МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІЕРСИТЕТ

КОВТУН Марія Григорівна

УДК 004.056.55:003.26

МЕТОДИ УДОСКОНАЛЕННЯ АРИФМЕТИЧНИХ ОПЕРАЦІЙ У ПОЛЯХ, КІЛЬЦЯХ ТА АЛГЕБРАЇЧНИХ КРИВИХ ДЛЯ КРИПТОГРАФІЧНИХ ЗАСТОСУВАНЬ

05.13.21 – «Системи захисту інформації»

Автореферат
дисертації на здобуття наукового ступеня
кандидата технічних наук

Київ 2018

Дисертацією є рукопис.

Робота виконана на кафедрі безпеки інформаційних технологій Національного авіаційного університету Міністерства освіти і науки України.

Науковий керівник**:**	доктор технічних наук, доцент **Гнатюк Сергій Олександрович**, Національний авіаційний університет, доцент кафедри безпеки інформаційних технологій.
Офіційні опоненти**:**	доктор технічних наук, професор **Смірнов Олексій Анатолійович**, Центральноукраїнський національний технічний університет, завідувач кафедри кібербезпеки та програмного забезпечення; доктор технічних наук, професор **Кузнецов Олександр Олександрович**, Харківський національний університет імені В. Н. Каразіна, професор кафедри безпеки інформаційних систем і технологій.

Захист відбудеться «27» червня 2018 р. о 13^{00} на засіданні спеціалізованої вченої ради Д 26.062.17 при Національному авіаційному університеті за адресою: 03058, м. Київ, пр. Космонавта Комарова, 1, ауд.11.111.

З дисертацією можна ознайомитись у Науково-технічній бібліотеці Національного авіаційного університету за адресою: 03058, м. Київ, пр. Космонавта Комарова, 1.

Автореферат розісланий «26» травня 2018 р.

В.о. ученого секретаря
спеціалізованої вченої ради
д.т.н., професор  В.В.Козловський

ЗАГАЛЬНА ХАРАКТЕРИСТИКА РОБОТИ

Актуальність. У новому тисячолітті суспільство переходить до інформаційної ери зі швидкоплинними інформаційними процесами, що зумовлюється постійним розвитком та удосконаленням інформаційних технологій. Для надання юридичної значущості даним процесам та електронним документам, що полягає у чіткій формалізації та їх автоматизації, в Україні були прийняті Закони України «Про електронний цифровий підпис», «Про електронні документи та електронний документообіг», «Про електронні довірчі послуги», які передбачають використання електронного цифрового підпису (ЕЦП) юридичними та фізичними особами, як аналог власного підпису. Процедура формування та перевірки ЕЦП виконується згідно державного стандарту ДСТУ 4145-2002. У напрямку інтеграції України у міжнародне суспільство, було надано нормативного статусу цілій низці міжнародних стандартів у галузі криптографії, а також розгорнуто гілки для RSA та ECDSA у Центральному засвідчувальному органі (ЦЗО) України.

Для забезпечення довірчого інформаційного простору, в Україні створено Національну систему ЕЦП, в межах якої сертифікуються ключі ЕЦП та ключі для вироблення спільного секрету. Під час розгортання та її експлуатації, виникає велика кількість юридичних, економічних та технічних питань. Серед технічних, слід виділити інформаційно-телекомунікаційні системи (ІТС), завдяки яким і можлива робота довірчого інформаційного простору України. Зараз ЕЦП використовується у багатьох державних і приватних установах у безперервному режимі для виконання електронних платежів у Національному банку України, для податкової звітності Державної фіскальної служби, різноманітні державні реєстри, державні закупівлі та торги тощо.

Досвід експлуатації таких систем за кордоном і в Україні, показує тенденцію зростання кількості звернень до складових частин – центрів сертифікації ключів (ЦСК) та періодичних сезонних імпульсів, пов'язаних зі здачею податкової звітності, формуванню різноманітних звітів, проведенням торгів та закупівель, подачею податкових декларацій державними службовцями. З часом, такі навантаження можуть перевищити на які розраховані ЦСК та зменшити якість обслуговування користувачів відповідних ІТС, кількість яких постійно зростає, особливо, де використовується ЕЦП, що вимагає безперервного процесу модернізації Національної системи ЕЦП та її складових. Модифікація полягає, як у використанні апаратних засобів, з кращою обчислювальною потужністю, а також і телекомунікаційного обладнання, розрахованого на більшу пропускну здатність. Однак, заміна апаратного забезпечення буває фінансово невигідна або технічно неможлива. В таких випадках єдиним рішенням є удосконалення лише програмної частини ЦСК, тому виникає інтерес до підвищення швидкодії виконання операцій з ЕЦП, а також до пошуку математичного апарату для перспективних криптографічних перетворень. Зараз, активно використовуються схеми ЕЦП: на еліптичних кривих (ЕК) (ДСТУ 4145-2002, ECDSA, ECGDSA, ECKDSA, ГОСТ 34.10-2012, СТБ 34.101.45-2011); на перетвореннях у полях та кільцях (DSA); на перетвореннях у кільцях (RSA).

Алгоритми підпису, що базуються на арифметичних перетвореннях на ЕК використовують – операції над точками, які в свою чергу базуються на арифметичних операціях над координатами точок, що представлені як елементи базового поля та поля порядку ЕК. Елементи полів можуть бути представлені як великі поліноми чи великі цілі числа, які також використовуються в алгоритмах ЕЦП, що базуються на арифметичних перетвореннях у полях та кільцях.

Таким чином, *актуальною науково-технічною задачею* є підвищення швидкодії криптографічних операцій у ІТС ЦСК Національної системи ЕЦП, шляхом зменшення обчислювальної складності алгоритмів криптографічних перетворень на основі розробки та удосконалення методів арифметичних операцій над числами, поліномами і точками

ЕК зі зменшеною обчислювальною складністю.

Зв'язок роботи з науковими програмами, планами, темами.

Тематика дисертаційної роботи та одержані результати безпосередньо пов'язані з «Основними науковими напрямами та найважливішими проблемами фундаментальних досліджень у галузі природничих, технічних і гуманітарних наук НАН України на 2014-2018 роки», Стратегією кібербезпеки України від 15 березня 2016 року №96/2016 і Рамковою програмою ЄС з досліджень та інновацій «Горизонт 2020». Результати роботи відображені у звітах держбюджетних НДР Національного авіаційного університету «Квантово-криптографічні методи захисту критичної інформаційної інфраструктури держави» (д.р. № 0117U006770), «Методи забезпечення конфіденційності державних інформаційних ресурсів в інформаційно-комунікаційних системах» (№ 61/09.01.08), «Новітні технології криптографічного захисту інформації» (№ 100/14.01.06), у яких здобувач брав участь в якості виконавця.

Мета та завдання дослідження. Метою дисертаційної роботи є підвищення швидкодії інформаційно-телекомунікаційних систем центрів сертифікації ключів Національної системи ЕЦП за рахунок розробки та удосконалення методів арифметичних перетворень над числами, поліномами і точками еліптичної кривої зі зменшеною обчислювальною складністю і протидією до атак на їх реалізацію.

Для досягнення поставленої мети **необхідно розв'язати такі основні задачі**:

- проаналізувати методи постановки та перевірки ЕЦП, які використовуються у Національній системі ЕЦП Україні та шляхи, щодо підвищення їх швидкодії;
- розробити метод ділення великих цілих чисел у кільці цілих чисел зі зменшеною обчислювальною складністю;
- розробити метод мультиплікативного інвертування, приведення полінома за фіксованим модулем та здобуття кубічного кореня у полі $GF(2^m)$ зі зменшеною обчислювальною складністю;
- розробити метод арифметичних перетворень в групі точок ЕК зі зменшеною обчислювальною, структурною складністю і протидією до атак на реалізацію;
- розробити програмні моделі криптографічних перетворень на ЕК, створити на їх основі бібліотеку криптографічних перетворень;
- експериментально дослідити розроблену бібліотеку на підтвердження наукових результатів.

Об'єктом дослідження є процес криптографічних перетворень з відкритим ключем у інформаційно-телекомунікаційних системах ЦСК Національної системи ЕЦП.

Предметом дослідження є методи та способи арифметичних перетворень над числами, поліномами і точками ЕК, що застосовуються у криптографічних перетвореннях з відкритим ключем.

Методи дослідження. Проведені дослідження базуються на сучасних методах оцінки складності алгоритмів та теорії алгоритмів (для аналізу складності алгоритму скалярного множення та арифметичних операцій у групі точок ЕК, полях та кільцях); теорії криптографії (для аналізу криптографічних перетворень, побудованих на ЕК, полях та кільцях); ймовірності та комбінаторики (для аналізу складності алгоритмів); теорії еліптичних кривих (для удосконалення арифметичних операцій на ЕК у формі Вейерштрасса та Едвардса, пошуку бірационально еквівалентних відображень кривої Вейерштрасса до кривої Едвардса); теорія кілець, полів та ідеалів (для удосконалення методів мультиплікативного інвертування у полі $GF(2^m)$, здобуття кубічного кореня у полі $GF(2^m)$, приведенням полінома за фіксованим модулем у полі $GF(2^m)$, ділення великих цілих чисел у полі $GF(p)$ та кільці цілих чисел).

Наукова новизна отриманих результатів. У ході розв'язання поставлених задач *отримала подальший розвиток* теорія перетворень на ЕК, а також отримані такі результати:

- *вперше розроблено метод* автоматизації приведення довільного полінома за фіксованим модулем у полі $GF(2^m)$, який враховує степені членів для заданого тричлена та п'ятичленна, що не приводиться, для різних цільових апаратних платформ, що дозволяє будувати алгоритми приведення за фіксованим модулем з меншою обчислювальною складністю по відношенню з побітовим методом.

- *удосконалено метод* скалярного множення в групі точок ЕК над полем $GF(2^m)$, який за рахунок проміжних обчислень на кривій Едвардса, при $d_1 = d_2$, дозволяє підвищити стійкість до атак на реалізацію та підвищити швидкодію операції СК при генерації ключів, накладанні та перевірці ЕЦП за алгоритмами ДСТУ 4145-2002 та ECDSA.

- *удосконалено метод* здобуття n - вимірного кореня в полі $GF(2^m)$, де m - непарне, на прикладі кубічного кореня, який за рахунок розкладу показника степеню за допомогою адитивного ланцюга на множники, дозволяє зменшити обчислювальну складність алгоритму пошуку бірaціонально еквівалентних кривих Едвардса до кривих Вейерштрасса з ДСТУ 4145-2002 та рекомендованих NIST FIPS 186-4.

- *удосконалено метод* ділення «в стовпчик» великих цілих чисел, який за рахунок спрощення операції порівняння великих чисел, враховуючи двійкову довжину чисел; проведення операцій зсуву, додавання і віднімання за значущими словами, дозволяє знизити обчислювальну складність звичайного та розширеного алгоритму Евкліда, під час генерації загальних параметрів криптосистеми RSA.

- *удосконалено метод* мультиплікативного інвертування на основі розширеного алгоритму Евкліда у полі $GF(2^m)$, який за рахунок використання інформації про двійкову довжину параметрів рівняння Безу: відмова від обчислення степеню полінома, а лише уточнення, зсуви і додавання лише за значущими словами, дозволяє знизити обчислювальну складність при генерації ключів, накладанні та перевірці ЕЦП за алгоритмами ДСТУ 4145-2002 та ECDSA.

Практичне значення отриманих результатів полягає:

1. У розробці алгоритму ділення великих цілих чисел «в стовпчик», який дозволив підвищити швидкодію в 1,5-3 разів для чисел однакової довжини починаючи з довжини числа 512 біт, і з 128 біт для випадку, коли різниця в довжині між діленим та дільником складає 2 рази.

2. У розробці алгоритму мультиплікативного інвертування в полі $GF(2^m)$ на основі розширеного алгоритму Евкліда, який дозволив підвищити швидкодію реалізації в 1.2-1.8 разів відносно алгоритму прототипу.

3. У розробці алгоритму побудови процедури приведення за фіксованим модулем у полі $GF(2^m)$, який дозволяє будувати алгоритми для поліномів, що не приводяться, на різних цільових платформах, що дозволяють збільшити швидкодію операції приведення за модулем у 34-197 разів зі зростанням двійкової довжини відносно звичайного побітового алгоритму.

4. У розробці алгоритму здобуття n - вимірного кореня в полі $GF(2^m)$, на прикладі здобуття кубічного кореня в полі $GF(2^m)$, який дозволив зменшити обчислювальну складність в 4-4.9 разів і підвищити швидкодію в 2,8-3,7 разів зі зростанням двійкової довжини елемента поля.

5. У розробці алгоритму скалярного множення на основі удосконаленого методу з використанням проміжних обчислень на кривій Едвардса, при умові рівності параметрів

$d_1 = d_2$, який дозволив підвищити швидкодію скалярного множення на 6%, ЕЦП на 5-7% та перевірки ЕЦП на 6-7% для поля $\boldsymbol{GF}\left(2^{257}\right)$.

6. Алгоритми реалізовано у бібліотеках криптографічних примітивів «Шифр+v.2.1» системи криптографічного захисту інформації «Шифр-X.509», що має дійсний позитивний експертний висновок Держспецзв'язку України від 16.05.2017 №04/03/02-1674 (Акт від 29.09.2017 р. №12/09-17). Результати дисертаційних досліджень впроваджено у навчальний процес кафедри безпеки інформаційних технологій НАУ (Акт від 18.01.2018 р.).

Особистий внесок здобувача. Основні положення і результати дисертаційної роботи, що виносяться до захисту, отримані автором самостійно. У роботах, написаних у співавторстві, автору належать: у публікації [6] досліджувались обчислювальна та просторова складності алгоритму мультиплікативного інвертування на основі розширеного алгоритму Евкліда у двійковому полі, та був запропонований удосконалений метод для підвищення швидкодії; у роботах [1, 7] досліджувалась та була доповнена класифікація алгоритмів ділення та приведення за модулем великих цілих чисел, а також було проведено дослідження обчислювальної складності алгоритму ділення великих цілих чисел «в стовпчик» та удосконалених методів з ефективною програмною реалізацією; у роботі [2] досліджено приклади операції приведення за фіксованим модулем у двійковому полі та розроблено метод побудови алгоритму приведення за фіксованим модулем, який не залежить від характеристики полінома, що не приводиться; в роботі [12] виконано розклад показників степенів на множники для підвищення швидкодії операції здобуття кубічного кореня у двійковому полі; в роботі [3, 5] проведено дослідження обчислювальної складності алгоритму пошуку біраціонально еквівалентних кривих Едвардса до кривих Вейерштрасса та запропоновано удосконалені методи для програмної оптимізації; в роботі [8] розроблено модель операції СМ на основі проміжних обчислень на кривих Едвардса та досліджено швидкодію запропонованого і відомого методів; в патентах [9-11] досліджувалась швидкодія та обчислювальна складність запропонованих способів та прототипів.

Апробація результатів дисертації. Основні положення дисертаційної роботи доповідалися та обговорювалися на наступних конференціях: Науково-практична конференція «Проблеми експлуатації і захисту інформаційно-комунікаційних систем» (Київ, 2014); Всеукраїнська науково-практична конференція «Інформаційна безпека держави, суспільства та особистості» (Кіровоград, 2015); Міжнародна науково-практична конференція «Проблеми та перспективи розвитку IT-індустрії» (Харків, 2015); П'ятнадцята міжнародна науково-практична конференція молодих учених і студентів «ПОЛІТ»: Сучасні проблеми науки. Інформаційно-діагностичні системи: тези доповідей (Київ, 2015); Дванадцята міжнародна науково-технічна конференція «ABIA-2015» (Київ, 2015); П'ята міжнародна науково-технічна конференція «ITSEC» (Київ, 2015); Шістнадцята міжнародна науково-практична конференція «Безпека інформації у інформаційно-телекомунікаційних системах» (Київ, 2015); 3rd International Conference on the Actual Problems Of Unmanned Aerial Vehicles Developments «APUAVD 2015» (Ukraine, Kyiv, 2015); Сімнадцята міжнародна науково-практична конференція «Безпека інформації у інформаційно-телекомунікаційних системах» (Київ, 2016); 16th International Conference on Control, Automation and Systems «ICCAS 2016» (Korea, Gyeongju, 2016), 1st International Conference on Computer Science, Engineering and Education Applications (ICCSEEA2018) (Ukraine, Kyiv, 2018).

Публікації. Основні положення і результати дисертаційної роботи викладено в 20 наукових публікаціях: 7 наукових статей (4 – у міжнародних рецензованих виданнях, що входять до баз даних Scopus та 3 – у вітчизняних фахових наукових журналах), 1 розділ колективної монографії, 3 патенти України на корисну модель, 9 матеріалів та тез доповідей.

Структура та обсяг дисертації. Дисертація складається з анотації, змісту, переліку умовних позначень, вступу, п'ятьох розділів, висновку, додатків, списку використаних джерел (в кінці кожного розділу основної частини дисертації). Обсяг основного тексту дисертації складає 121 сторінку, 6 додатків на 37 сторінках, 26 рисунків, 35 таблиць. Перелік використаних джерел складається з 113 найменувань на 15 сторінках. Загальний обсяг дисертаційної роботи складає 158 сторінок.

ОСНОВНА ЧАСТИНА

У **вступі** обґрунтовано актуальність теми, сформульовано мету та задачі досліджень, відображено наукову новизну і практичну значимість отриманих результатів, впровадження отриманих результатів та їх апробація.

У **першому розділі** проведено аналіз побудови і функціонування ІТС ЦСК Національної системи ЕЦП, для якої характерним є виконання великої кількості криптографічних транзакцій (наприклад, формування та перевірка ЕЦП згідно ДСТУ 4145-2002, ECDSA чи RSA). Операція постановки ЕЦП складається безпосередньо із обчислення геш-функції, формуванні криптографічної стійкої двійкової послідовності, та самої математичної операції формування ЕЦП. У той же, час операція перевірки ЕЦП складається з наступних операцій:

1. Отримання/завантаження сертифікату відкритого ключа підписувача, перевірки його цілісності (ЕЦП) та відповідності загальносистемним параметрам.

2. Перевірка статусу сертифікату підписувача за списком відкликаних сертифікатів (СВС) чи за OCSP запитом, що включає:

2.1. За СВС: завантаження СВС на адресу, що вказана у сертифікаті підписувача; перевірка його цілісності (за допомогою ЕЦП); пошук за ідентифікатором у списку (список може налічувати десятки або і сотні тисяч записів). Далі відбувається перевірка всього ланцюжка сертифікатів, аж до кореневого – самопідписаного (сертифікат ЦЗО України).

2.2. За OCSP: відправка запиту до серверу OCSP, вказавши ідентифікатор сертифікату, що вказаний у сертифікаті підписувача; отримання відповіді від OCSP та перевірка ЕЦП на відповіді, що включає завантаження сертифікату OCSP з відповідного сховища, або вилучення цього з OCSP відповіді. Далі відбувається перевірка всього ланцюжка сертифікатів, аж до кореневого – самопідписаного (сертифікат ЦЗО України).

3. Обчислення геш-функції та самої математичної операції перевірки ЕЦП.

Таким чином час виконання транзакцій з ЕЦП можна записати наступним чином: $T = T_G + T_V$, $T_G = \sum_{i=1}^{n}\left(T_i^{\text{EDS}} + T_i^T\right)$ – формування ЕЦП та $T_V = \sum_{j=1}^{m}\left(T_j^{\text{EDS}} + T_j^T\right)$ – перевірка ЕЦП, де m – кількість запитів для перевірки, n – кількість накладання ЕЦП, T_i^{EDS} – час криптографічних транзакцій, пов'язаних з ЕЦП, T_i^T – час на передачу інформації по каналам зв'язку. Транзакції ЕЦП складаються: формування ЕЦП $T_G^{EDS} = T_H + T_{SM} + T_F$, перевірка ЕЦП $T_V^{EDS} = T_H + 2T_{SM} + T_F$, де T_H, T_{SM}, T_F – час виконання операції гешування (ГОСТ 34.311-95), виконання СМ та польових операцій в алгоритмах формування і перевірки ЕЦП згідно ДСТУ 4145-2002.

У табл. 1 представлений час реалізації стандартизованих функцій гешування з розміром даних 16кБ та СМ, реалізованих за алгоритмами ДСТУ 4145-2002 та ECDSA (NIST криві) в проективних координатах Лопаса-Дахаба, використовуючи метод Монтгомері та бінарний алгоритм приведення за модулем. Заміри часу проводилися для виконання 1 млн. операцій, за допомогою обчислювальної системи з процесором Intel Core i7-6700 2,60 GHz, під управлінням ОС Windows 10 x86-64 на мові високого рівня C++ (Microsoft Visual C++2015).

Таблиця 1

Час виконання складових операцій при формуванні та перевірці ЕЦП

Геш-функція	Гешування, МБ/с	Скалярне множення, мс		
		Поле, m	ДСТУ 4145-2002	ECDSA
ГОСТ 34.311-95	34.87	163	1.0624	1.1021
ДСТУ 7564:2014-256	101.79	167	1.4464	
ДСТУ 7564:2014-384	75.62	173	0.8057	
ДСТУ 7564:2014-512	75.59	179	1.5222	
SHA-1	422.30	191	1.1709	
SHA-224	148.81	233	2.3468	3.0743
SHA-256	148.81	257	3.1619	
SHA-384	244.14	283		3.7848
SHA-512	256.15	307	2.758	
SHA-512/224	252.01	367	5.2973	
SHA-512/256	260.42	409		8.5287
		431	6.5643	
		571		13.218

Виходячи з даних, зрозуміло, що у більшості випадків практичного застосування ЕЦП, час виконання СМ переважає над гешуванням. Тому підвищення швидкодії криптографічних перетворень на ЕК можливе за рахунок зменшення обчислювальної складності операції СМ.

Криптографічні перетворення, які покладені в основі ДСТУ 4145-2002 та ECDSA, являються перетвореннями на ЕК. Вони базуються на операції СМ точок ЕК, Рис. 1, до якої входить операції додавання і подвоєння точок ЕК, що в свою чергу виконуються над координатами точок – елементами двійкового поля. З точки зору процесора, операції над координатами точок – поліномами, представляються у вигляді машинних слів фіксованої довжини: додавання, віднімання, множення, ділення, інвертування, піднесення до степеню, видобування квадратного кореня і т. д.

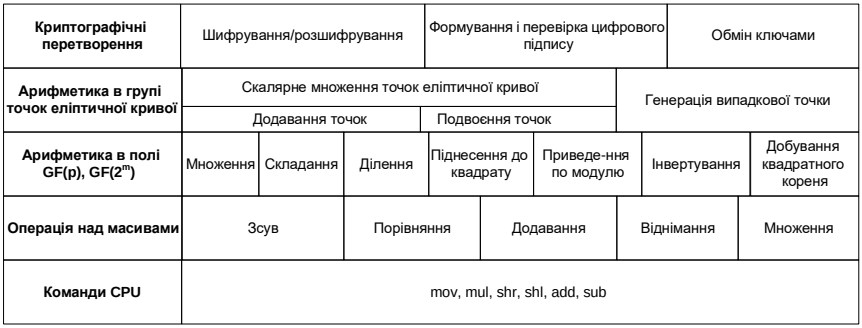

Рис. 1. Ієрархія операцій криптографічних операцій з відкритим ключем на еліптичних кривих

Тому щоб пришвидшити швидкість формування і перевірки ЕЦП, потрібно зменшити обчислювальну складність і підвищити швидкодію основної операції СМ за рахунок: перетворень в проміжних обчисленнях базової точки ЕК та довільної точки ЕК; а також обчислювальної складності арифметичних операцій над числами і поліномами. А саме ділення, приведення за модулем та інвертування, здобуття кубічного кореня (для переходу від кривих Вейерштрасса до кривих Едвардса).

Криптографічними перетвореннями на ЕК, а також підвищенням швидкодії СМ на ЕК займаються такі вчені як Бернштейн (D. J. Bernstein), Ланге (T. Lange), Козєл (B. Koziel), Молоні (R. Moloney), Горбенко І.Д., Бессалов А.В. та інші.

Також був проведений аналіз розробки квантових комп'ютерів та квантового криптоаналізу. На даний момент вони знаходяться на початку свого розвитку і в найближчі 10-15 років представлятимуть суто теоретичний інтерес.

Другий розділ присвячений удосконаленню методу ділення великих цілих чисел «в стовпчик» для криптосистеми RSA, який був обраний за рахунок простоти розуміння та реалізації (програмної та апаратної), оскільки використовує операції додавання, віднімання і зсуву. Результатом може бути як ціле, так і залишок, а також відсутні обмеження на дільник. Для подання чисел використовувалась фіксована бітова довжина. Результат множення або піднесення до квадрату чисел одинарної точності буде подано як число подвійної довжини (в 2 рази більшої до зарезервованої). Розглядалися два випадки: ділення великих цілих чисел однакової двійкової довжини – кількість машинних слів діленого та дільника однакові (1); ділення великих цілих чисел, коли двійкова довжина діленого в 2 рази перевищує довжину дільника (2).

Знизити обчислювальну складність операції ділення і підвищити швидкодію реалізації вдалося за рахунок наступних підходів:

- при порівнянні великих цілих чисел порівнювати номера старших бітів, а в разі їх рівності, проводити порівняння лише за значимими словами;
- проводити зсуви за одну ітерацію, знаючи різницю (більше 0) номерів старших бітів. При зсувах вправо використовувати лише значущі слова, а вліво – значущі слова, з урахуванням можливого переносу;
- проводити операцію віднімання за значущими словами, оскільки зменшуване більше від'ємника.

Таблиця 2

Результати експериментальної оцінки виконання операції ділення

	PC1	**PC2**	**PC1**	**PC2**	**PC1**	**PC2**	**PC1**	**PC2**	**PC1**	**PC2**	**PC1**	**PC2**
ρ	0.1		0.2		0.5		0.6		0.8		0.9	
	Час, мс											
Кількість машинних слів: діленого - 128 (4096 біт), дільника - 128 (4096 біт)												
div*	2.06	1.61	2	1.39	1.29	0.94	1.03	0.77	0.55	0.39	0.3	0.19
div	6.24	4.27	5.54	3.73	3.35	2.26	2.62	1.79	1.3	0.87	0.66	0.42
	3.03	**2.66**	**2.77**	**2.69**	**2.59**	**2.42**	**2.55**	**2.35**	**2.37**	**2.24**	**2.21**	**2.25**
Кількість машинних слів: діленого - 128 (4096 біт), дільника - 64 (2048 біт)												
div*	2.37	1.73	2.17	1.65	2	1.51	1.92	1.42	1.58	1.14	1.31	1.13
div	6.22	4.31	5.8	4.07	5.13	3.57	4.81	3.28	3.79	2.59	3.37	2.32
	2.63	**2.49**	**2.68**	**2.46**	**2.57**	**2.36**	**2.50**	**2.31**	**2.41**	**2.27**	**2.57**	**2.05**

ρ - відношення числа використовуваних біт до числа зарезервованих у великому числі (дільник);

div – реалізація алгоритму прототипу;

div*- реалізація алгоритму, удосконаленого методу;

У табл. 2 представлено порівняння швидкодії методу прототипу і удосконаленого, на основі програмної реалізації за допомогою Visual C++2010. Заміри часу проводилися для 100 тис. операцій, за допомогою обчислювальних систем Intel Core i3 M350 (PC1) і Intel Xeon E5 - 2640 (PC2), під управлінням ОС Windows 7 SP1 x86-64. У таблиці показано порівняння реалізацій лише для двох випадків, при довжині машинного слова $w=32$. Експеримент показав, що на час реалізації впливає відношення кількості одиничних бітів.

У табл. 3 представлено час реалізації генерації ключів для RSA з використанням алгоритму прототипу і удосконаленого. Використовувався тестовий генератор псевдовипадкових послідовностей з ДСТУ 4145-2002 на основі ГОСТ 28147-89 (наперед заданою послідовністю), оскільки генерація ключів – це імовірнісний алгоритм, що дозволяє генерувати одну і туж послідовність для заданої довжини ключа. Для генерації

простих чисел p і q використовується алгоритм Рабіна-Міллера, де число випробувань дорівнює 50. Для наочності, наводяться значення для відкритої експоненти $e = 65537$. Програмна реалізація відтворена за допомогою Visual C++2015 на Intel Core i7-6700HQ 2.6 GHz під управлінням Windows 10 x86-64.

Таблиця 3

Результати експериментальної оцінки генерації ключів RSA

Довжина ключа	Час, с		Виграш	Довжина ключа	Час, с		Виграш
	Відомий метод	Удосконалений метод			Відомий метод	Удосконалений метод	
512	0.014	0.013	1.077	4096	3.153	2.803	1.125
1024	0.0762	0.07	1.089	8192	147.107	129.166	1.139
2048	0.3799	0.345	1.101				

За допомогою запропонованого методу ділення великих цілих чисел, вдалося підвищити швидкодію програмної реалізації в 1,5-3 рази, порівнюючи з прототипом з ростом двійкової довжини цілого числа: в разі (1) для чисел довжиною від 512 біт і в разі (2) - від 128 біт, що в свою чергу дало змогу підвищити швидкодію генерації ключів RSA на 7-14%.

У **третьому розділі** розглядається удосконалення методу мультиплікативного інвертування полі $\boldsymbol{GF}(2^m)$ та пропонується метод автоматизації приведення довільного полінома за фіксованим модулем у полі $\boldsymbol{GF}(2^m)$. Для зменшення впливу трудомісткої операції інвертування, пропонують переходити до проективного подання точок ЕК, проте повністю позбутися від даної операції – неможливо. У даному розділі, алгоритмом прототипом, обирався розширений алгоритм Евкліда.

Він основується на двох інваріантах $ba + df = u$ і $ca + ef = v$ для деяких d і e, які обчислюються явно. На кожній ітерації, якщо виконується умова $\deg(u) \geq \deg(v)$, часткове розподілення u через v, виконується зсув $x^j v$ для u, де $j = \deg(u) - \deg(v)$. У результаті чого, степінь u залишається постійною, або зменшується мінімум на 1. Додавання $x^j c$ з b дозволяє зберегти інваріанти. Алгоритм виконує в середньому $\deg(a) = k$ ітерацій і зупиняється при умові $\deg(u) = 0$, у цьому випадку $u = 1$ и $ba + df = 1$, отже $b = a^{-1} \bmod f(x)$.

Удосконалити розширений алгоритм Евкліда для мультиплікативного інвертування, в якому вдалося знизити обчислювальну складність і підвищити швидкодію реалізації, за рахунок наступних підходів:

- застосування методу «наступного відповідного», що дозволило відмовитися від обчислення $\deg(v)$, а лише уточнювати її за рахунок степеню полінома $u(x)$;

- застосування методу «врахування значущих елементів», який застосовувався при операціях додавання та зсуву поліномів. Степені поліномів $u(x)$ і $v(x)$ – зменшуються, а поліномів $b(x)$ і $c(x)$ – зростають. Це дозволило проводити операції додавання і зсуву поліномів лише за значущими словами;

- застосування алгоритму-трюку «обчислення номера старшого значущого біта» в машинному слові, без операції галуження. Обчислення степеню полінома $u(x)$ на кожній ітерації, базуються на попередніх значеннях.

Експерименти проводилися для різних показників розширення двійкових полів m, на мобільних процесорах Intel Core i3 M350 і настільних процесорах Intel Core i5-3570, Intel Core i5-4670 під управлінням ОС Windows 7 SP1 x86-64. Програмна реалізація виконана за допомогою Visual C++2015. За основу бралися двійкові поля з ДСТУ 4145-

2002 і NIST FIPS 186-4. У табл. 4 наведено результати експериментальних досліджень програмної реалізації запропонованого методу в проективних координатах Лопеса-Дахаба.

Таблиця 4

Результати експериментальної оцінки виконання операції інвертування в двійковому полі

m	Час, мкс											
	Intel Core i3-350M				Intel Core i5-3570				Intel Core i5-4670			
	ICC XE2013		MCC2010		ICC XE2013		MCC2010		ICC XE2013		MCC2010	
	Inv	Inv*	Inv	Inv*	Inv	Inv*	Inv	Inv*	Inv	Inv*	Inv	Inv*
89	6.71	5.44	6.27	5.1	2.53	1.95	2.76	1.84	2.53	1.95	2.37	1.84
163	16.08	11.34	14.38	11.96	6.85	4.05	6.33	4.65	6.85	3.95	6.13	4.05
191	18.17	14.52	17.38	14.71	7.73	5.46	7.85	5.48	7.73	5.26	7.65	5.48
233	27.13	22.12	24.57	19.39	11.8	7.04	11.59	7.65	11.8	7.02	11.02	6.9
257	31.56	25.18	27.93	24.54	13.21	7.99	13.33	8.56	12.17	7.81	12.33	7.6
307	37.72	30.45	34.24	26.11	17.98	11.11	17.64	12.41	17.68	9.58	17.54	11.41
367	53.18	42.17	46.05	33.81	23.35	14.78	21.84	16.63	22.35	13.18	21.64	14.63
409	61.31	40.18	54.48	47.76	26.41	16.97	26.81	18.51	25.97	14.93	26.41	17.51
431	67.75	54.24	59.1	44.03	28.99	17.86	29.29	19.25	28.27	17	28.99	18.25
571	103.4	64.86	94.42	70.26	46.46	25.47	44.87	26.98	43.39	24.64	44.67	26.83

- [*] - удосконалений алгоритм, із запропонованими підходами для оптимізації.
- степінь полінома близька до m .

Результати експерименту показали виграш в швидкодії в 1.2-1.8 разів.

У табл. 5 представлено вплив удосконаленого методу інвертування при формуванні та перевірці ЕЦП згідно ДСТУ 4145-2002: СМ відбувалося у 2 потоки (метод Монтгомері) в проективних координатах Лопеса-Дахаба. Програмна реалізація відтворена за допомогою Visual C++2015 на Intel Core i7-6700HQ 2.6 GHz, під управлінням Windows 10 x86-64.

Таблиця 5

Результати експериментальної оцінки виконання формування і перевірки ЕЦП

m	Формування ЕЦП			Перевірка ЕЦП		
	Inv, мс	Inv*, мс	Виграш	Inv, мс	Inv*, мс	Виграш
163	1.693	1.69	1.0018	1.853	1.845	1.0042
167	1.747	1.744	1.0019	1.879	1.871	1.0043
173	1.871	1.868	1.0018	1.993	1.985	1.0040
179	2.002	1.999	1.0016	2.256	2.249	1.0033
191	2.324	2.32	1.0016	2.488	2.479	1.0035
233	3.522	3.516	1.0017	3.767	3.752	1.0041
257	4.541	4.534	1.0015	4.979	4.962	1.0034
307	6.506	6.497	1.0014	7.045	7.023	1.0032
367	9.559	9.547	1.0012	10.389	10.36	1.0028
431	13.615	13.6	1.0011	14.445	14.406	1.0027

Проведений аналіз публікацій, присвячених ефективній реалізації криптографічних алгоритмів на ЕК показав, що найчастішою операцією являється приведення за фіксованим модулем. В роботах показані алгоритми для деяких поліномів, що не приводяться, з рекомендованого переліку NIST FIPS 186-4, а також описується загальна ідея. У розділі розробляється метод побудови алгоритмів приведення за фіксованим модулем, що дозволяє збільшити швидкодію операції формування і перевірки ЕЦП на основі ДСТУ 4145-2002 та ECDSA, враховуючи поліном, що не приводиться, та розрядність цільової архітектури.

На прикладі п’ятичлена $f(x)=x^k+x^l+x^g+x^e+1$, де $k>l>g>e$, розглянемо застосування методу для побудови алгоритму на основі полінома, що не приводиться. Для цього, представимо модуль у такому вигляді:

$$\begin{array}{cccc} x^{k+r} & x^{k+r-1} & \dots & x^{k+r-(w-1)} \\ x^{l+r} & x^{l+r-1} & \dots & x^{l+r-(w-1)} \\ x^{g+r} & x^{g+r-1} & \dots & x^{g+r-(w-1)} \\ x^{e+r} & x^{e+r-1} & \dots & x^{e+r-(w-1)} \\ x^{r} & x^{r-1} & \dots & x^{r-(w-1)} \end{array}$$

Рис. 2. Представлення модуля після вирівнювання

Де горизонтально записані біти – коефіцієнти при членах полінома, які утворюють одне машинне слово, довжиною w-біт, $r = \lceil 2(k-1)/w \rceil \cdot w - k$, де r - це різниця між старшими степенями полінома, що приводимо за модулем.

Дане представлення дозволяє формувати слово з бітів $(x_{i+r}, x_{i+r-1}, \dots, x_{i+r-(w-1)})$ і складати його за модулем зі словами $(x_{i+r}, x_{i+r-1}, \dots, x_{i+r-(w-1)})$, $(x_{g+r}, x_{g+r-1}, \dots, x_{g+r-(w-1)})$, $(x_{e+r}, x_{e+r-1}, \dots, x_{e+r-(w-1)})$, $(x_{r}, x_{r-1}, \dots, x_{r-(w-1)})$. Дану операцію необхідно повторювати зменшуючи на кожній ітерації значення r на величину w, доки $r > 0$. Останньою ітерацією являється розгляд не всього слова, а лише його частини $r(\mathrm{mod}\ w)$ (рис.3).

Враховуючи, що значення z_1, z_2, z_3 і z_4 можуть бути однакові, то існує можливість об'єднання кроків 4.1-4.3, а також кроків 6-9.

Вхід: поліном $c(x)$ степеню не більше $2(k-1)$.
Вихід: поліном $d(x) \equiv c(x) (\mathrm{mod} f(x))$.
1. $m \leftarrow \lceil 2(k-1)/w \rceil - 1$, $n \leftarrow \lceil k/w \rceil$, $r \leftarrow \lceil 2(k-1)/w \rceil \cdot w - k$, $s_1 \leftarrow \lceil (l+r)/w \rceil \cdot w - (l+r)$, $z_1 \leftarrow m - (\lceil (l+r)/w \rceil - 1)$
2. $s_2 \leftarrow \lceil (g+r)/w \rceil \cdot w - (g+r)$, $z_2 \leftarrow m - (\lceil (g+r)/w \rceil - 1)$, $s_3 \leftarrow \lceil (e+r)/w \rceil \cdot w - (e+r)$, $z_3 \leftarrow m - (\lceil (e+r)/w \rceil - 1)$
3. $s_4 \leftarrow \lceil r/w \rceil \cdot w - r$, $z_4 \leftarrow m - (\lceil r/w \rceil - 1)$
4. for $i \leftarrow m; i \geq n; i--$
4.1. $t \leftarrow c_i$, $d_{i-z_1} \leftarrow c_{i-z_1} \oplus (t << (w - s_1))$, $d_{i-z_2} \leftarrow c_{i-z_2} \oplus (t >> s_2)$
4.2. $d_{i-z_2-1} \leftarrow c_{i-z_2-1} \oplus (t << (w - s_2))$, $d_{i-z_3} \leftarrow c_{i-z_3} \oplus (t >> s_3)$, $d_{i-z_3-1} \leftarrow c_{i-z_3-1} \oplus (t << (w - s_3))$
4.3. $d_{i-z_4} \leftarrow c_{i-z_4} \oplus (t >> s_4)$, $d_{i-z_4-1} \leftarrow c_{i-z_4-1} \oplus (t << (w - s_4))$.
5. $t \leftarrow c_{i-1}(x_{i-1}, x_{i-2}, \dots, x_{(k \bmod w)}, 0_{(k \bmod w)-1}, \dots, 0_0)$ // розглядаються старші біти, від $(w-1)$ до $(k \bmod w)$, решта бітів ігноруються.
6. if $(n - z_1) \geq 0$ then $d_{n-z_1} \leftarrow c_{n-z_1} \oplus (t >> s_1)$, if $(n - z_1 - 1) \geq 0$ then $d_{n-z_1-1} \leftarrow c_{n-z_1-1} \oplus (t << (w - s_1))$
7. if $(n - z_2) \geq 0$ then $d_{n-z_2} \leftarrow c_{n-z_2} \oplus (t >> s_2)$, if $(n - z_2 - 1) \geq 0$ then $d_{n-z_2-1} \leftarrow c_{n-z_2-1} \oplus (t << (w - s_2))$
8.if $(n - z_3) \geq 0$ then $d_{n-z_3} \leftarrow c_{n-z_3} \oplus (t >> s_3)$, if $(n - z_3 - 1) \geq 0$ then $d_{n-z_3-1} \leftarrow c_{n-z_3-1} \oplus (t << (w - s_3))$
9. if $(n - z_4) \geq 0$ then $d_{n-z_4} \leftarrow c_{n-z_4} \oplus (t >> s_4)$, if $(n - z_4 - 1) \geq 0$ then $d_{n-z_4-1} \leftarrow c_{n-z_4-1} \oplus (t << (w - s_4))$
10. $d_{n-1} \leftarrow c_{n-1}(0_{w-1}, 0_{w-2}, \dots 0_{(k \bmod w)}, x_{(k \bmod w)-1}, x_{(k \bmod w)-2}, \dots, x_0)$. // розглядаються молодші біти від $(k \bmod w) - 1$ до 0, решта бітів ігноруються.
11. Return $(d(x))$.

Рис.3. Псевдокод побудови алгоритмів приведення за фіксованим модулем на прикладі довільного п'ятичлена

Таблиця 6

Час реалізації побітового та послівного методів для 32-розрядних платформ

Поліном, що не приводиться	**Побітовий метод, мс**	**Послівний метод, мс**	**Виграш**
$f_{128}(x) = x^{128} + x^7 + x^2 + x^1 + 1$	0,324494	0,009327	34,8
$f_{256}(x) = x^{256} + x^{10} + x^5 + x^2 + 1$	1,151691	0,015098	76,28
$f_{512}(x) = x^{512} + x^8 + x^5 + x^2 + 1$	5,420564	0,027486	197,21

У табл. 6 наведено результати практичної реалізації запропонованого методу на обчислювальній системі з процесором Intel Core i5-3570, під управлінням ОС Windows 7 SP1 x86-64. Програмна реалізація виконана за допомогою Visual C++ 2015.

Результати табл. 6, показують, що реалізація алгоритму дозволила збільшити швидкодію операції приведення за модулем у 34-197 разів відносно побітового методу зі зростанням двійкової довжини для поліномів з ДСТУ 7624:2014.

У табл. 7 показано результати впливу використання побітового приведення за модулем та послівного при формуванні та перевірці ЕЦП згідно ДСТУ 4145-2002, використовуючи удосконалений метод мультиплікативного інвертування.

Таблиця 7

Результати експериментальної оцінки виконання формування і перевірки ЕЦП

Поле, m	**Час постановки ЕЦП, мс**			**Час перевірки ЕЦП, мс**		
	Побітовий метод	**Послівний метод**	**Виграш**	**Побітовий метод**	**Послівний метод**	**Виграш**
163	1.69	0.228	7.41	1.845	0.237	7.78
167	1.744	0.258	6.76	1.871	0.248	7.54
173	1.868	0.252	7.41	1.985	0.259	7.66
179	1.999	0.259	7.72	2.249	0.259	8.68
191	2.32	0.267	8.69	2.479	0.285	8.70
233	3.516	0.58	6.06	3.752	0.591	6.35
257	4.534	0.688	6.59	4.962	0.693	7.16
307	6.497	0.938	6.93	7.023	0.912	7.70
367	9.547	1.366	6.99	10.36	1.457	7.11
431	13.6	1.967	6.91	14.406	2.088	6.90

Послівний метод дозволив підвищити швидкодію при формуванні ЕЦП в 6-9.4 разів, при перевірці ЕЦП в 7-9.4.

У **четвертому розділі** розглядається удосконалення методу здобуття n-вимірного кореня в полі $GF(2^m)$, де m - непарне, на прикладі кубічного кореня, який був необхідний для підвищення швидкодії пошуку бірaціонально еквівалентних кривих Едвардса до кривих Вейерштрасса, представлених в ДСТУ 4145-2002 (див. розділ 5).

Пропонується розкладати показник степеню кубічного кореня в адитивний ланцюг, що дозволяє зменшити кількість операцій множення:

$1/3 = \sum_{j=0}^{\lfloor m-1 \rfloor/2} 2^{2\cdot j} \bmod (2^m - 1)$ для полів з непарною характеристикою, можна спростити застосувавши відому ітераційну схему, де початкове $n = 2$ і $(k-2)n$ - парне:

$$1 + 2^n + \ldots + 2^{(k-2)n} = \begin{cases} (1+2^n)\times(1+2^{2n}+\ldots+2^{(k-3)n}), & \text{якщо } k-1 \equiv 0 \bmod 2 \\ 1+2^n(1+2^n)\times(1+2^{2n}+\ldots+2^{(k-4)n}), & \text{якщо } k-1 \equiv 1 \bmod 2 \end{cases}$$

У табл. 8 представленні розклади показника степеню в адитивний ланцюг в залежності від характеристики полів $GF(2^m)$, представлених у ДСТУ 4145-2002.

Розроблено алгоритми знаходження кубічного кореня для полів з ДСТУ 4145-2002. Експериментальна оцінка швидкодії здобуття кубічного кореня та обчислювальна складність для різних показників розширення m полів $GF(2^m)$, використовуючи процесор Intel Core i7-2600 під управлінням ОС Windows 7 SP1 x86-64, приведена у табл. 9. Програмна реалізація виконана за допомогою Visual C++2015. Число випробувань складає 1 млн. операцій.

Для порівняння обчислювальної складності, приймається відношення операцій: 1**S**=0.1**M**. Виграш в обчислювальній складності показує 4-4,9 разів зі зростанням розширення поля. Виграш швидкодії програмної реалізації показує 2.4-3.7 разів.

Таблиця 8

Розклад адитивного ланцюга

Поле, m	**Розклад в адитивний ланцюг**
163	$(1+2^2)(1+2^4(1+2^4)(1+2^8)(1+2^{16})(1+2^{32}(1+2^{32})(1+2^{64})))$
167	$(1+2^2)(1+2^4)(1+2^8(1+2^8)(1+2^{16})(1+2^{32}(1+2^{32})(1+2^{64})))$
173	$1+2^2(1+2^2)(1+2^4(1+2^4)(1+2^8(1+2^8)(1+2^{16})(1+2^{32}(1+2^{32})(1+2^{64}))))$
179	$(1+2^2)(1+2^4(1+2^4)(1+2^8)(1+2^{16}(1+2^{16})(1+2^{32}(1+2^{32}))(1+2^{64})))$
191	$(1+2^2)(1+2^4)(1+2^8)(1+2^{16})(1+2^{32})(1+2^{64}(1+2^{64}))$
233	$1+2^2(1+2^2)(1+2^4)(1+2^8(1+2^8)(1+2^{16})(1+2^{32}(1+2^{32})(1+2^{64}(1+2^{64}))))$
257	$1+2^2(1+2^2)(1+2^4)(1+2^8)(1+2^{16})(1+2^{32})(1+2^{64})(1+2^{128})$
307	$(1+2^2)(1+2^4(1+2^4)(1+2^8)(1+2^{16}(1+2^{16})(1+2^{32}(1+2^{32})(1+2^{64})(1+2^{128}))))$
367	$(1+2^2)(1+2^4)(1+2^8)(1+2^{16}(1+2^{16})(1+2^{32}(1+2^{32})(1+2^{64}(1+2^{64})(1+2^{128}))))$
431	$(1+2^2)(1+2^4)(1+2^8)(1+2^{16}(1+2^{16})(1+2^{32}(1+2^{32})(1+2^{64})(1+2^{128}(1+2^{128}))))$

Таблиця 9

Обчислювальна складність і швидкодія здобуття кубічного кореня

Поле, m	**Відомий метод**		**Удосконалений метод**		**Виграш**	
	Кількість операцій	**Час реалізації, мс**	**Кількість операцій**	**Час реалізації, мс**	**Склад-ність**	**Швидко-дія**
163	81**M**+162**S**	0.0233	8**M**+162**S**	0.0093	4.02	2.51
167	83**M**+166**S**	0.024	8**M**+166**S**	0.0095	4.05	2.53
173	86**M**+172**S**	0.0261	10**M**+172**S**	0.0104	3.79	2.51
179	89**M**+178**S**	0.0277	9**M**+178**S**	0.0114	3.99	2.43
191	95**M**+190**S**	0.0292	7**M**+190**S**	0.0099	4.38	2.95
233	116**M**+232**S**	0.0481	10**M**+232**S**	0.0173	4.19	2.78
257	128**M**+256**S**	0.0629	8**M**+256**S**	0.0201	4.57	3.13
307	153**M**+306**S**	0.086	10**M**+306**S**	0.0284	4.52	3.03
367	183**M**+366**S**	0.1315	10**M**+366**S**	0.0361	4.71	3.64
431	215**M**+430**S**	0.1953	10**M**+430**S**	0.0523	4.87	3.73

У **п'ятому розділі** увага приділена пошуку біраціонально еквівалентних кривих Едвардса до кривих Вейерштрасса для поля $\boldsymbol{GF}(2^m)$, представлених в ДСТУ 4145-2002 з використанням кубічного кореня, а також розробляється алгоритм з використанням відповідних базових точок Едвардса в проміжних обчисленням СМ.

Це зумовлено тим, що недоліком операцій над ЕЦП являється їх недостатня швидкодія і вразливість до атак на реалізацію.

Операціям на кривій Едвардса властивий повний уніфікований груповий закон, який є лінійним (без галужень) з точки зору виконання інструкцій процесором, які властиві при додаванні точок ЕК в формі Вейерштрасса (наприклад, формула складання ідентична для P і P, а також P і $-P$).

Алгоритм СМ точок на кривій Вейерштрасса для існуючих криптосистем з проміжними розрахунками на кривій Едвардса:

Обчислення деяких перетворень (може бути виконаний раніше):

1. Пошук біраціонально еквівалентної кривої Едвардса.

2. Обчислення перетворення базової точки P кривої Вейерштрасса до точки P' на кривій Едвардса.

Скалярне множення:

1. $Q' = k \cdot P'$ використовуючи алгоритм Монтгомері з диференціальним w-проективним додаванням і подвоєнням точок.

2. Перетворення точки Q' на кривій Едвардса до точки Q на кривій Вейерштрасса.

3. Return Q .

Таблиця 10

Час пошуку бірaціонально еквівалентної кривої і точки Едвардса до кривої Вейерштрасса для ДСТУ 4145-2002 (Intel Core i7-6700 2,60 GHz (Microsoft Windows 10 x86-64))

m	**Час реалізації, мс**		**Виграш**	m	**Час реалізації, мс**		**Виграш**
	LMZ	LMZ*			LMZ	LMZ*	
163	0.1202	0.0805	1.49	233	0.2741	0.2054	1.33
167	0.1507	0.1054	1.43	257	0.2676	0.1854	1.44
173	0.1252	0.0872	1.44	307	0.3883	0.2408	1.61
179	0.1412	0.0967	1.46	367	0.6256	0.3807	1.64
191	0.1739	0.123	1.41	431	0.8382	0.4762	1.76

- LMZ* - метод Li-Miri-Zhu з використанням удосконаленого методу здобуття кубічного кореня.

Аналіз відомих методів пошуку бірaціонально еквівалентної кривої показав, що найбільш ефективним є метод Li-Miri-Zhu. Подальше зменшення обчислювальної складності та підвищення швидкодії реалізації можливе за рахунок наступних підходів: передобчислень та використання удосконаленого методу при здобутті кубічного кореня. Удосконалений метод пошуку бірaціонально еквівалентних кривих і точок показав виграш у швидкодії в 1,3-1,8 разів (див.табл.10).

Таблиця 11

Порівняння швидкодії реалізації операції СМ в проективних координатах для ДСТУ 4145-2002 (Intel Xeon E3-1270v5 3.6GHz, Windows) використовуючи спеціалізований набір інструкцій

m	**Час реалізації СМ, мс**				
	Бірaціонально еквівалентна крива Вейерштрасса до БЕК 251	**Криві Вейерштрасса з ДСТУ4145-2002**	**Бірaціональна крива Едвардса для кривих з ДСТУ4145-2002**		**БЕК 251**
			$d_1 \neq d_2$	$d_1 = d_2$	$d_1 = d_2$
	Алгоритм Монтгомері (проективні координати Лопеса-Дахаба)		**Алгоритм Монтгомері (проективні w-координати)**		
163		0.183	0.354		
167		0.186	0.353		
173		0.203	0.378	0.214	
179		0.211	0.400		
191		0.226	0.427		
233		0.399	0.759		
251	0.527				0.489
257		0.531	0.981	0.505	
307		0.719	1.323		
367		1.062	1.984		
431		1.602	2.943		

Реалізація алгоритму СМ була виконана за методом Монтгомері за допомогою Visual C++2015 та gcc 5.4.0 з урахуванням розробленого методу приведення за фіксованим модулем і удосконаленого методу інвертування на основі розширеного алгоритму Евкліда. Заміри часу проводилися для 10 тис. операцій, за допомогою обчислювальних

систем з процесорами Intel Xeon E3-1270v5 3,60 GHz під управлінням Microsoft Windows Server 2012 R2 та Intel Xeon E5-2640 2.5 GHz під управлінням CentOS Linux v7.0 x86-64.

У табл. 11-12 представлені результати вимірів швидкодії реалізації операції СМ для двійкових кривих Вейерштрасса і відповідних біраціонально еквівалентних кривих Едвардса в проективних w-координатах.

Таблиця 12

Порівняння швидкодії реалізації операції СМ в проективних координатах для ДСТУ 4145-2002 (Intel Xeon E5-2695v3 2.3 GHz, CentOS Linux v7.0 x86-64)

m	**Час реалізації СМ, мс**				
	Біраціонально еквівалентна крива Вейерштрасса до ВЕС 251	**Криві Вейерштрасса з ДСТУ4145-2002**	**Біраціональна крива Едвардса для кривих з ДСТУ4145-2002**		**ВЕС 251**
			$d_1 \neq d_2$	$d_1 = d_2$	$d_1 = d_2$
	Алгоритм Монтгомері (проективні координати Лопеса-Дахаба)		**Алгоритм Монтгомері (проективні w-координати)**		
163		0.197	0.401		
163#		0.254	0.360		
167		0.188	0.397		
167#		0.177	0.394		
173		0.209	0.433	0.282	
173#		0.287	0.397	0.282	
179		0.214	0.443		
179#		0.214	0.670		
191		0.219	0.439		
191#		0.215	0.455		
233		0.368	0.679		
233#		0.361	0.668		
251	0.519				0.466
251#	0.512				0.472
257		0.525	1.325	0.495	
257#		0.518	0.980	0.487	
307		0.723	1.572		
307#		0.701	1.341		
367		1.285	2.394		
367#		1.071	2.013		
431		1.809	3.170		
431#		1.588	3.072		

- # - спеціалізований набір інструкцій процесора.

Результати показують, що швидкодія операції СМ на кривих Вейерштрасса переважає над біраціонально еквівалентними кривими Едвардса з двома параметрами. Однак за умови $d_1 = d_2$, швидкодія реалізації СМ для кривих Едвардса зростає, починаючи з поля, розміром 257 біт: для процесора Intel Xeon E3-1270v5 3.6GHz (Microsoft Windows Server 2012 R2 x86-64) та Intel Xeon E5-2695v3 2.3 GHz (CentOS Linux v7.0 x86-64) виграш в швидкодії склав 5% і 6%, відповідно.

Для кривої БЕК251, швидкодія реалізації СМ склала: для процесора Intel Xeon E3-1270v5 3,60 GHz (Microsoft Windows Server 2012 R2) - 7%; Intel Xeon E5-2695v3 2.3 GHz (CentOS Linux v7.0 x86-64) - 11%.

Табл. 13 показує виграш при формуванні та перевірки ЕЦП на біраціонально

еквівалентних кривих Едвардса, при умові $d_1 = d_2$: для процесора Intel Xeon E5-2695v3 2,30 GHz (CentOS Linux v7.0 x86-64) та Intel Xeon E3-1270v5 3,60 GHz (Microsoft Windows Server 2012 R2 x86-64) виграш 6% при формуванні та 4% і 6% при перевірці, відповідно.

Таблиця 13

Час реалізації формування і перевірки ЕЦП згідно ДСТУ 4145-2002

Поле m	Час, мс							
	Формування ЕЦП				Перевірка ЕЦП			
	W	E $d_1 \neq d_2$	E $d_1 = d_2$	Виграш	W	E $d_1 \neq d_2$	E $d_1 = d_2$	Виграш
257*	0,539	1,185	0,510	1,06	1,251	2,345	1,207	1,04
257**	0,535	1,599	0,507	1,06	1,164	2,309	1,111	1,05
257#	0,535	0,984	0,506	1,06	0,556	0,982	0,525	1,06

* - Intel Xeon E5-2695v3 2,30 GHz (CentOS Linux v7.0 x86-64) зі стандартним набором інструкцій;
** - Intel Xeon E5-2695v3 2,30 GHz (CentOS Linux v7.0 x86-64) з спеціалізованим набором інструкцій;
# - Intel Xeon E3-1270v5 3,60 GHz (Microsoft Windows Server 2012 R2 x86-64) з спеціалізованим набором інструкцій і СМ у два потоки при перевірці ЕЦП;
W – двійкова крива Вейерштрасса;
E - бірaціонально еквівалентна крива Едвардса.

У **додатках** наведено патенти на корисну модель, дані бірaціонально еквівалентних кривих Едвардса до двійкових кривих Вейерштрасса з ДСТУ 4145-2002, результати експертних оцінок для СМ та ЕЦП на додаткових процесорах, розроблені алгоритми здобуття кубічного кореня в двійковому полі та акти на впроваджених результатів дисертаційної роботи.

ВИСНОВКИ

У дисертаційній роботі, відповідно до поставленої мети, розв'язана актуальна науково-технічна задача підвищення швидкодії ІТС ЦСК Національної системи ЕЦП шляхом зменшення обчислювальної складності криптографічних алгоритмів на основі розробки нових методів та алгоритмів арифметичних перетворень числами, поліномами і точками ЕК.

У процесі виконання дисертаційної роботи отримані такі основні результати:

1. Проведено аналіз функціонування складових Національної системи ЕЦП України, та встановлено, що воно на пряму залежить від часу та кількості операцій формування та перевірки ЕЦП. Результати проведеного аналізу дали можливість визначити завдання дисертаційного дослідження щодо розробки та удосконалення методів для підвищення швидкодії ІТС ЦСК.

2. Удосконалений метод ділення великих цілих чисел дозволив збільшити швидкодію операції генерації ключів RSA на 7-14% зі збільшенням двійкової довжини, використовуючи компілятор Visual C++2015 на Intel Core i7-6700HQ 2,60 GHz під управлінням Windows 10 x86-64.

3. Удосконалений метод інвертування на основі розширеного алгоритму Евкліда в полі $\boldsymbol{GF}(2^m)$ дозволив підвищити швидкодію при формуванні та перевірці ЕЦП для ДСТУ 4145-2002 в 1.0011-0.0019 і 1.0027-0.0043, використовуючи компілятор Visual C++2015 на Intel Core i7-6700HQ 2,60 GHz під управлінням Windows 10 x86-64. Виграш при постановці та перевірці ЕЦП для 1 робочого дня середнього банку склав 1-9 с та 3-20 с відповідно.

4. Удосконалений метод здобуття n - мірного кореня в полі $\boldsymbol{GF}(2^m)$, на прикладі здобуття кубічного кореня в полі $\boldsymbol{GF}(2^m)$, дозволив збільшити швидкодію відшукання

біраціонально еквівалентних кривих Едвардса в 1,3-1,8 разів, використовуючи компілятор Visual C ++ 2015 на Intel Core i7-6700HQ 2,60 GHz під управлінням Windows 10 x86-64.

5. Розроблений метод автоматизації приведення довільного полінома за фіксованим модулем у полі $GF(2^m)$, дозволив в незалежності від полінома (тричлена, п'ятичлена), що не приводиться, згенерувати алгоритми приведення за модулем для різних цільових платформ, а також дозволив підвищити швидкодію при формуванні та перевірці ЕЦП, згідно ДСТУ 4145-2002 в 6.-9.4 і 7-9.4 разів відповідно.

6. Використання біраціонально еквівалентних кривих Едвардса з одним параметром для поля 257 при виконанні операції СМ дозволили підвищити швидкодію формування ЕЦП на 5-7% та перевірки ЕЦП на 6-7% для кривих з ДСТУ 4145-2002, в залежності від процесора.

7. Виграш при використанні біраціонально еквівалентних кривих Едвардса для поля 257 згідно ДСТУ 4145-2002 складає при постановці 12-13 с, при перевірці 13-23 с для 1 робочого дня середнього банку, як складової Національної системи ЕЦП.

8. При порівнянні значимості експериментальних оцінок (часу) удосконалених методів здобуття кубічного кореня, мультиплікативного інвертування в двійковому полі та ділення великих цілих чисел і прототипів за допомогою t-тест Стьюдента і тест Манна-Уітні, було встановлено, що відмінності між вибірками є статистично значущими.

9. На основі запропонованих удосконалених методів та відповідних програмних моделей криптографічних перетворень на ЕК, було розроблено бібліотеку криптографічних примітивів, яка використовується у діяльності «Сайфер ЛТД» (акт від 28.09.2017 року № 12/09-17). Результати дисертаційних досліджень впроваджено у навчальний процес кафедри безпеки інформаційних технологій НАУ (акт впровадження від 18.01.2018 р.).

ПУБЛІКАЦІЇ ЗДОБУВАЧА ЗА ТЕМОЮ ДИСЕРТАЦІЇ

1. М.Г. Ковтун, В.Ю. Ковтун. «Подходы к повышению производительности операции деления больших целых чисел, на основе расширенного алгоритма Евклида» в *Информационные технологии и защита информации в информационно-коммуникационных системах: раздел коллективной монографии*. В.С. Пономаренко, Харьков: ТОВ «Щедра садиба плюс», 2015, с. 208-219.

2. M. Kovtun, A. Okhrimenko, T. Gancarczyk, V. Karpinskyi, S. Gnatyuk. «Method of Algorithm Building for Modular Reducing by Irreducible Polynomial», *in Proc. of the 16th International Conference on Control, Automation and Systems*, Oct. 16-19, 2016, Gyeongju, Korea. pp.1476-1479. DOI:10.1109/ICCAS.2016.7832498. *(Scopus)*

3. M. Kovtun, Z. Hu, S. Gnatyuk and N. Seilova, «Method of Searching Birationally Equivalent Edwards Curves Over Binary Fields», *Advances in Intelligent Systems and Computing*, pp. 309-319, 2018. DOI:10.1007/978-3-319-91008-6_31. (Scopus)

4. M. Kovtun, V. Kovtun, A. Okrimenko. «Commands Integrity and Authority in Control Radio Link of UAV», *2015 IEEE International Conference Actual Problems of Unmanned Aerial Vehicles Developments (APUAVD)*, 2015. DOI: 10.1109/APUAVD.2015.7346593. *(Scopus)*

5. M.G. Kovtun, V.Y. Kovtun, A.A. Okrimenko and S.A. Gnatyuk. «Search method development of birationally equivalent binary Edwards curves for binary Weierstrass curves from DSTU 4145-2002», in *Proc. PIC S&T*, Kharkov, Ukraine, Oct. 13-15, 2015. pp. 5-8. DOI: 10.1109/INFOCOMMST.2015.7357253. *(Scopus)*

6. М.Г. Булах, В.Ю. Ковтун, «Методы повышения производительности операции инвертирования в двоичном поле», *Безпека інформації*, том 20, № 1, с. 55-61, 2014.

7. М.Г. Ковтун, В.Ю. Ковтун, С.А. Гнатюк, О.М. Бердник, «Подходы к повы-шению производительности расширенного алгоритма Евклида для деления больших чисел

двойной точности на большие числа одинарной точности», *Безпека інформації*, том 21, № 1, с. 40-51, 2015.

8. М. Ковтун, «Применение кривых Эдвардса для защищенной реализации механизмов электронной цифровой подписи согласно ДСТУ 4145-2002», *Системи обробки інформації*, том. 5, №. 151, с. 130-137, 2017.

9. А.О. Охріменко, В.Ю. Ковтун, М.Г. Ковтун, С.П. Євсеєв, О.Г. Король та С.Ю. Ковтун. «Спосіб множення цілих чисел». Україна. Патент 111632, Бюл. 22. Листопад 25, 2016.

10. А.О. Охріменко, В.Ю. Ковтун, М.Г. Ковтун. «Спосіб приведення за модулем цілих чисел». Україна. Патент 118066, Бюл. 14. Липень 25, 2017.

11. А.О. Охріменко, В.Ю. Ковтун, М.Г. Ковтун, С.П. Євсеєв, О.Г. Король, Р.В. Грищук, Г.П. Коц. «Спосіб піднесення до квадрату цілих чисел». Україна. Патент 118065, Бюл.14. Липень 25, 2017.

12. М.Г. Ковтун, С.А. Гнатюк, В.И. Трофименко. «Ускоренное извлечение r-го корня в двоичном поле» в *Докл. Межд. науч.–практ. Конф. Информационные и телекоммуникационные технологии: образование, наука, практика*, Алматы, Казахстан, Декабрь, 2-4, 2015, с. 547-551.

13. М.Г. Булах, В.Ю. Ковтун. «Модифицированный алгоритм мультипликативного инвертирования в двоичном поле», *Науч.-практ. Конф. «Проблемы эксплуатации и защиты информационно-коммуникационных систем»,* 2014, Киев, Украина, с. 11.

14. М.Г. Ковтун, В.Ю. Ковтун. «Подходы к повышению производительности операции деления больших целых чисел, на основе расширенного алгоритма Евклида», *18 Між. Наук.-прак. Конф. «Проблеми та перспективи розвитку IT-індустрії»,* 2015, Харків, Україна, с. 31.

15. М.Г. Ковтун, С.А. Гнатюк. «Модифицированный расширенный алгоритм Евклида для деления больших целых чисел двойной точности на числа одинарной точности», *15 Між. Наук.-практ. Конф.:Політ. Сучасні проблеми науки,* 2015, Київ, Україна, с. 121.

16. М.Г. Ковтун, С.А. Гнатюк. «Ускоренное мультипликативное инвертирование в двоичном поле для ДСТУ 4145-2002», *12 Між. Наук.-техн. Конф.:АВІА,* 2015, Київ, Україна, с. 2.62-2.65.

17. М.Г. Ковтун, С.А. Гнатюк. «Классификация алгоритмов деления и приведения по модулю для целых чисел в криптографических приложениях», *5th International Scientific Conference: ITSEC*, Киев-2015, с. 56-57.

18. М.Г. Ковтун, В.Ю. Ковтун, С.А. Гнатюк. «Быстрое деление целых чисел для криптографических приложений», *Безопасность информации в информационно-телекоммуникационных системах: 17 Межд. Конф.*, Киев-2015, с. 12-13.

19. М.Г. Ковтун. «Модифицированный алгоритм Евклида для деления больших целых чисел двойной и одинарной точности», *Інформаційна безпека держави, суспільства та особистості,* Кировоград, 2015, с. 55.

20. М.Г. Ковтун, А.А. Охрименко. «Методы построения алгоритма приведения по фиксированному модулю неприводимого полинома», *18 Межд. Научн.-практ. Конф.: Безопасность информации в информационно-телекоммуникационных системах,* Киев-2016, с. 21.

АНОТАЦІЯ

Ковтун М.Г. Методи удосконалення арифметичних операцій у полях, кільцях та алгебраїчних кривих для криптографічних застосувань. – Рукопис**.**

Дисертація на здобуття наукового ступеня кандидата технічних наук за спеціальністю 05.13.21 – «Системи захисту інформації». –Національний авіаційний університет, Київ, 2018.

Дисертаційна робота присвячена вирішенню актуальної науково-технічної задачі підвищення швидкодії інформаційно-телекомунікаційних систем центрів сертифікації ключів Національної системи електронного цифрового підпису для ДСТУ 4145-2002, ECDSA (IEEE P1363-2000), RSA (IEEE P1363-2000) без фінансових витрат.

Підвищення швидкодії операції електронного цифрового підпису полягає в зменшенні обчислювальної складності алгоритмів криптографічних перетворень на основі розробки удосконалених методів та алгоритмів арифметичних операцій над числами, поліномами і точками еліптичних кривих (ЕК), в основному у зменшенні часу виконання трудомісткої операції скалярного множення. В роботі удосконалено метод ділення великих цілих чисел одинарної та подвійної точності на основі алгоритму ділення в стовпчик, що дозволив підвищити швидкодію генерації загальних параметрів криптосистеми RSA. Удосконалено метод здобуття n - го кореня, на прикладі кубічного кореня, який дозволив підвищити швидкодію пошуку бірaціонально еквівалентних кривих Едвардса до кривих Вейерштрасса з ДСТУ 4145-2002 та рекомендованих NIST FIPS 186-4 у двійковому полі. Удосконалено метод інвертування в двійковому полі, вперше розроблено метод побудови алгоритму приведення за фіксованим модулем (три-,п’ятичленна), що дозволив будувати алгоритми для різних цільових платформ, та удосконалено метод скалярного множення в групі точок еліптичної кривої, за рахунок використання бірaціонально еквівалентних кривих Едвардса при операції скалярного множення, що дозволило підвищити швидкодію при формуванні та перевірці ЕЦП згідно ДСТУ 4145-2002 та ECDSA. На основі запропонованих удосконалених методів було розроблено бібліотеку криптографічних примітивів «Cipher+».

Ключові слова: еліптична крива, двійкова крива Едвардса та Вейерштрасса, RSA, ECDSA, ДСТУ 4145-2002, ЕЦП, здобуття кубічного кореня, скалярне множення, інвертування, центр сертифікації ключів.

АННОТАЦИЯ

Ковтун М.Г. Методы совершенствования арифметических операций в полях, кольцах и алгебраических кривых для криптографических приложений. – Рукопись.

Диссертация на соискание научной степени кандидата технических наук по специальности 05.13.21 – «Системы защиты информации». – Национальный авиационный университет, Киев, 2018.

Диссертационная работа посвящена решению актуальной научно-технической задачи криптографических преобразований для электронной цифровой подписи (ЭЦП) в информационно-телекоммуникационных системах центров сертификации ключей (ЦСК), путем уменьшения вычислительной сложности алгоритмов криптографических операций на основе разработки усовершенствованных методов и алгоритмов арифметических преобразований над числами, полиномами и точками эллиптической кривой (ЭК) с уменьшенной вычислительной сложностью и противодействием к атакам на их реализацию за счет уменьшения времени формирования и проверки ЭЦП для ДСТУ 4145-2002, ECDSA, RSA без финансовых затрат.

Повышение быстродействия операции формирования и проверки ЭЦП, состоит в уменьшении вычислительной сложности и повышении быстродействия основной

операции скалярного умножения за счет: преобразований в промежуточных вычислениях базовой и произвольной точках эллиптической кривой; а также уменьшения вычислительной сложности арифметических операций над числами и полиномами. А именно деление, приведение по модулю и мультипликативное инвертирование, извлечение кубического корня (для перехода от кривых Вейерштрасса к кривым Эдвардса в двоичном поле). В работе усовершенствован метод деления «в столбик» больших целых чисел, который за счет упрощения операции сравнения больших чисел, учитывая двоичную длину чисел, проведения операций сдвига, сложения и вычитания по значимыми словам, позволил снизить вычислительную сложность обычного и расширенного алгоритма Евклида. Рассматривались два варианта: длинные больших целых чисел одинаковой двоичной длины - количество машинных слов делимого и делителя одинаковые; деления больших целых чисел, когда двоичная длина делимого в 2 раза превышает длину делителя. Метод позволил повысить быстродействие операции генерации ключей RSA на 7-14% с увеличением двоичной длины. Усовершенствован метод мультипликативного инвертирования на основе расширенного алгоритма Евклида в двоичном поле, который за счет использования информации о двоичной длине параметров уравнения Безу: отказ от вычисления степени полинома, а лишь уточнение, проводить сдвиги и сложение только по значимыми словам, позволил снизить вычислительную сложность при генерации ключей, наложении и проверке ЭЦП по алгоритмам ДСТУ 4145-2002 и ECDSA: увеличение быстродействия при формировании и проверке ЭЦП для ДСТУ 4145-2002 в 1.0011-0.0019 и 1.0027-0.0043 раз соответственно. Впервые разработан метод автоматизации приведения произвольного полинома по фиксированному модулю в двоичном поле, учитывающий степени членов для заданного неприводимого трехчлена и пятичленна, а также для разных целевых аппаратных платформ, который позволяет строить алгоритмы приведения по фиксированному модулю с меньшей вычислительной сложностью, по отношению с побитовым методом: увеличение быстродействия при формировании и проверке ЭЦП, согласно ДСТУ 4145-2002 в 6-9.4 7-9.4 раза соответственно. Усовершенствован метод получения n - мерного корня в поле $\boldsymbol{GF}(2^m)$, где m - нечетное, на примере кубического корня, который за счет разложения показателя степени с помощью аддитивной цепи на множители, позволяет уменьшить вычислительную сложность алгоритма поиска бирациональных эквивалентных кривых Эдвардса к кривым Вейерштрасса ДСТУ 4145-2002 и рекомендованных NIST FIPS 186-4: при отыскании бирационально эквивалентных кривых Эдвардса к кривым Вейерштрасса, увеличение быстродействия составило в 1.3-1.8 раз. Усовершенствован метод скалярного умножения в группе точек ЭК над полем $\boldsymbol{GF}(2^m)$, который за счет промежуточных вычислений на кривой Эдвардса, при $d_1 = d_2$ для поля 257 позволили повысить быстродействие формирования ЭЦП на 5-7% и проверки ЭЦП на 6-7% для кривых ДСТУ 4145-2002, в зависимости от процессора.

Методы реализованы в библиотеках «Шифр+v.2.1» системы криптографической защиты информации «Шифр-X.509».

Ключевые слова: эллиптическая кривая, двоичная кривая Эдвардса и Вейерштрасса, RSA, ECDSA, ДСТУ 4145-2002, ЭЦП, извлечение кубического корня, скалярное умножение, деление целых чисел, инвертирование, Национальная система ЭЦП, Центр сертификации ключей.

ABSTRACT

Kovtun M. Methods of implementation of high speed arithmetic operations in fields, rings and algebraic curves for cryptographic applications. – Manuscript**.**

Thesis for a Candidate of Technical Science degree in specialty 05.13.21 – «Information Security Systems». – National Aviation University, Kyiv, 2018.

Thesis is devoted to solving the actual scientific and technical problem of speed-up information and telecommunication systems of the certification authority in National Electronic Digital Signature System for DSTU 4145-2002, ECDSA, RSA without significant financial costs. Speed-up of digital signature operations are in reducing the time of a labor-intensive scalar multiplication operation. The method of dividing large integers of single and double precision based on the school division algorithm is improved. This allows to speed-up of common parameters generation for the RSA cryptosystem. Extracting of n -root method as an example of a cubic root is improved. This allows to speed-up of searching birationally equivalent Edwards curves to Weierstrass curves from DSTU 4145-2002 and recommended by NIST FIPS 186-3 in a binary field. Multiplicative inversion method in a binary field is improved. First proposed method of algorithm building for modular reducing by irreducible polynomial (trinomial, pentanomial) was developed. This allows the constructing of algorithms for various target platforms. Scalar multiplication method in the points group is improved by using birationally equivalent Edwards curves, which allowed to speed-up duration of creation and verification of digital signature in accordance with DSTU 4145-2002 and ECDSA. All proposed methods in dissertation thesis are implemented in library of cryptographic primitives "Cipher+".

Keywords: elliptic curve, Edwards and Weierstrass binary curves, RSA, ECDSA, DSTU 4145-2002, DS, cubic roots, scalar multiplication, inverting, National DS system, key certification center.