з порожнистою світловедучою жилою.

Дірчастий світлопровід із суцільною світловедучою жилою є серцевиною з кварцового скла в оболонці з фотонних кристалів (кварцове скло з повітряними порожнинами-каналами), що має менший середній коефіцієнт заломлення по відношенню до жили. Тому хвилеводні властивості таких світлопроводів забезпечуються одночасно двома ефектами: повного внутрішнього відбиття, як в звичайних світлопроводах, і зонними властивостями фотонного кристала.

Окрім відміченої вище можливості створення одномодових дірчастих волоконних світлопроводів для дуже широкого спектрального діапазону, незвичайними є їх дисперсійні властивості, які залежать від розмірів повітряних каналів і їх взаємного розташування. Ці волокна можуть мати аномальну дисперсію в більш короткохвильовій області спектру, ніж звичайні світлопроводи, аж до довжин хвиль 0,8 мкм а залежність дисперсії від довжини хвилі в широкому спектральному діапазоні може бути дуже слабкою.

Якщо змінювати однаково всі геометричні розміри структури дірчастого волокна (за умови збереження співвідношення між ними), то можна отримати у волокні одномодовий режим поширення як з малою, так і великою ефективною площею поперечного перетину моди. Тобто, можна створювати дірчасті волокна з діаметром світловедучої жили, що у багато разів перевищує або, навпаки, є меншим

за діаметр світловедучої жили стандартного одномодового волокна. При цьому в ньому буде зберігатися одномодовий режим поширення світла.

Великі розміри світловедучої жили при одномодовому режимі поширення в широкому спектральному діапазоні, а також реальність створення дірчастих волокон з малими втратами і слабкою залежністю дисперсії від довжини хвилі роблять перспективним їх застосування у волоконно-оптичних системах зв'язку в якості передавального середовища.

Знаходять комерційне застосування оптичні волокна з кращими параметрами вигину, що полегшує їх прокладання всередині будівель. Застосування звичайного ОВ в мережах FTTH, FTTX і т. п., пов’язано з деякими обмеженнями внаслідок великих оптичних втрат при надмірному вигині волокна в кабелі. Наприклад, на довжині хвилі 1550 нм при вигині радіусу 10 мм сигнал в стандартному волокні втрачає більше 60% своєї потужності; при цьому велика вірогідність погіршення якості і навіть втрати зв'язку для кінцевих споживачів. Основний принцип полягає в створенні навколо серцевини кругової області з нижчим, у порівнянні з периферійною зовнішньою оболонкою, показником заломлення.

З'явилися нові типи полімерних оптичних волокон зі зниженими втратами і розширеною смугою пропускання. Це дозволяє перейти до їх промислового застосування. У полімерного волокна є серйозні переваги в порівнянні з кварцовим: великий діаметр серцевини значно полегшує з'єднання; гнучкість полегшує швидке розгортання мережі і не вимагає залучення спеціально навченого, високооплачуваного персоналу. Розроблено перфторполімерне волокно, в якому вдалося знизити втрати до 50 дБ/км для діапазону довжин хвиль 650–1300 нм. Керувати структурою полімерів значно простіше завдяки низькій температурі плавлення (175°С). Це дозволило створювати не тільки двовимірні періодичні структури, що подібні до структур в кварцових ОВ, але також неперіодичні структури, зокрема системи розташованих на концентричних колах отворів програмованого змінного діаметру. Саме за цією технологією створено полімерне волокно з градієнтним профілем ефективного показника заломлення.

По мірі розширення галузей застосування оптичних волокон (зокрема, у телекомунікаційній та комп’ютерній сферах) удосконалюються самі волокна, з’являються їх нові параметри, які оптимізуються для різних застосувань.

Сьогодні застосовується 7 стандартизованих типів оптичних волокон, характеристики яких регламентовані рекомендаціями Міжнародного Союзу Електрозв'язку (табл.3.1).

ITU-T – (International Telecommunication Union – Telecommunication Standardization Sector) – Сектор стандартизації Міжнародного союзу електрозв'язку. Кожний клас (тип) оптичних волокон може мати різні підкласи (категорії), у яких волокна можуть відрізнятися по деяких характеристиках.

Таблиця 3.1 - Типи сучасних оптичних волокон

№	Клас (тип) оптичних волокон	Рекомендація ITU-T
1	Багатомодове 50/125 мкм із градієнтним профілем показника заломлення	G.651
2	Стандартне одномодове	G.652
3	Одномодове зі зміщеною дисперсією	G.653
4	Одномодове зі зміщеною довжиною хвилі відсічки	G.654
5	Одномодове з ненульовою зміщеною дисперсією	G.655
6	Одномодове з ненульовою дисперсією для широкосмугової оптичної передачі	G.656
7	Одномодове зі зменшеними втратами на вигинах з малими радіусами	G.657

Основний тип одномодового оптичного волокна, застосовуваного в кабелях FinMark – це стандартне волокно Fujikura FutureGuide LWP, що відповідає вимогам ITU-T G.652.D. Це оптичне волокно має низькі втрати в області гідроксильного піка (1383 нм), що дозволяє більш широко використати CWDM технології при передачі. Нижче подано в якості прикладу характеристики одномодового оптичного волокна Fujikura FutureGuide LWP.

Оптичні характеристики:

а) коефіцієнт загасання:

1) на довжині хвилі 1310 нм: ≤ 0.35 дБ/км

2) на довжині хвилі 1383 нм: ≤ 0.31 дБ/км

3) на довжині хвилі 1550 нм: ≤ 0.21 дБ/км

4) на довжині хвилі 1625 нм: ≤0.23 дБ/км

б) коефіцієнт хроматичної дисперсії:

1) при вимірі в діапазоні довжин хвиль 1285-1330 нм: ≤ 3.5 пс/(нм·км)

2) при вимірі в діапазоні довжин хвиль 1270 - 1340 нм: ≤ 5.3 пс/(нм·км)

3) при вимірі на довжині хвилі 1550 нм: ≤ 18 пс/(нм·км)

в) довжина хвилі нульової дисперсії: 1300 - 1324 нм

г) нахил нульової дисперсії: ≤ 0.092 пс/(нм2·км)

д) довжина хвилі відсічення: 1260 нм

е) поляризаційна модовая дисперсія (PMD): ≤ 0.2 пс/км1/2

ж) діаметр модового поля:

1) на довжині хвилі 1310 нм: 9.2 ± 0.4 мкм

2) на довжині хвилі 1550 нм: 10.4 ± 0.8 мкм

Механічні характеристики:

а) діаметр оболонки: 125.0 ± 0.7 мкм

б) похибка концентричності серцевини: ≤ 0.5 мкм

в)похибка концентричності оболонки/покриття: ≤ 12 мкм

г) зусилля зняття покриття: 1.3 - 8.9 Н

д) діаметр покриття: 245 ± 5 мкм

е) неокруглість покриття: ≤ 1.0%

ж) випробування на міцність (proof-test): ≥ 1.0 % (0.7 ГПа)

к) радіус власної кривизни волокна: ≥ 4.0 м

На вимогу замовника оптичний кабель FinMark також виробляється з іншими типами оптичних волокон: багатомодовим 50/125 мкм, одномодовим з ненульовою зміщеною дисперсією (ITU-T G.655), з волокном підвищеної гнучкості (ITU-T G.657.A) для кабелів внутрішньої прокладання. Характеристики одномодового ОВ зі зменшеними втратами на вигинах з малими радіусами (рекомендація ITU-T G.657)наведено в табл.3.2.

Таблиця 3.2 - Характеристики одномодового ОВ зі зменшеними втратами на вигинах з малими радіусами (рекомендація ITU-T G.657)

Параметр	ITU-T G.657.A	ITU-T G.657.B
Втрати на вигинах 1 виток ∅15 мм λ=1550нм	Не нормується	≤ 0.5 дБ
Втрати на вигинах 1 виток ∅15 мм λ=1625 нм	Не нормується	≤ 1 дБ
Втрати на вигинах 1 виток ∅20 мм λ=1550 нм	≤ 0.75 дБ	≤ 0.1 дБ
Втрати на вигинах 1 виток ∅20 мм λ=1625 нм	≤1.5 дБ	≤ 0.2 дБ
Втрати на вигинах 10 витків ∅30 мм λ=1550 нм	≤ 0.25 дБ	≤ 0.03 дБ
Втрати на вигинах 10 витків ∅30 мм λ=1625 нм	≤ 1 дБ	≤ 0.1 дБ
Діаметр модового поля, мкм	8.6-9.5	6.3-9.5
Загасання на довжині хвилі 1310нм, дБ/км	≤ 0.35	≤ 0.35
Загасання на довжині хвилі 1383нм, дБ/км	≤ 0.31	Не нормується
Загасання на довжині хвилі 1550нм, дБ/км	≤ 0.21	≤ 0.21

Волокно ITU-T G.657.B застосовується на обмежених відстанях і має особливо малі втрати на вигинах.

ВИСНОВКИ

Запропоновано новий метод захисту авторського права на цифрові зображення з вбудуванням цифрових водяних знаків. Отримано патент на корисну модель «Спосіб захисту авторського права на цифрові зображення» та свідоцтво про реєстрацію авторського права на твір «Комп'ютерна програма для захисту цифрових зображень». Створена комп'ютерна програма для захисту цифрових зображень дозволяє здійснить виявлення факту порушення авторських або суміжних прав. Програма може бути використана у випадку, коли при передачі твору підписується ліцензійна угода між ліцензіаром та ліцензіатом. Програма надає можливість правовласнику як виявити правопорушника, так і захистити своє право в судовому чи адміністративному порядку.

Досліджено проблеми витоку інформації в каналах мобільного зв'язку та запропонована комплексна система захисту мовної інформації в приміщенні.

Розглянуто організація доступу до інформації засобами біометричної аутентифікації та можливості використання ДНК-чипів в системах контролю та доступу. Досліджено та проаналізовано застосування сучасних технічних засобів захисту інформації в інформаційних мережах та методів апаратного захисту програмного забезпечення.

Запропоновано нові протоколи цифрового підпису на еліптичних кривих над скінченним векторним полем та гіпереліптичних кривих. Доказана захищеність розробленої схеми сліпого підпису за критерієм анонімності.

Досліджено ефективність визначення порядку еліптичної кривої із застосуванням технології CUDA. Проведено порівняльний аналіз методів обчислень з урахуванням архітектурних особливостей масивно-паралельних пристроїв і традиційних процесорних систем. На основі технології CUDA розроблена бібліотека кріптопрімітивів CudaMPZ, в яку на даний момент входять: реалізація базових арифметичних операцій над довгими числами; модульна арифметика; арифметика в кільцях поліномів; поліноміальна арифметика над полями Галуа характеристики 2. Показано, що використання обчислювальних резервів графічних прискорювачів дає вагомі результати навіть при використанні алгоритмів, що базуються на повному переборі варіантів. Концепція GPGPU дозволила значно знизити питому вартість високопродуктивних обчислень, зменшити габарити і енергоспоживання паралельних обчислювальних систем.

Розглянуто функціональні властивості одномодових волокон та досліджено конструкції захисного полімерного покриття оптоволокна. Наведено характеристики одномодового оптоволокна.

ПЕРЕЛІК ПОСИЛАНЬ

1. Андрущенко, Д.М. Защита авторских прав на цифровые изображения / Д.М. Андрущенко // Радіоелектроніка. Інформатика. Управління. – 2014. – №1. – С.135-139.

2. Пат. 81168 Україна, МПК H04L 9/8 (2006.01). Спосіб захисту авторського права на цифрові зображення / Д.М. Андрущенко, Г.Л. Козіна, Л.М. Карпуков. – № u2012 14519, заявл. 18.12.2012, опубл. 25.06.2013, Бюл. № 12, 2013 р. – 3 с.

3. Андрущенко, Д.М. Комп'ютерна програма для захисту цифрових зображень / Д.М. Андрущенко, Г.Л. Козіна // Свідоцтво про реєстрацію авторського права на твір №. 56327 – К.: Державний департамент інтелектуальної власності України. — Дата реєстрації: 05.09.2014.

4. Андрущенко, Д.М. Система для исследования стойкости робастных стеганографических алгоритмов / Д.М. Андрущенко // Восточно-Европейский журнал передовых технологий. – 2013. – № 6/12(66). – С. 41-44.

5. Андрущенко, Д.М. Метод авторизации через интернет для защиты shareware программ / Д.М. Андрущенко, Г.Л. Козіна // Восточно-Европейский журнал передовых технологий. – , 2014. – № 4/2 (70). – С. 23-27.

6. Андрущенко, Д.М. Комп'ютерна програма "Захист програмних продуктів" / Д.М. Андрущенко, Г.Л. Козіна // Свідоцтво про реєстрацію авторського права на твір №. 46740 – К.: Державний департамент інтелектуальної власності України. — Дата реєстрації: 11.12.2012.

7. Лізунов, С.І. Витік інформації в каналах мобільного зв'язку / С.І. Лізунов // Сучасні проблеми і досягнення в галузі радіотехніки, телекомунікацій та інформаційних технологій: VI Міжн. наук.-практ. конф., 17-19 вересня 2014 р. : тези доповідей.– Запоріжжя, 2014. – С.339-341.

8. Лізунов, С.І. Застосування сучасних технічних засобів захисту інформації в інформаційних мережах / С.І. Лізунов, Л.М. Карпуков // Використання сучасних інформаційних технологій в діяльності органів внутрішніх справ: Всеукр. науково-практ. семінар, 22 листопада 2013 р.: матеріали семінару – Дніпропетровськ, 2013. – С. 5-8.

9. Цинько, Д.К. Комплексна система захисту мовної інформації в приміщенні / Д.К. Цинько, С.І. Лізунов // Тиждень науки: щорічна наук.-практ. конф. викладачів, науковців, молодих учених і аспірантів, 14-18 квітня 2014 р.: тези доповідей в 5 томах. – Запоріжжя, 2014. – Т.2. – С. 81-82.

10. Лізунов, С.І. Організація доступу до інформації засобами біометричної аутентифікації / С.І. Лізунов // Використання сучасних інформаційних технологій в діяльності органів внутрішніх справ: Всеукр. науково-практ. семінар, 22 листопада 2013 р.: матеріали семінару – Дніпропетровськ, 2013. – С. 11-14.

11. Воскобойник, В.О. Дослідження можливості використання ДНК-чипів в системах контролю та доступу / В.О. Воскобойник, А.В. Кравцова // Тиждень науки: щорічна наук.-практ. конф. викладачів, науковців, молодих учених і аспірантів, 13-17 квітня 2015 р.: тези доповідей. – Запоріжжя, 2015. (надано до друку)

12. Галкін, В.А. Аналіз способів реалізації загрози типу «злом пароля» / В.А. Галкін, Д.В. Бєліков // Тиждень науки: щорічна наук.-практ. конф. викладачів, науковців, молодих учених і аспірантів, 14-18 квітня 2014 р.: тези доповідей в 5 томах. – Запоріжжя, 2014. – Т.2. – С. 62-63.

13. Корольков, Р.Ю. Сучасні методи апаратного захисту програмного забезпечення. Технологія HASP / Р.Ю. Корольков, А.В. Тверденко // Захист інформації і безпека інформаційних систем: II Міжн. наук.-техн. конф., 30 травня – 01 червня 2013 р.: матеріали конф.– Львів, 2013. – С. 160-161.

14. Говоров, А.О. Апаратний захист програмного забезпечення. Технологія HASP / А.О. Говоров, А.В. Тверденко // Тиждень науки: щорічна наук.-практ. конф. викладачів, науковців, молодих учених і аспірантів, 15-19 квітня 2013 р.: тези доповідей в 5 томах. – Запоріжжя, 2013. – Т.1. – С. 192-193.

15. Калинин, Д.А. Быстродействие шифров “КАЛИНА” и AES / Д.А. Калинин, Г.Л. Козина // Радіоелектроніка. Інформатика. Управління. – 2013. – №1. – С. 62-65.

16. Козіна, Г.Л. Криптопротоколи: схеми цифрового підпису: навч.посіб. / Г.Л. Козіна, М.А. Молдов’ян, Г.В. Неласа. – Запоріжжя: ЗНТУ, 2014. – 170 с.

17. Козина, Г.Л. Протокол слепой цифровой подписи на основе стандарта ECGDSA / Г.Л. Козина, Г.И. Никулищев, Н.А. Молдовян // Вопросы защиты информации. – 2014. – №1.– С.40-45.

18. Нікуліщев, Г.І. Протокол сліпого електронного цифрового підпису на еліптичних кривих над скінченим векторним полем / Г.І. Нікуліщев // Радіоелектроніка. Інформатика. Управління. – 2013. – №2. – С.83-94.

19. Нікуліщев, Г.І. Анонімність як критерій оцінки захищеності протоколів сліпого електронного цифрового підпису / Г.І. Нікуліщев, Г.Л. Козіна // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. – 2012. – №2. – С. 59-65.

20. Неласая, А.В. Использование масивно - параллельных вычислительных устройств для определения порядка эллиптической кривой / А.В. Неласая, М.И. Верещак // ITSEC: V міжн. наук.-техн. конф., 19–22 травня 2015 р.: матеріали конф.– К., 2015. – С.21-22.

21. Верещак, М.И. Внутреннее представление чисел в библиотеке длинной арифметики для GPU // М.И. Верещак, А.В. Неласая / Кластерні обчислення (CC'13): Друга міжн. наук.-техн. конф., 29 березня 2013 р.: тези доповідей. – Львів, 2013. – С. 225-228.

22. Верещак, М.И. Проблемы разработки массивно-параллельных алгоритмов базовых арифметических операций / М.И. Верещак, А.В. Неласая // Сучасні проблеми і досягнення в галузі радіотехніки, телекомунікацій та інформаційних технологій: VI Міжн. наук.-практ. конф., 19-21 вересня 2012 р.: тези доповідей. – Запоріжжя, 2012. – С.299-300.

23. Верещак, М.И. Оценка эффективности библиотеки криптопримитивов для графических ускорителей // М.И. Верещак, А.В. Неласая / Питання оптимізації обчислень (ПОО-XL): Міжнародна наукова конференція, 30 вересня-4 жовтня 2013 р.: Праці конф. – К., 2013. – С. 51.

24. Щекотихін, О.В. Компоненти та пристрої волоконно-оптичних ліній зв'язку: навчальний посібник / О.В. Щекотихін, Д.М. Піза, Т.І. Бугрова– Запоріжжя: ЗНТУ, 2015. – 306 с.

25. Щекотихин, О.В. Пассивные оптические сети доступа: монографія / О.В. Щекотихин, И.Н. Сметанин, Д.М. Піза– Запоріжжя: ЗНТУ, 2015. – 276 с.

26. Щекотихин, О.В. Новые волоконно-оптические световоды для систем передачи информации / О.В. Щекотихин, М.А. Звонарева // Тиждень науки: щорічна наук.-практ. конф. викладачів, науковців, молодих учених і аспірантів, 15-19 квітня 2013 р.: збірник тез доповідей в 5 томах. – Запоріжжя, 2013. – Т.1. – С. 133-134.

27. Пиза, Д.М. Влияние интерференции помех на системы помехозащиты импульсно-доплеровских радаров / Д.М. Пиза, А.П. Залевский, А.С. Сиренко // Радіоелектроніка. Інформатика. Управління. – 2013. – №1. – С.51-54.

28. Пиза, Д.М. Метод адаптации автокомпенсатора при воздействии комбинированных помех / Д.М. Пиза, А.С. Сиренко, Е.А. Звягинцев // Радіоелектроніка. Інформатика. Управління. – 2013. – №2. – С. 50-58.

29. Пат. № 78120 Україна, МПК G01S 7/36 (2013.01). Спосіб захисту когерентно-імпульсних радіолокаційних станцій від комбінованих завад / Піза Д.М., Сіренко А.С. – заяв. 20.08.2012; опубл. 11.03.2013, Бюл. №5, 2012.

30. Костенко, В.О. Электропитание охранной сигнализации от высоковольтной линии электропередач / В.О. Костенко, И.Н. Сметанин, О.В. Щекотихин // Радіоелектроніка. Інформатика. Управління. – 2014. – №1. – С.40-45.

31. Карпуков, Л.М. Прямой метод синтеза полосно-пропускающих шлейфовых фильтров с чебышевской характеристикой / Л.М. Карпуков, Р.Ю. Корольков // Радіотехніка. – 2012. – № 171. – С. 300 – 305.

32. Карпуков, Л.М. Прямой синтез шлейфных фильтров нижних частот с чебышевской характеристикой / Л.М. Карпуков, Р.Ю.Корольков // Радіоелектроніка. Інформатика. Управління. – 2014. – №1. – С.35-39.

33. Фурманова, Н.И. Сравнение программ проектирования с точки зрения микрополосковой топологии на примере полос-нопропускающих фильтров с отверстиями в экране / Н.И. Фурманова, А.Ю. Фарафонов, С.Н. Романенко, Э.Н.

Шинкаренко, М.В.Мищенко // Радіоелектроніка. Інформатика. Управління. – 2012. – №2. – С.53-56.

34. Залевский, А.П. Оценка эффективности пространственно-временной и время-пространственной фильтрации сигналов в когерентно-импульсных РЛС / А.П. Залевский, Д.М. Пиза, И.С. Пресняк, А.С. Сиренко // Радіоелектроніка. Інформатика. Управління. – 2012. – №2. – С.39-44.

35. Куцак, С.В. Оценка параметров Н-плоскостного поглощающего фильтра гармоник / С.В. Куцак, Л.М. Логачева // Радіотехніка. – 2014. – № 179. – С. 60-67.

36. Куцак, С.В. Моделирование импедансными поверхностями периодических неоднородностей в прямоугольных волноводах [Текст] / С.В. Куцак // Радіотехніка. – 2013. – № 175. – С. 102-108.

37. Романенко, С.Н. Расчет шлейфных направленных ответвителей на МПЛ с учетом дисперсии и потерь в линиях / С.Н. Романенко, В.П. Дмитренко, В.А. Воскобойник // Радіоелектроніка. Інформатика. Управління. – 2013. – №2. – С.71-79.

38. Романенко, С.Н. Взаимодействие плоской электромагнитной волны со слоем метаматериала. Численное моделирование / С.Н. Романенко, В.П. Дмитренко, Р.Д. Пулов // Радіоелектроніка. Інформатика. Управління. – 2012. – №2. – С.30-34.

39. Логачова, Л.М. Дифракція хвилі Н10 на стику регулярного і нерегулярного хвилеводів з діелектричною пластиною скінченної довжини / Л.М. Логачова, С.В. Куцак, В.П. Бондарєв, Н.Ю. Копильова // Радіоелектроніка. Інформатика. Управління. – 2012. – №2. – С.14-19.

40. Пат. № 72287 Україна. МПК7 G01 R 27/28. Пристрій для виміру та визначення параметрів N – вимірних передатних функцій нелінійних систем / С. П. Гулін, О. С. Гулін, В. П. Дмитренко – заяв. 20.02.2012; опубл. 10.08.2012, Бюл. №15, 2012.

41. Закон України «Про авторське право і суміжні права» [Електронний ресурс] // Відомості Верховної Ради України (ВВР) – 1994. – № 13. – С.64 – Режим доступу: http://zakon2.rada.gov.ua/laws/show/3792-12

42. Пат. 2347266 Росія, МПК G06F17/00. Способ и устройство для получения и удаления информации относительно объектов цифровых прав / ЛИ Биунг-рае, КИМ Тае-сунг, ДЗУНГ Киунг-им та ін. – 2006138021/09; заявл. 15.03.2005; опубл. 10.05.2008 р. – 42 с.

43. Пат. № 57243 Україна, МПК H03M 13/37. Спосіб захисту авторських прав векторних зображень цифровими водяними знаками у вигляді електронного коду / В.В. Карпінець, Ю.Є. Яремчук. – № u201015193, заявл. 16.12.2010, опубл. 10.02.2011, Бюл.№ 3, 2011 р. – 5 с.

44. Служба мітки часу та цифрового підпису [Електронний ресурс].– Режим доступу: https://metkavremeni.com/timestamp_pgp_sign_file-ukrainian.html

45. e-notārs [Електронний ресурс].– Режим доступу: http://www.e-notars.lv/

46. DNA Chip Technology / Office of Science Education and Outreach: Research Technique Fact Sheets [Електронний ресурс].– Режим доступу: http://www.genome.gov/DIR/VIP/Learning_Tools/Fact_Sheets/dna_chip.html

47. Nature communications: Logic gates based on ion transistors [Електронний ресурс]. – Режим доступу: http://www.nature.com/ncomms/journal/v3/n5/full/ncomms1869.html

48. Аникин, И.В. Программно-аппаратная защита информации. Защита программного обеспечения от отладки и дизассемблирования. Учебное пособие / И.В. Аникин, В.И. Горлова. – Казань: КГТУ им. А.Н. Туполева, 2003. – 80с.

49. Краснопевцев, А.А. О защите приложений с использованием внешнего аппаратного модуля / А.А.Краснопевцев // Безопасность информационных технологий. – 2011. – № 1. – С.102-104.

50. Горбатов, В.С. Основы технологии PKI / В.С. Горбатов, О.Ю. Полянская. – М.: Горячая линия-Телеком, 2004. – 248 с.

51. Молдовян, Н.А. Теоретический минимум и алгоритмы цифровой подписи. / Н.А. Молдовян – СПб.: БХВ-Петербург, 2010. – 304 с.

52. Болотов А.А. Алгоритмические основы эллиптической криптографии / А.А. Болотов, С.Б. Гашков, А.Б. Фролов, А.А. Часовских. – М.: МЭИ, 2000. – 100 с.

53. Костин, А.А. О реализации протоколов слепой подписи и коллективной подписи на основе стандартов цифровой подписи / А.А. Костин, Н.А. Молдовян, А.М. Фаль // ИБРР-2009: VI Санкт-Петербургская межрегиональная конференция, 28-30 октября 2009 г.: материалы конф. – СПб., 2009. – С.111.

54. Савчук, М.Н. Математические основания асимметрической криптографии / М.Н. Савчук // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. – 2003. – №6. – С. 140-148.

55. Koblitz, N. Hyperelliptic cryptosystem / N. Koblitz // Journal of Crypto. – 1989. – № 1. – P. 139-150.

56. Dolgov, V. Hyperelliptic Curves in Cryptography / V. Dolgov, A. Nelasa // 2-nd International Conference "Advanced Computer Systems and Networks: Design and Application", ACSN’2005, 21-23 September 2005. – Lviv, 2005. – С. 121-122.

57. Неласа, Г.В. Удосконалення методів перетворень в якобіанах гіпереліптичних кривих для криптографічних додатків : дис. на здобуття наук. ступеня канд. техн. наук : спец. 05.13.21 „Системи захисту інформації” / Неласа Ганна Вікторівна. — Харків, 2010. — 265 с.

58. Інформаційні технології. Криптографічний захист інформації. Цифровий підпис, що ґрунтується на еліптичних кривих. Формування та перевіряння: ДСТУ 4145: 2002. – [Чинний від 2002-03-13]. К.: Держстандарт України, 2002. – 38 с.: табл. – (Національний стандарт України).

59. Долгов, В.И. Геометрический подход к сложению дивизоров гиперэллиптической кривой / В.И Долгов, А.В. Неласая // Радіоелектроніка. Інформатика. Управління. – 2007. – №2. – С.44-50.

60. Шафаревич, И. Р. Основы алгебраической геометрии. / И.Р. Шафаревич– М.: Наука, 1972. – 568 с.

61. Handbook of elliptic and hyperelliptic curve cryptography / Cohen H., Frey G., Avanzi R. et. al. . – Chapman & Hall/CRC : Taylor&Francis Group, 2005. – 808 p.

62. Gaudry, P. Counting Points on Hyperelliptic Curves over Finite Fields / P. Gaudry, R. Harley // The 4th Algorithmic Number Theory Symposium -- ANTS IV, Berlin : Springer Verlag. – 2000. – LNCS 1838. – P. 297-312.

63. Мамфорд, Д. Лекции о тэта-функциях. / Д. Мамфорд– М.: Мир, 1988. – 448 с.

64. Cantor, D.G. Computing in the Jacobian of a hyperelliptic curve / D.G. Cantor // Math. Comp. 48. – 1987. – P. 95-101.

65. Furukawa, E. Counting Points for Hyperelliptic Curves of Type y2 = x5 +ax over Finite Prime Fields / E. Furukawa, M. Kawazoe and T. Takahashi // Selected Areas in Cryptography (SAC 2003), LNCS 3006. – Springer. – 2004. – P. 26–41.

Додаток А

Перелік публікацій за тематикою НДР

1. Андрущенко, Д.М. Защита авторских прав на цифровые изображения / Д.М. Андрущенко // Радіоелектроніка. Інформатика. Управління. – 2014. – №1. – С.135-139.

2. Пат. 81168 Україна, МПК H04L 9/8 (2006.01). Спосіб захисту авторського права на цифрові зображення / Д.М. Андрущенко, Г.Л. Козіна, Л.М. Карпуков. – № u2012 14519, заявл. 18.12.2012, опубл. 25.06.2013, Бюл. № 12, 2013 р. – 3 с.

3. Андрущенко, Д.М. Комп'ютерна програма для захисту цифрових зображень / Д.М. Андрущенко, Г.Л. Козіна // Свідоцтво про реєстрацію авторського права на твір №. 56327 – К.: Державний департамент інтелектуальної власності України. — Дата реєстрації: 05.09.2014.

4. Андрущенко, Д.М. Система для исследования стойкости робастных стеганографических алгоритмов / Д.М. Андрущенко // Восточно-Европейский журнал передовых технологий. – 2013. – № 6/12(66). – С. 41-44.

5. Андрущенко, Д.М. Метод авторизации через интернет для защиты shareware программ / Д.М. Андрущенко, Г.Л. Козіна // Восточно-Европейский журнал передовых технологий. – , 2014. – № 4/2 (70). – С. 23-27.

6. Андрущенко, Д.М. Комп'ютерна програма "Захист програмних продуктів" / Д.М. Андрущенко, Г.Л. Козіна // Свідоцтво про реєстрацію авторського права на твір №. 46740 – К.: Державний департамент інтелектуальної власності України. — Дата реєстрації: 11.12.2012.

7. Лізунов, С.І. Витік інформації в каналах мобільного зв'язку / С.І. Лізунов // Сучасні проблеми і досягнення в галузі радіотехніки, телекомунікацій та інформаційних технологій: VI Міжн. наук.-практ. конф., 17-19 вересня 2014 р. : тези доповідей.– Запоріжжя, 2014. – С.339-341.

8. Лізунов, С.І. Застосування сучасних технічних засобів захисту інформації в інформаційних мережах / С.І. Лізунов, Л.М. Карпуков // Використання сучасних інформаційних технологій в діяльності органів внутрішніх справ: Всеукр. науково-практ. семінар, 22 листопада 2013 р.: матеріали семінару – Дніпропетровськ, 2013. – С. 5-8.

9. Цинько, Д.К. Комплексна система захисту мовної інформації в приміщенні / Д.К. Цинько, С.І. Лізунов // Тиждень науки: щорічна наук.-практ. конф. викладачів, науковців, молодих учених і аспірантів, 14-18 квітня 2014 р.: тези доповідей в 5 томах. – Запоріжжя, 2014. – Т.2. – С. 81-82.

10. Лізунов, С.І. Організація доступу до інформації засобами біометричної аутентифікації / С.І. Лізунов // Використання сучасних інформаційних технологій в

діяльності органів внутрішніх справ: Всеукр. науково-практ. семінар, 22 листопада 2013 р.: матеріали семінару – Дніпропетровськ, 2013. – С. 11-14.

11. Воскобойник, В.О. Дослідження можливості використання ДНК-чипів в системах контролю та доступу / В.О. Воскобойник, А.В. Кравцова // Тиждень науки: щорічна наук.-практ. конф. викладачів, науковців, молодих учених і аспірантів, 13-17 квітня 2015 р.: тези доповідей. – Запоріжжя, 2015. (надано до друку)

12. Галкін, В.А. Аналіз способів реалізації загрози типу «злом пароля» / В.А. Галкін, Д.В. Бєліков // Тиждень науки: щорічна наук.-практ. конф. викладачів, науковців, молодих учених і аспірантів, 14-18 квітня 2014 р.: тези доповідей в 5 томах. – Запоріжжя, 2014. – Т.2. – С. 62-63.

13. Корольков, Р.Ю. Сучасні методи апаратного захисту програмного забезпечення. Технологія HASP / Р.Ю. Корольков, А.В. Тверденко // Захист інформації і безпека інформаційних систем: II Міжн. наук.-техн. конф., 30 травня – 01 червня 2013 р.: матеріали конф.– Львів, 2013. – С. 160-161.

14. Говоров, А.О. Апаратний захист програмного забезпечення. Технологія HASP / А.О. Говоров, А.В. Тверденко // Тиждень науки: щорічна наук.-практ. конф. викладачів, науковців, молодих учених і аспірантів, 15-19 квітня 2013 р.: тези доповідей в 5 томах. – Запоріжжя, 2013. – Т.1. – С. 192-193.

15. Калинин, Д.А. Быстродействие шифров “КАЛИНА” и AES / Д.А. Калинин, Г.Л. Козина // Радіоелектроніка. Інформатика. Управління. – 2013. – №1. – С. 62-65.

16. Козіна, Г.Л. Криптопротоколи: схеми цифрового підпису: навч.посіб. / Г.Л. Козіна, М.А. Молдов’ян, Г.В. Неласа. – Запоріжжя: ЗНТУ, 2014. – 170 с.

17. Козина, Г.Л. Протокол слепой цифровой подписи на основе стандарта ECGDSA / Г.Л. Козина, Г.И. Никулищев, Н.А. Молдовян // Вопросы защиты информации. – 2014. – №1.– С.40-45.

18. Нікуліщев, Г.І. Протокол сліпого електронного цифрового підпису на еліптичних кривих над скінченим векторним полем / Г.І. Нікуліщев // Радіоелектроніка. Інформатика. Управління. – 2013. – №2. – С.83-94.

19. Нікуліщев, Г.І. Анонімність як критерій оцінки захищеності протоколів сліпого електронного цифрового підпису / Г.І. Нікуліщев, Г.Л. Козіна // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. – 2012. – №2. – С. 59-65.

20. Неласая, А.В. Использование масивно - параллельных вычислительных устройств для определения порядка эллиптической кривой / А.В. Неласая, М.И. Верещак // ITSEC: V міжн. наук.-техн. конф., 19–22 травня 2015 р.: матеріали конф.– К., 2015. – С.21-22.

21. Верещак, М.И. Внутреннее представление чисел в библиотеке длинной арифметики для GPU // М.И. Верещак, А.В. Неласая / Кластерні обчислення (CC'13):

Друга міжн. наук.-техн. конф., 29 березня 2013 р.: тези доповідей. – Львів, 2013. – С. 225-228.

22. Верещак, М.И. Проблемы разработки массивно-параллельных алгоритмов базовых арифметических операций / М.И. Верещак, А.В. Неласая // Сучасні проблеми і досягнення в галузі радіотехніки, телекомунікацій та інформаційних технологій: VI Міжн. наук.-практ. конф., 19-21 вересня 2012 р.: тези доповідей. – Запоріжжя, 2012. – С.299-300.

23. Верещак, М.И. Оценка эффективности библиотеки криптопримитивов для графических ускорителей // М.И. Верещак, А.В. Неласая / Питання оптимізації обчислень (ПОО-XL): Міжнародна наукова конференція, 30 вересня-4 жовтня 2013 р.: Праці конф. – К., 2013. – С. 51.

24. Щекотихін, О.В. Компоненти та пристрої волоконно-оптичних ліній зв'язку: навчальний посібник / О.В. Щекотихін, Д.М. Піза, Т.І. Бугрова– Запоріжжя: ЗНТУ, 2015. – 306 с.

25. Щекотихин, О.В. Пассивные оптические сети доступа: монографія / О.В. Щекотихин, И.Н. Сметанин, Д.М. Піза– Запоріжжя: ЗНТУ, 2015. – 276 с.

26. Щекотихин, О.В. Новые волоконно-оптические световоды для систем передачи информации / О.В. Щекотихин, М.А. Звонарева // Тиждень науки: щорічна наук.-практ. конф. викладачів, науковців, молодих учених і аспірантів, 15-19 квітня 2013 р.: збірник тез доповідей в 5 томах. – Запоріжжя, 2013. – Т.1. – С. 133-134.

27. Пиза, Д.М. Влияние интерференции помех на системы помехозащиты импульсно-доплеровских радаров / Д.М. Пиза, А.П. Залевский, А.С. Сиренко // Радіоелектроніка. Інформатика. Управління. – 2013. – №1. – С.51-54.

28. Пиза, Д.М. Метод адаптации автокомпенсатора при воздействии комбинированных помех / Д.М. Пиза, А.С. Сиренко, Е.А. Звягинцев // Радіоелектроніка. Інформатика. Управління. – 2013. – №2. – С. 50-58.

29. Пат. № 78120 Україна, МПК G01S 7/36 (2013.01). Спосіб захисту когерентно-імпульсних радіолокаційних станцій від комбінованих завад / Піза Д.М., Сіренко А.С. – заяв. 20.08.2012; опубл. 11.03.2013, Бюл. №5, 2012.

30. Костенко, В.О. Электропитание охранной сигнализации от высоковольтной линии электропередач / В.О. Костенко, И.Н. Сметанин, О.В. Щекотихин // Радіоелектроніка. Інформатика. Управління. – 2014. – №1. – С.40-45.

31. Карпуков, Л.М. Прямой метод синтеза полосно-пропускающих шлейфовых фильтров с чебышевской характеристикой / Л.М. Карпуков, Р.Ю. Корольков // Радіотехніка. – 2012. – № 171. – С. 300 – 305.

32. Карпуков, Л.М. Прямой синтез шлейфных фильтров нижних частот с чебышевской характеристикой / Л.М. Карпуков, Р.Ю.Корольков // Радіоелектроніка. Інформатика. Управління. – 2014. – №1. – С.35-39.

33. Фурманова, Н.И. Сравнение программ проектирования с точки зрения микрополосковой топологии на примере полос-нопропускающих фильтров с отверстиями в экране / Н.И. Фурманова, А.Ю. Фарафонов, С.Н. Романенко, Э.Н. Шинкаренко, М.В.Мищенко // Радіоелектроніка. Інформатика. Управління. – 2012. – №2. – С.53-56.

34. Залевский, А.П. Оценка эффективности пространственно-временной и время-пространственной фильтрации сигналов в когерентно-импульсных РЛС / А.П. Залевский, Д.М. Пиза, И.С. Пресняк, А.С. Сиренко // Радіоелектроніка. Інформатика. Управління. – 2012. – №2. – С.39-44.

35. Куцак, С.В. Оценка параметров Н-плоскостного поглощающего фильтра гармоник / С.В. Куцак, Л.М. Логачева // Радіотехніка. – 2014. – № 179. – С. 60-67.

36. Куцак, С.В. Моделирование импедансными поверхностями периодических неоднородностей в прямоугольных волноводах [Текст] / С.В. Куцак // Радіотехніка. – 2013. – № 175. – С. 102-108.

37. Романенко, С.Н. Расчет шлейфных направленных ответвителей на МПЛ с учетом дисперсии и потерь в линиях / С.Н. Романенко, В.П. Дмитренко, В.А. Воскобойник // Радіоелектроніка. Інформатика. Управління. – 2013. – №2. – С.71-79.

38. Романенко, С.Н. Взаимодействие плоской электромагнитной волны со слоем метаматериала. Численное моделирование / С.Н. Романенко, В.П. Дмитренко, Р.Д. Пулов // Радіоелектроніка. Інформатика. Управління. – 2012. – №2. – С.30-34.

39. Логачова, Л.М. Дифракція хвилі Н10 на стику регулярного і нерегулярного хвилеводів з діелектричною пластиною скінченної довжини / Л.М. Логачова, С.В. Куцак, В.П. Бондарєв, Н.Ю. Копильова // Радіоелектроніка. Інформатика. Управління. – 2012. – №2. – С.14-19.

40. Пат. № 72287 Україна. МПК7 G01 R 27/28. Пристрій для виміру та визначення параметрів $N-$вимірних передатних функцій нелінійних систем / С. П. Гулін, О. С. Гулін, В. П. Дмитренко – заяв. 20.02.2012; опубл. 10.08.2012, Бюл. №15, 2012.