Міністерство освіти і науки України
Вінницький національний технічний університет

ТИТАРЧУК ЄВГЕНІЙ ОЛЕКСАНДРОВИЧ

УДК 004.056.55

ЗАХИСТ ПЕРСОНАЛЬНОЇ ІНФОРМАЦІЇ КОРИСТУВАЧІВ КОМП'ЮТЕРНИХ СИСТЕМ ПРИ ВИКОРИСТАННІ ПУБЛІЧНИХ ХМАРНИХ СЕРВІСІВ

Спеціальність 05.13.05 – «Комп’ютерні системи та компоненти»

АВТОРЕФЕРАТ
дисертації на здобуття наукового ступеня
кандидата технічних наук

Вінниця - 2018

Дисертацією є рукопис.

Робота виконана у Вінницькому національному технічному університеті, Міністерство освіти і науки України.

Науковий керівник: доктор технічних наук, професор,
Квєтний Роман Наумович,
Вінницький національний технічний університет,
завідувач кафедри автоматики та інформаційно-вимірювальної техніки.

Офіційні опоненти: доктор технічних наук, професор,
Вишнівський Віктор Вікторович,
Державний університет телекомунікацій,
завідувач кафедри інформаційної та кібернетичної безпеки

доктор технічних наук, старший
науковий співробітник,
Семенов Сергій Геннадійович,
Національний технічний університет «Харківський політехнічний інститут»,
завідувач кафедри обчислювальної техніки та програмування

Захист відбудеться «22» червня 2018 р. о $14^{\underline{00}}$ годині на засіданні спеціалізованої вченої ради Д 05.052.01 у Вінницькому національному технічному університеті за адресою: 21021, Україна, м. Вінниця, вул. Хмельницьке шосе, 95, ГНК, ауд. 210.

З дисертацією можна ознайомитись у бібліотеці Вінницького національного технічного університету за адресою: 21021, Україна, м. Вінниця, вул. Хмельницьке шосе, 95, ГНК.

Автореферат розісланий « » травня 2018 р.

Учений секретар
спеціалізованої вченої ради С. М. Захарченко

ЗАГАЛЬНА ХАРАКТЕРИСТИКА РОБОТИ

Обґрунтування вибору теми дослідження. Розповсюдження мереж з високою потужністю, низька вартість комп'ютерів і пристроїв зберігання даних, а також широке впровадження віртуалізації, сервіс-орієнтованої архітектури, привели до значного розвитку хмарних сервісів, що дають можливість користувачам виконувати обчислення та зберігати дані на віддалених інтернет-серверах. Сучасні комп'ютерні системи все частіше містять у своєму складі відразу декілька компонентів представлених публічними чи приватними хмарними сервісами. Використання компонентів, що представлені сторонніми хмарними сервісами, дозволяє значно спростити розробку комп'ютерної системи та покращити її характеристики за рахунок гнучкого масштабування обчислювальних ресурсів, збору статистики використання, вибір місця фізичного розташування серверів, тощо. Проте в цьому проявляється головний недолік хмарних сервісів – приватна інформація користувача фактично стає доступна третій стороні – провайдеру хмарного рішення, крім цього, данні можуть стати вразливими під час їх передачі каналами зв'язку, обробці та зберіганні.

Задачам забезпечення інформаційної безпеки хмарних сервісів комп'ютерних обчислень, а також засобам захисту приватної інформації користувачів, зокрема, застосуванню гомоморфного шифрування, приділена велика увага в роботах Дж. Риза, П. Фингара, В. Романченко, Крейга Джентрі

Не дивлячись на значну кількість серйозних наукових досліджень, теоретичних робіт і численних публікацій, задача захисту приватної інформації користувачів на сучасному етапі розвитку науково-дослідної бази стосується в основному проблем захисту від доступу до конфіденційної інформації з боку осіб, що є сторонніми до обчислювального процесу, чи її зберігання. Проте, залишається недослідженим механізм захисту інформації користувачів від неправомірного доступу до неї зі сторони провайдеру хмарного сервісу, а саме, не виявлені особливості застосування гібридної криптографії для захисту інформації під час її зберігання у хмарному сховищі і, особливо, захист інформації під час виконання обчислень на стороні хмарного сервісу. Більшість сучасних хмарних сервісів створені саме для обробки інформації. Тому, є актуальною не тільки задача аналізу недоліків існуючих інформаційних систем та побудови нових, що організовують обчислення у публічному хмарному сервісі, але й створення нових методів шифрування, що дозволять реалізувати захист даних при виконанні обчислень у таких сервісах з високою ефективністю.

Зв'язок роботи з науковими програмами, планами, темами. Робота виконувалася відповідно до Указу Президента України «Про Положення про технічний захист інформації в Україні» (у редакції від 11.04.2008) та згідно положенню «Захист інформації на об'єктах інформаційної діяльності. Створення комплексу технічного захисту інформації.» Державної служби спеціального зв'язку та захисту інформації України.

Основний зміст роботи складають наукові дослідження, що були проведені на кафедрі автоматики та інформаційно-вимірювальної техніки Вінницького національного технічного університету в 2012-2017 роках.

Мета і завдання дослідження. Метою роботи є підвищення ефективності захисту інформації в комп`ютерних системах, що використовують у своєму складі публічні хмарні сервіси, на основі розробки та впровадження нових методів і засобів шифрування.

Основними задачами дослідження є:

1. Аналіз задач, пов'язаних з використанням публічних хмарних технологій у складі комп'ютерної системи: огляд існуючих моделей та стратегій розгортання хмарних сервісів; аналіз сучасних методів захисту інформації під час її передавання, зберігання та оброблювання у публічному хмарному сервісі.
2. Розроблення методу захисту інформації користувачів у комп'ютерній системі, що містить у своєму складі публічні хмарні сервіси комп'ютерних обчислень, на основі частково гомоморфного алгоритму шифрування.
3. Визначення критерію ефективності методу частково гомоморфного шифрування, що орієнтований на використання у складі комп'ютерної системи, один або декілька компонентів якої представлені публічними хмарними сервісами.
4. Розроблення теоретично обґрунтованої модифікації методу криптографії на основі еліптичних кривих з метою надання їй гомоморфних властивостей відносно операції додавання.
5. Розроблення математичної моделі комп'ютерної системи з обмеженням доступу до інформації, що в ній обробляється, зі сторони провайдеру хмарного сервісу з використанням частково гомоморфного алгоритму шифрування на основі еліптичних кривих.
6. Реалізація розробленого алгоритму частково гомоморфного шифрування на основі еліптичних кривих з використанням обчислювальних потужностей технічних засобів.
7. Розроблення алгоритмічного забезпечення та програмного моделювального комплексу.
8. Забезпечення практичного впровадження результатів роботи.

Об'єктом дослідження є процес оброблення даних публічним хмарним сервісом у складі комп'ютерної системи.

Предметом дослідження є методи та засоби побудови системи для реалізації анонімності користувачів у хмарному сервісі комп'ютерних обчислень.

Методи дослідження. В роботі використано методи абстрактної алгебри для визначення точок еліптичної кривої, системного аналізу схем частково гомоморфного шифрування для визначення їх переваг та недоліків, комп'ютерне моделювання та експериментальне дослідження описуваних схем шифрування для аналізу та перевірки достовірності отриманих теоретичних результатів. Реалізації алгоритму частково гомоморфного шифрування виконувалося за допомогою середовища програмування Microsoft Visual Studio 2015. Оброблення експериментальних даних виконувалося за допомогою програми Microsoft Excel пакету MS Office.

Наукова новизна отриманих результатів полягає в подальшому розвитку теоретичних засад побудови захищених інформаційних комп'ютерних систем, що виконують обчислення у публічних хмарних сервісах, які дозволили знизити ризик втрати персональної інформації користувачів даних інформаційних систем.

− Запропоновано та розроблено нову математичну модель взаємодії компонентів комп'ютерної системи, яка на відміну від існуючих, використовує метод частково гомоморфного шифрування на основі еліптичних кривих, що дозволяє захистити інформацію користувача від несанкціонованого доступу до неї зі сторони провайдера хмарного сервісу, враховуючи необхідність її обробки.

− Запропоновано новий метод частково гомоморфного шифрування відносно операції додавання, що на відміну від існуючих аналогів використовує математичний апарат еліптичних кривих, який, при однаковій криптографічній стійкості запропонованого алгоритму робить його швидшим, ніж аналогічні алгоритми відносно часу виконання однакової кількості операцій гомоморфного додавання, а його довжину ключа – меншою.

− Запропоновано метод кодування чисел точками еліптичної кривої з попередньою побудовою таблиці відповідності, що на відміну від існуючих аналогів включає етап попередньої генерації n-точок еліптичної кривої (де n – максимальне число, яке необхідно декодувати), що дозволяє виконувати операцію декодування числа, при відомому його максимальному розмірі.

Практичне значення отриманих результатів. На основі розроблених моделей та методів створено алгоритмічне та програмне забезпечення інформаційної системи забезпечення анонімності користувачів з використанням частково гомоморфного шифрування на еліптичних кривих.

− Розроблено методику інформаційного захисту комп'ютерних систем, що використовують публічні хмарні сервіси, на основі алгоритму частково гомоморфного шифрування.

− На основі запропонованих алгоритмів та моделей розроблено програмний модуль, що реалізує схему частково гомоморфного шифрування відносно операції додавання на основі еліптичних кривих.

− Реалізовано програмне забезпечення, що реалізує ядро системи деперсоналізації користувачів при використанні інформаційної системи, що виконує обчислення на стороні хмарного сервісу публічного типу.

− Результати проведених досліджень впроваджено в інтелектуальні програмні засоби забезпечення анонімності на основі алгоритму частково гомоморфного шифрування користувачів комп'ютерної системи «Liquidity» ТОВ "СКАЙСОФТТЕК" (Код реєстрації 40524859, м.Вінниця) для збору анонімних відгуків та параметрів використання мобільного додатку. Акт впровадження №5 від 14 грудня 2017 року.

Особистий внесок здобувача у роботах, які виконані у співавторстві, полягає в наступному: [1] – виконано аналіз основних напрямів атак на публічний хмарний сервіс; [2] – розроблено алгоритм та програмний засіб, що його реалізує для шифрування інформації користувача, при використанні хмарного сервісу

DropBox; [3] – розроблено математичну модель протоколу обміну ключами серед груп користувачів без використання центрального серверу; [4] – розроблено протокол взаємодії елементів системи голосування, що дозволяє інформаційно захистити персональні дані користувачів; [5] – розроблено математичну модель алгоритму шифрування на основі еліптичних кривих та модель деперсоналізації користувачів з використанням алгоритму частково гомоморфного шифрування на основі еліптичних кривих; [6] – проведено аналіз криптографічної стійкості алгоритму частково гомоморфного шифрування на еліптичних кривих; [7] – розроблено протокол взаємодії елементів фінансової системи, що дозволяє захистити персональні дані користувачів.

Апробація результатів дисертації. Основні результати та положення дисертаційної роботи доповідались та обговорювались на міжнародних наукових конференціях: всеукраїнському конкурсі наукових робіт з напрямку «Інформатика та кібернетика», де робота була нагороджена дипломом переможця ІІІ ступеня. – м. Вінниця, 2014; XLI, XLII, XLIII, XLIV регіональні науково-технічні конференції професорсько-викладацького складу, співробітників та студентів ВНТУ з участю працівників науково-дослідних організацій та інженерно-технічних працівників підприємств м. Вінниці та області. – м. Вінниця, 2013, 2014, 2015, 2016; І Міжнародна конференція Infocom Advanced Solution 2015 присвячена 70-річчю кафедри автоматики та управління в технічних системах НТУУ “КПІ”. – м. Київ, 2015; міжнародна науково-практична Інтернет-конференція. Наукові дослідження і їх практичне застосування. Сучасний стан та шляхи розвитку. – 2014; IX Міжнародна науково-практична конференція «Інтернет-Освіта-Наука. ІОН2014». – м. Вінниця, 2014; XII Міжнародна конференція «Контроль і управління в складних системах. КУСС 2014». – м. Вінниця, 2014; XIII міжнародна конференція «Контроль і управління в складних системах. КУСС-2016». – м. Вінниця, 2016; IV Міжнародна наукова конференція «Вимірювання, контроль та діагностика в технічних системах». – м. Вінниця, 2017.

Публікації. За результатами виконаних досліджень опубліковано 14 наукових праць: 4 статті у виданнях, що входять до переліку фахових видань України, 1 стаття у журналі, що входить до наукометричної бази Scopus, 2 статі у інших виданнях, що не входять до переліку ВАК, 7 тез доповідей.

Структура та обсяг дисертаційної роботи. Дисертаційна робота складається зі вступу, чотирьох розділів, висновків, списку використаних джерел та додатків. Робота містить 108 сторінок основного друкованого тексту, 29 рисунків, 9 таблиць, список використаних джерел із 110 найменувань та сім додатків. Загальний обсяг роботи – 162 сторінки.

ОСНОВНИЙ ЗМІСТ РОБОТИ

У **вступі** обґрунтовано актуальність теми, зазначено зв’язок з науковими програмами, сформульовано мету та завдання дослідження, наведено наукову новизну і практичну цінність отриманих результатів, подано відомості щодо апробації роботи та публікацій, особистого внеску здобувача.

У **першому розділі** проведено аналіз існуючих моделей хмарних сервісів та способи їх розгортання, проаналізовано загрози безпеки, що виникають при їх

використанні та найбільш поширені методу захисту інформації в комп'ютерних системах та мережах під час роботи з публічними хмарними серверами.

Проведено аналіз задач, пов'язаних з використанням публічних хмарних технологій комп'ютерних обчислень. Виконано аналіз існуючих моделей та стратегій розгортання хмарних сервісів, сучасних методів захисту інформації, при її передачі, зберіганні та обробці у публічному хмарному сервісі, при його використанні у складі комп'ютерної системі.

Наразі найбільш розповсюдженим методом інформаційного захисту від багатьох видів атак на хмарні сервіси є використання симетричних та асиметричних алгоритмів шифрування інформації для забезпечення цілісності та конфіденційності інформації, а також сертифікатів для визначення автентичності комп'ютерних систем що беруть участь у обміні інформацію. Проте для виконання обчислень інформація розшифровується і стає доступною для несанкціонованого доступу. Зараз лише з'являються методи та алгоритми орієнтовані на захист інформації підчас обчислень у хмарній системі. Універсальними методами захисту є методи гомоморфного шифрування, проте їх продуктивність надзвичайно низька, що робить актуальним розробку більш вузько орієнтованих моделей з вищою продуктивністю.

Під час огляду існуючих рішень виявлено, що сучасні хмарні сервіси, які обробляють дані користувачів, містять частину даних, що обробляється у відкритому вигляді, а це робить їх уразливими до читання/копіювання.

У **другому розділі** запропоновано формалізацію компонентів найпростішої комп'ютерної системи, що використовує хмарний сервіс, у вигляді трьох основних компонентів: клієнтська програма – компонент комп'ютерної системи, що може бути представлений додатком, що використовує кінцевий користувач системи. Особливістю клієнтської програми у системі є те, що вона взаємодіє з користувачем, надає дані для обробки, проте потребує ізоляції від інших інформаційних потоків системи; локальний сервер – сервер, що розгорнутий на обчислювальних ресурсах організації, яка володіє комп'ютерною системою. Локальний сервер приймає участь у обміні інформацією з користувачем та має вільний доступ до усіх даних усіх користувачів, які вони надають системі безпосередньо, або вони збираються клієнтським програмним забезпеченням. Зазвичай локальний сервер містить власну базу, в якій міститься інформація що дозволяє ідентифікувати користувачів системи; хмарний сервіс – віддалений сервер, що дозволяє виконати певну операцію (F), що складається з окремих підзадач (f). Зазвичай хмарний сервер реалізовує одну з функцій системи, що потребує значних обчислювальних ресурсів, гнучкого масштабування або міжрегіонального розподілення. В залежності від специфіки можливостей, яку надає комп'ютерна система, хмарний сервіс може взаємодіяти з клієнтським додатком безпосередньо або через локальний сервер. Хмарний сервіс не має прямого доступу до інформації про окремих користувачів, проте опрацьовує інформацію (X) яка їм належить:

$$F(X) = f_1(X) \cup f_2(X) \cup \ldots \cup f_n(X)$$

Для захисту інформації за допомогою методів частково гомоморфного шифрування необхідно обмежити кількість арифметичних операцій кожної підзадачі ($f \to f'$) та загальну функцію ($F \to F'$) до того набору, який підтримує обраний метод гомоморфного шифрування без необхідності додаткового розшифрування. Кожен окремий набір вхідних даних повинен бути зашифрований з використанням різних сеансових ключів шифрування (k):

$$X_i' = E(X_i + k_i),$$

Тоді, для методу шифрування гомоморфного відносно операції додавання:

$$F'(X') = f_1'(X_1') + f_2'(X_2') + \cdots + f_n'(X_n')$$

Після отримання результатів, їх необхідно розшифрувати, та виконати зворотне відображення $F' \to F$.

Значним недоліком такого методу є висока обчислювальна складність, або взагалі неможливість перетворення функції яку виконує хмарний сервіс. Крім того, в більшості випадків, метод відображення функції F буде представлений різними алгоритмами для різних комп'ютерних систем.

Для покращення ефективності створюваного методу захисту інформації було розроблено алгоритм шифрування, що дає змогу виконувати арифметичну дію додавання між зашифрованими цілими числами швидше за аналоги.

Головними параметрами системи шифрування основаній на еліптичній кривій, є параметри, що визначають саму еліптичну криву: велике просте число (p) – модуль поля еліптичної кривої, коефіцієнти кривої (a, b), а також, параметри точки генератора (G), що належить еліптичній кривій: її координати (G_x, G_y) та порядок (r) – велике просте число.

Отже, відкритими параметрами системи (відомими всім учасникам) є крива $E_p(a, b)$, її параметри, кількість точок кривої (N, фактично, модуль поля утвореного точками кривої) та точка-генератор, що належить цій кривій – G.

Нехай необхідно безпечно додати набір цілих чисел $(a_0, a_1, \dots, a_n)$. Перед шифруванням необхідно виконати кодування усіх чисел $(a_0, a_1, \dots, a_n)$, які необхідно гомоморфно додати, точками еліптичної кривої E_p $(A_0, A_1, \dots, A_n)$. Пропонується виконати кодування числа шляхом його множення на точку-генератор еліптичної кривої.

$$A_i = a_i G$$

Всі операції відбуваються у полі еліптичної кривої E_p, тому після кожної дії необхідно виконати операцію модуля по числу p. Для візуального спрощення формул ця дія пропущена.

Після чого необхідно згенерувати закритий ключ шифрування системи – випадкове, ціле число n, таке що $n < p$, де p – модуль поля еліптичної кривої. На основі закритого ключа генерується та опубліковується відкритий ключ шифрування (P) системи:

$$P = nG$$

Отримавши публічний ключ шифрування, кожна з сторін генерує закритий сеансовий ключ $(k_i, k_i < p)$ для кожного числа, після чого шифрує закодовані

числа у вигляді пари точок – власне зашифрованого числа та підказки необхідної для його розшифрування:

$$A'_i = (k_i G, A_i + k_i P) \bmod p$$

Таким чином, шифротекст одного й того самого числа буде різним при повторному шифруванні.

Для надання методу шифрування гомоморфних рис відносно операції додавання зашифрованих точок, необхідно виконувати додавання наступним чином – додавати окремо праві та ліві частини:

$$\sum_{i=0}^{n} A'_i = (\sum_{i=0}^{n} k_i G\,, \sum_{i=0}^{n} (A_i + k_i P))$$

Для розшифрування результату необхідно помножити першу частину зашифрованого результату на приватний ключ шифрування та відняти її від другої:

$$\sum_{i=0}^{n} A_i = \sum_{i=0}^{n} (A_i + k_i P) - n \sum_{i=0}^{n} k_i G = \sum_{i=0}^{n} A_i + \sum_{i=0}^{n} k_i P - \sum_{i=0}^{n} k_i P = \sum_{i=0}^{n} A_i$$

Отриманий результат являє собою число, закодоване точкою еліптичної кривої E, що є сумою (S) точок, якими було закодовано вхідний набір чисел (a_i).

$$S = \sum_{i=0}^{n} A_i = \sum_{i=0}^{n} a_i G$$

Для декодування цієї суми необхідно згенерувати табличну функцію, відносно перших n_{max} точок еліптичної кривої, де n_{max} – це максимальне число, яке може бути декодовано.

$$F(P) = a$$

Таблиця 1 – Таблична функція перших n точок еліптичної кривої

№ п/п	Точка кривої
1	$1 \cdot G$
2	$2 \cdot G$
…	
i	$i \cdot G$
…	
n_{max}	$n_{max} \cdot G$

Генерація точок необхідна тільки один раз, при використанні нової кривої E, проте може зайняти значний період часу.

Збереження ж усього обсягу точок може потребувати значного обсягу пам’яті. У роботі було розраховано обсяг пам’яті, необхідний для збереження числа точок N_P, що відповідає беззнаковому цілому числу розрядністю у чотири байти – 2^{32}. Для прикладу використаємо еліптичну криву P-256. Обсяг пам’яті, необхідної для збереження однієї координати точки даної еліптичної кривої V_p дорівнює 256 бітам. Тому мінімальна кількість Gb пам'яті необхідної для збереження цієї кількості точок дорівнює:

$$V = \frac{2 \cdot V_p \cdot N_P}{2^3 \cdot 2^{30}} = \frac{2 \cdot 256 \cdot 2^{32}}{2^3 \cdot 2^{30}} = 256 \text{ (Gb)}$$

Даний обсяг пам’яті є значним, проте співвідносним з обсягами баз даних сучасних застосунків, тому можна зробити висновок, що метод декодування точок придатний до реалізації на більшості з сучасних платформ.

У роботі було виконано порівняння модифікованого методу шифрування з початковим. Задача дискретного логарифмування на еліптичній кривій (elliptic curve discrete logarithm problem, ECDLP) E(F_p) з основою $q \in E(F_p)$ полягає у знаходженні для даного $p \in E(F_p)$ такого цілого числа x, що $xq = p$ (якщо воно існує).

Найкращими з відомих на сьогоднішній день алгоритмів рішення ECDLP є метод «Великих та малих кроків» а також ρ-метод Поларда. Перевагою останнього є менший обсяг використання пам'яті та можливість розподілених обчислень. Алгоритм Поларда має складність $O(\sqrt{p})$ операцій складання в групі $\langle E(F_p, +)\rangle$.

Для методу шифрування на основі еліптичних кривих, кількість операцій, що необхідно виконати для розкриття приватного ключу шифрування:

$$r = \sqrt{n} + 1$$

де, n – порядок поля.

Встановлено, що криптостійкість частково гомоморфного алгоритму шифрування зменшується на кількість операцій гомоморфного додавання (m) відносно вихідного алгоритму ECDH, проте, так як порядок m значно менший n це не призводить до значної втрати криптографічної стійкості:

$$r \leq \sqrt{n} + 1 - m$$

Визначемо ефективність алгоритму частково гомоморфного шифрування. Пропонується визначати на основі двох незалежних параметрів – кількості арифметичних операцій, що виконується алгоритмом за одиницю часу (k_{op}) та часом, витраченим на шифрування та розшифрування даних (t_s):

$$t_s = t_{enc} + t_{dec}$$

У **третьому розділі** розроблено загальну методику для побудови комп’ютерних систем, що використовують публічні хмарні сервіси, з захистом приватної інфомації користувача від провайдерів хмарного рішення, побудованому на основі алгоритму частково гомоморфного шифрування. Дана методика включає наступні етапи:

1. Формалізація задачі обчислення – на цьому етапі виводиться основна математична модель обчислень, які необхідно здійснити для досягнення мети.
2. Перетворення моделі – на цьому етапі необхідно виділити ресурсовитратну частину обчислень яку можливо перенести в публічний хмарний сервіс. Також необхідно виконати відображення підзадач, які виконуватиме хмарний сервіс з метою обмеження кількості арифметичних операцій до тої, яку підтримує обраний алгоритм гомоморфного шифрування.
3. Виділення головних структурних елементів – суб’єктів, що беруть участь у обчислювальному процесі, або є складовими комп’ютерної системи. При цьому визначається рівень доступності інформації якою оперує комп’ютерна система для кожного з суб’єктів.

4. Створення протоколу системи – завершальний етап проектування моделі обчислень. На цьому етапі визначається послідовність передачі інформації, ключів шифрування, процесів шифрування та розшифрування інформації.

Узагальнена діаграма використання системи з процесами обміну та шифрування інформації показана на рисунку:

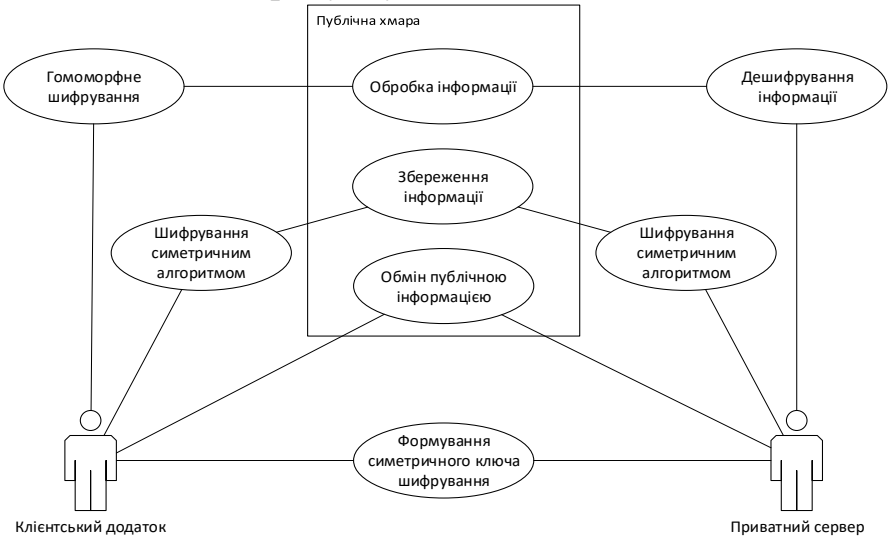

Рисунок 1 - Діаграма використання системи

Структурна блок-схема системи, що складається з трьох основних компонентів (головного серверу, хмарного сервісу, клієнтського додатку), має наступний вигляд:

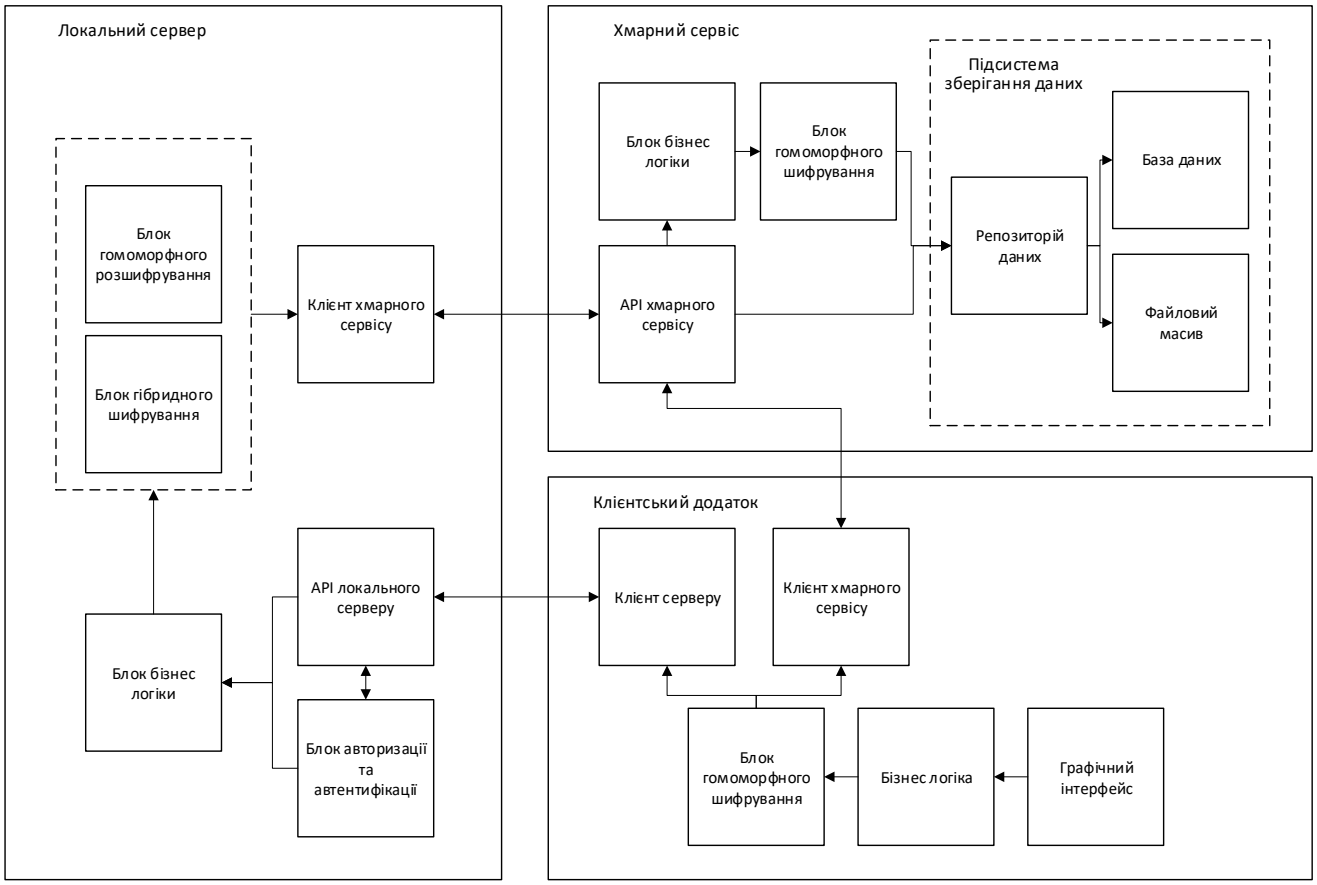

Рисунок 2 - Структурна схема комп'ютерної системи з хмарним сервісом

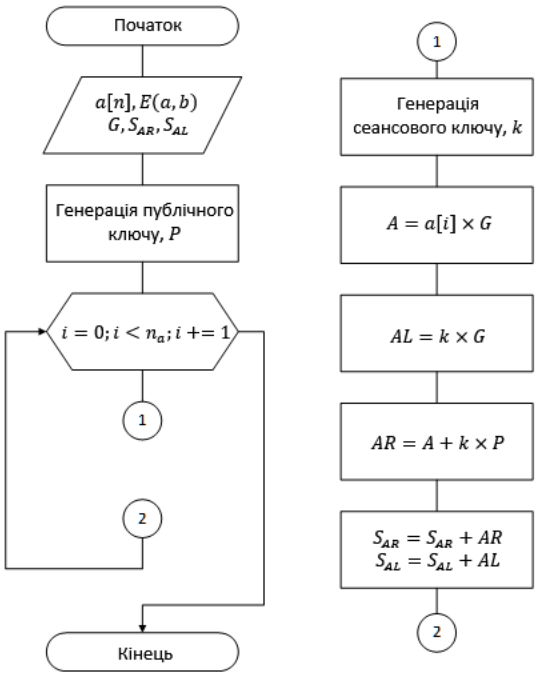

Рисунок 3 - Блок-схема алгоритму гомоморфного додавання точок

Для гомоморфного шифрування та додавання масиву чисел $a[n]$, необхідно визначити параметри еліптичної кривої, її точку генератор та згенерувати публічний ключ системи.

Після чого для кожної точки:

1. Згенерувати сеансовий ключ шифрування k.
2. Закодувати число з масиву (a) точкою еліптичної кривої (A). Для кодування числа точкою еліптичної кривої, його необхідно помножити на точку-генератор цієї кривої. Операція кодування є відносно простою та не вимагає значних затрат часу
3. Обрахувати підказку для розшифрування числа, помноживши сеансовий ключ шифрування на точку генератор еліптичної кривої.
4. Сформувати підказку для розшифрування (AL)
5. Зашифрувати точку за допомогою сеансового та публічного ключів (AR).
6. Підсумувати підказку та зашифровану точку з обрахованими сумами на попередніх кроках (S_{AR}, S_{AL}).

Для розшифрування точки еліптичної прямої необхідно помножити підказку для розшифрування результату на приватний ключ шифрування та відняти її від зашифрованого числа

Одержана точка (A_S) є закодованою сумою чисел, що були гомоморфно додані на попередньому етапі. Для отримання суми її необхідно декодувати.

В загальному випадку задача декодування точки є складною задачею, адже вимагає знаходження дискретного логарифму у області точок еліптичної кривої. Проте знаючи, що обчислена точка лежить на проміжку від 0 до певного, відносно невеликого цілого числа n_{max} $(a \in \{0 \dots n_{max}\})$, можна використати попередньо згенеровано дискретну функцію, яка повертає значення числа на основі точки еліптичної кривої.

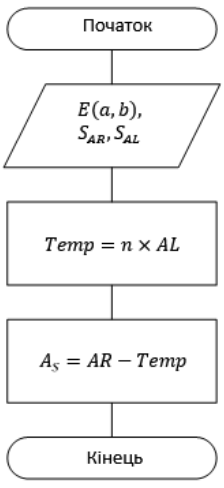

Рисунок 4 - Блок-схема алгоритму розшифрування

Дані для дискретної функції було згенеровано методом фіксованої точки, застосованого відносно числа, що необхідно закодувати. Час генерації точок алгоритмом додавання точки генератора показаний на рисунку 5 (.NET Framework 4.5.2, Windows 10, Intel i5-6600, 16Gb RAM, один потік).

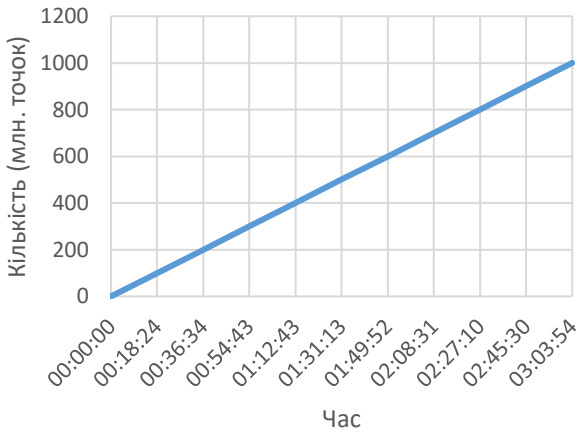

Рисунок 5 - Генерація точок шляхом циклічного додавання точки-генератора

При генерації точок є доцільним використати хеш-таблицю з заданим розміром. При цьому, у якості хеш функції $H(x)$ пропонується взяти суму координат точки по модулю кількості згенерованих точок та ланцюжковий метод вирішення колізій.

Порівняно з іншими, такий метод вирішення колізій дасть стабільний результат вставки ($O(1)$) навіть при значному та нерівномірному заповненні таблиці за рахунок часу операції зчитування. У найгіршому випадку кількість операцій зчитування буде дорівнювати $O(n)$, проте час зчитування не є таким критичним для даної задачі.

$$H(A) = \left(A_x + A_y\right) \bmod n_{max}$$

Таким чином, структура даних для зберігання точок матиме наступний вигляд:

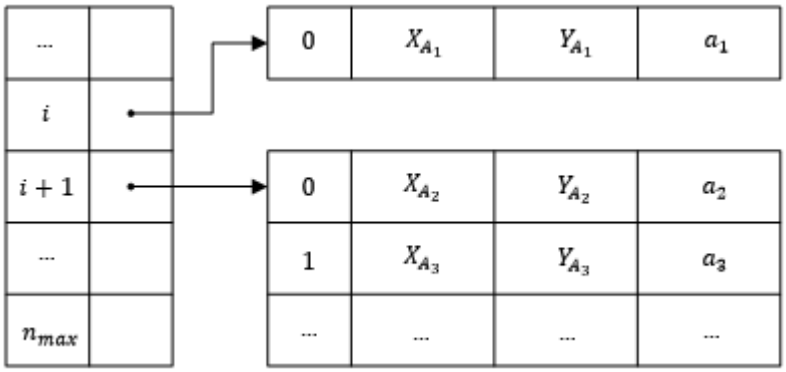

Рисунок 6 - Структура хеш-таблиці для збереження точок

Значний обсяг згенерованих точок робить неможливим розміщення усієї інформації у оперативній пам'яті комп'ютерної системи. Тому для оптимізації процесу зчитування пропонується розділити список хешів точок та власне самі точки. При цьому файл з хешами міститиме індекси координат точок в іншому файлі.

Для оптимізації розміру файлів пропонується наступна їх структура:

1. Файл з хеш-таблицею містить послідовність хеш-кодів точки $H(P)$ (4 байти), кількість точок в яких співпадає даний хеш-код N (4 байти) та послідовність індексів цих точок у файлі точок I (4 байти).

Загальна структура файлу показана на рисунку 7:

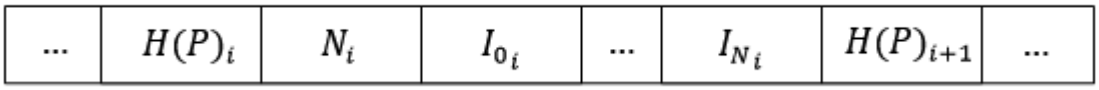

Рисунок 7 - Структура файлу хеш-кодів згенерованих точок

2. Файл з координатами точок еліптичної кривої містить послідовність координат X та Y відповідних точок.

Загальна структура файлу показана на рисунку 3.10.

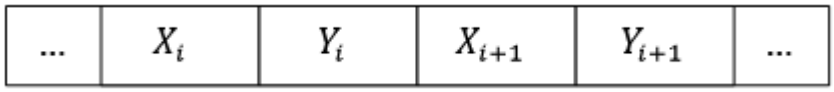

Рисунок 8 - Структура файлу з точками еліптичної кривої

Запропонована структура файлів дозволяє багато поточний режим пошуку індексу шуканої точки. Оптимальною є кількість потоків, що наближається кількістю до кількості обчислювальних ядер процесору комп'ютерної системи. Проте це вимагає збереження зсувів хеш-кодів, з яких почне пошук кожен новий потік відносно початку файлу.

Таблиця 2 - Розкладання на множники за допомогою методу решітки в полі чисел загального

Key size (bit)	MIPS-year
150	$3.8 \cdot 10^{10}$
205	$7.1 \cdot 10^{18}$
234	$1.6 \cdot 10^{28}$

Безпека, що забезпечується криптографічним підходом на основі еліптичних кривих залежить від того, наскільки важкою для вирішення виявляється задача, визначення n за відомими nP та P. Цю задачу зазвичай називають проблемою логарифмування на еліптичній кривій. Найбільш швидким з відомих на сьогодні методів логарифмування на еліптичній кривій є так званий ρ-метод Полларда. Час необхідний для розкриття приватного ключа шифрування виражений у MIPS-роках вказано у таблиці 2.

Метод Пейє (як і метод RSA) оснований на складності факторизації складеного числа, що є добутком двох простих чисел. Для вирішення цієї задачі можна використати метод розкладання на прості множники за допомогою решітки у полі чисел загального вигляду. Час необхідний для розкриття приватного ключа методу Пейє наведено у таблиці 3.

Таблиця 3 - Логарифмування на еліптичній кривій за допомогою ρ-метода Полларда

Key size (bit)	MIPS-year
512	$3 \cdot 10^{4}$
1024	$3 \cdot 10^{11}$
1280	$1 \cdot 10^{14}$
1536	$3 \cdot 10^{16}$
2048	$3 \cdot 10^{20}$

Для порівняння швидкодії, оберемо довжини ключів з співвідносною криптостійкістю: 2048 для алгоритму Пейє, та 256 для алгоритму на еліптичних кривих. Параметри кривої відповідають кривій P-256 (еліптичні криві рекомендовані NIST). Параметри кривої вказані у таблиці 4.

Таблиця 4 - Параметри кривої P-256

p	627710173538668076383578942320766641608390870039032496127 9
N	627710173538668076383578942317605901376719477318284228408 1
a	-3
b	64210519e59c80e70fa7e9ab72243049feb8deecc146b9b1
G_x	188da80eb03090f67cbf20eb43a18800f4ff0afd82ff1012
G_y	07192b95ffc8da78631011ed6b24cdd573f977a11e794811

Визначення швидкодії алгоритмів шифрування проведено двома різними способами. Перший спосіб дозволив визначати кількість часу, що необхідний для виконання певної кількості операцій гомоморфного додавання. Другий спосіб дозволяє визначати кількість тактів комп`ютерної системи, які необхідні для виконання цієї кількості операцій блоку даних. Перший спосіб використовує клас мови C# „Stopwatch”, що являє собою обгортку довкола системних функцій „QueryPerformanceFrequency” та „QueryPerformanceCounter”, що використовують HPET (High Precision Event Timer, таймер подій високої точності). Функції даного класу дозволяють визначати значення часу витраченого на виконання операції гомоморфного додавання.

Час виконання та кількості виконаних операцій додавання подано на рисунку 9 (C#, .NET Framework 4.5, математична бібліотека Mpir.NET 3.2, CPU Intel i5 6600, 16Gb RAM, 1 thread).

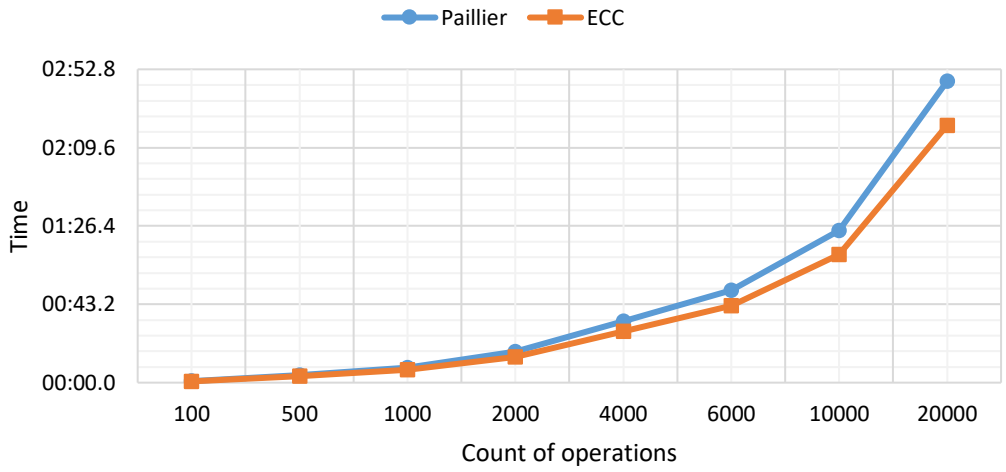

Рисунок 9 - Залежність часу виконання від кількості виконаних операцій додавання

Перевага алгоритму на еліптичних кривих складає ~1.4 секунди на 1000 операцій додавання.

Другий спосіб використовує асемблерну інструкцію «rdtsc», що визначає значення лічильнику часу. По цій причині переривання були відключені. Крім того використання цього способу не залежить від швидкості роботи мікропроцесору комп`ютерної системи. Та ж сама кількість тактів буде використовуватись для шифрування на мікропроцесорах з різною тактовою частотою.

Кількість тактів, необхідна для виконання 20000 операцій наведена у таблиці 5.

Таблиця 5 - Кількість тактів витрачених на гомоморфне додавання

	Кількість тактів	
Кількість операцій	ECC	Пейє
100	2144509398	2944547932
500	10607415320	14616484832
4000	85480277210	117032076186
20000	433757808476	586015919140

Коефіцієнт k_{op} для кожного з алгоритмів наведено у таблиці 6:

Таблиця 6 - Коефіцієнт ефективності алгоритмів частково гомоморфного шифрування

Алгоритм	k_{op} (сек)	k_{op} (тактів)
ECC	0.00653795	21687890
Пейє	0.00884065	29300795

Час розшифрування результату наведено у таблиці 7:

Таблиця 7 - Час розшифрування

Алгоритм	Час розшифрування (сек)	Час розшифрування (тактів)
ECC	0.003	6834558
Paillier	0.008	32391680

Загальній коефіцієнт ефективності з формули 2.32 для 100 операцій гомоморфного додавання:

$$t_{ECC} = t_{enc} + t_{dec} = 2044509398 + 6834558 = 2051343956$$

$$t_{\text{Paillier}} = t_{enc} + t_{dec} = 2944547932 + 32391680 = 2976939612$$

Порівняємо результати:

$$\Delta = \frac{t_{\text{Paillier}}}{t_{ECC}} = \frac{2976939612}{2151343956} = 1.38$$

Отже, алгоритм оснований на еліптичних кривих швидший на 38%.

У **четвертому розділі** було розглянуто питання практичного використання методики захисту даних користувача при використанні публічних хмарних сервісів

Представлено нову модель хмарної системи електронного голосування, що дасть користувачам системи можливість впевнитися у вірності зарахування їх вибору і при цьому забезпечить його таємність.

Система електронного голосування складається з трьох частин: керуючого модулю, модулю голосування, клієнтського модулю. UML діаграму прецедентів системи показано на рисунку:

Рисунок 10 - Діаграма прецедентів системи електронного голосування

Керуючий модуль – це приватний сервер що відповідає за авторизацію користувачів, зберігає у відкритому вигляді ваги варіантів для голосування та за отримання, розшифрування і обробку результатів голосування.

Модуль голосування – це публічний хмарний сервіс на якому зберігається поточний стан виборчої системи, до нього звертаються клієнтські модулі виборців для реєстрації свого вибору.

Клієнтський модуль – це додаток, що використовує виборець для авторизації у системі та процесу голосування.

При голосуванні клієнтська програма користувача передає серверу для голосування отриманий при авторизації ключ доступу. Сервер для голосування перевіряє його коректність

Після авторизації у керуючому сервері, клієнтська програма, крім ключу доступу отримує список варіантів відповідей ($a_0, a_1, \dots, a_m$), їх текстовий опис та відкриті параметри алгоритму шифрування – публічний ключ системи (P_S), та параметри еліптичної кривої. Коли користувач обирає один з варіантів (a_V), клієнтська програма повинна відобразити число-вагу обраного варіанту у область еліптичної кривої (P_V).

$$P_V = a_V \cdot G$$

Отриману у результаті попередньої дії точку необхідно зашифрувати, використавши відкритий ключ системи, отриманий у керуючого серверу. Для цього клієнтська програма генерує випадкове число ($k,\ a_m \cdot n + 1 < k < P_E$) – сеансовий приватний ключ. В результаті шифрування отримаємо пару точок (P'_V) еліптичної кривої E.

$$P'_V = (kG, P_V + kP_S)$$

Перша частина ($LP'_V = kG$) даної пари – підказка, що дозволяє власнику відкритого ключа, використавши приватний ключ виділити початкову точку з другої частини пари ($RP'_V = P_V + kP_S$). Точку RP'_V необхідно гомоморфно додати до загального попереднього результату голосування (S'_{i-1}), що зберігається на сервері голосування.

$$S'_i = S'_{i-1} + RP'_V$$

$$S' = \sum_{i=1}^{n} RP'_{V\,i}$$

По завершенні терміну проведення голосування керуючий сервер робить запит до серверу голосування для отримання загального результату. Сервер голосування у свою чергу опитує кожну з виборчих дільниць. Локальний сервер виборчої дільниці передає серверу голосування зашифровану суму S' по кожному з варіантів відповідей та список підказок $LP'_{V\,i}$.

Для отримання розшифрованої суми ваг варіантів відповідей,сервер повинен помножити кожну з підказок на приватний ключ шифрування системи (p) та відняти результат від суми (S').

$$S = S' - \sum_{i=1}^{n} p \cdot RP'_{V\,i}$$

Якщо підставити значення S' та RP'_V, отримаємо розшифроване значення суми ваг варіантів голосування користувачів:

$$S = S' - \sum_{i=1}^{n} p \cdot k_i \cdot G = \sum_{i=1}^{n} (P_{V\,i} + k_i P_S) - \sum_{i=1}^{n} k_i P_S = \sum_{i=1}^{n} P_{V\,i}$$

Після отримання розшифрованого варіанту, необхідно відобразити його з області точок еліптичної кривої, назад у область цілих чисел. Для цього сервер повинен згенерувати перші h точок еліптичної кривої, де h:

$$h = n \cdot x$$

Так як відповідь Ні (коли виборець не голосує) кодується як 1 та також додається до суми голосів, серверу необхідно виділити кількість голосів в залежності від загальної кількості проголосувавших (N):

$\begin{cases} 2x + y = S \\ x + y = N \end{cases}$ де, x – кількість людей проголосувавших за варіант, а y – проти.

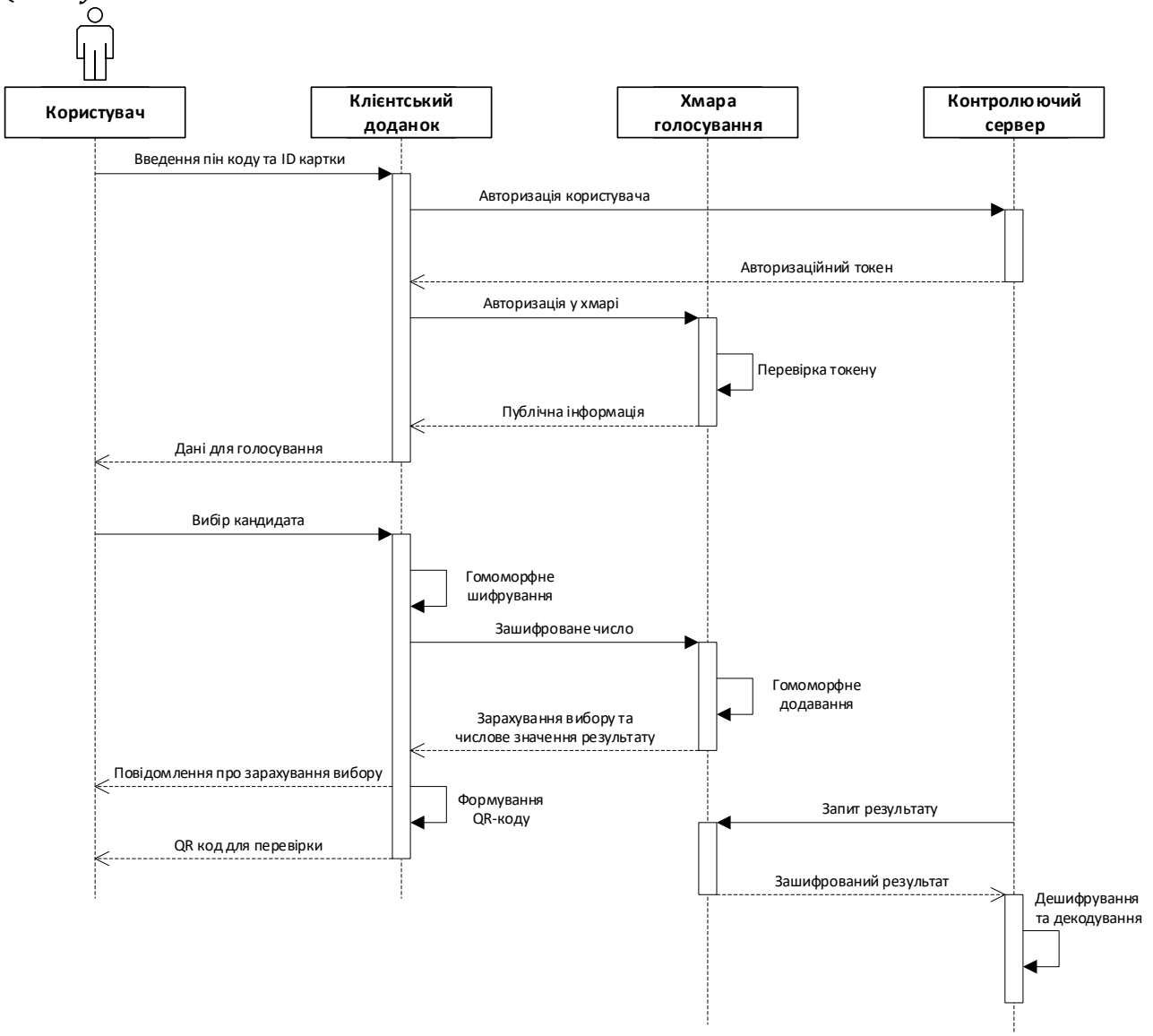

Рисунок 11 - Діаграма послідовностей комп’ютерної системи голосування з публічним хмарним сервісом

В ході даного розділу було розроблено та впроваджено інформаційно захищену хмарну систему для створення відгуків для мобільного додатку. Перевагою даної системи над існуючими аналогами є неможливість доступу до приватної інформації користувачів та загальної статистичної інформації додатку.

Задача створення модулю, який би відповідав за автоматизований збір інформації та формування звітів на основі відгуків користувачів є досить трудомісткою і розповсюдженою, тому існує значна кількість сервісів, що надають цей функціонал. Прикладами таких сервісів є Uservoice, HelpStack, Zendesk, SimpleFeedback, HappyFox.

Спільним недоліком даних систем є накопичення інформації про користувачів додатків, в яких вони використовуються. За звичайних умов, ця інформація захищена при передачі та збереженні. Проте, вона стає вразливою під час обробки у хмарному сервісі.

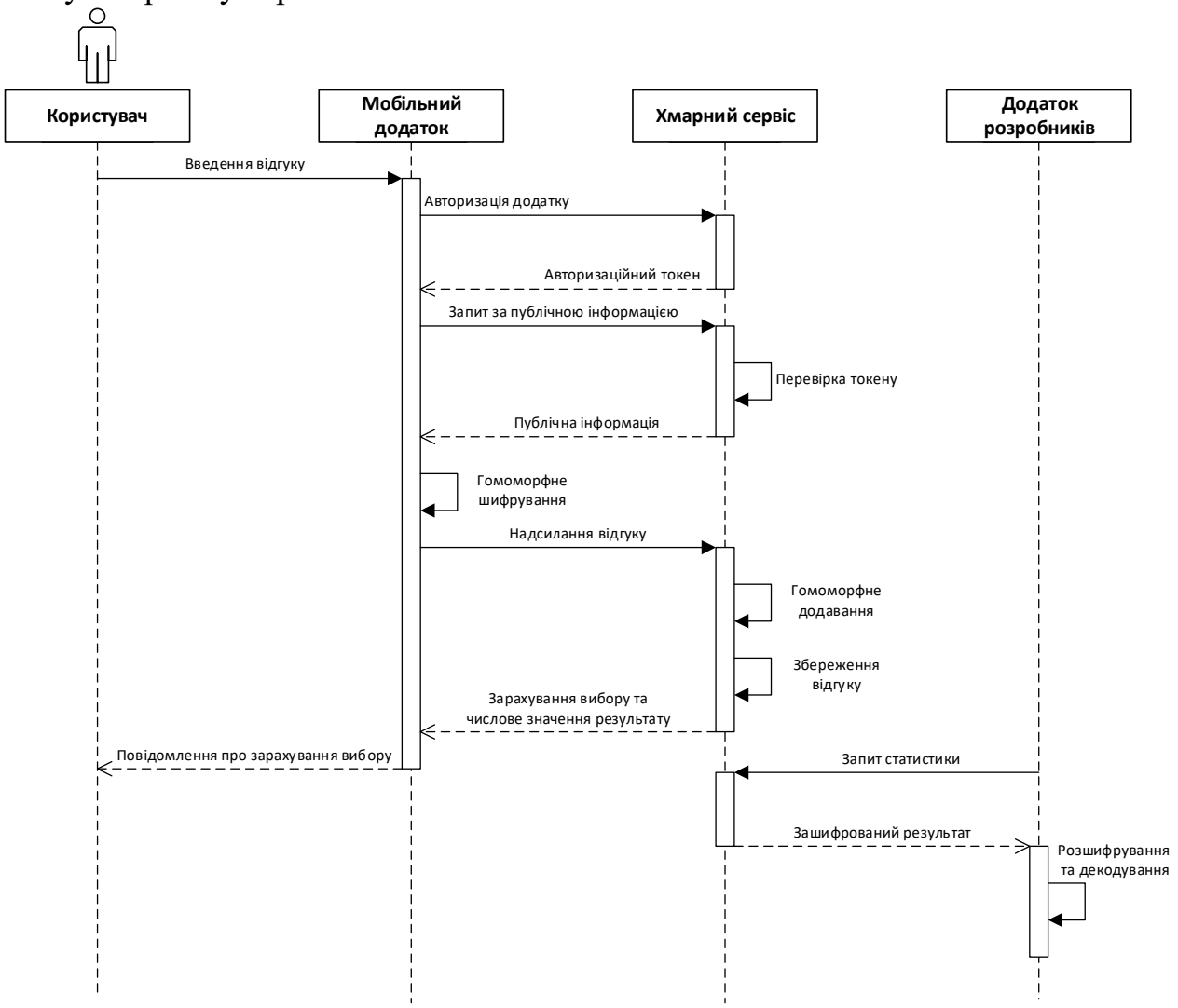

Рисунок 12 - Діаграма послідовностей процесу збереження відгуку

Під час тестування було додано 1000 відгуків кожного типу. Для тестування використовувався метод деперсоналізації на основі частково гомоморфного шифрування з використанням алгоритму на основі еліптичних кривих та на

основі алгоритму Пейє. Час виконання тесту для кожного з алгоритмів наведено у таблиці:

Таблиця 8 - Час виконання тесту

Назва методу	Час виконання
Алгоритм на основі еліптичних кривих	4152 мс
Алгоритм Пейє	4156 мс

За результатами експерименту виявлено, що середня швидкість опрацювання одного відгуку при використанні системи забезпечення анонімності на основі методу частково гомоморфного шифрування на еліптичних кривих є на 2% швидшим ніж при використанні методу Пейє. Значна розбіжність з експериментальними значеннями отриманими в 3му розділі пояснюється використанням бібліотеки LibPaillier 0.8, що реалізована на мові більш низького рівня, ніж у попередніх експериментах.

ОСНОВНІ РЕЗУЛЬТАТИ ТА ВИСНОВКИ

У дисертаційній роботі проведено дослідження присвячені підвищенню ефективності методів захисту інформації в комп`ютерних системах, що використовують у своєму складі публічні хмарні сервіси на основі розробки нових методів та засобів шифрування.

Основні результати досліджень є такими:

1. Проведено аналіз проблем пов’язаних з використанням публічних хмарних технологій комп’ютерних обчислень. Показано, що значною загрозою для сучасних комп’ютерних систем є неправомірні дії зчинені власниками сторонніх обчислювальних ресурсів які використовує комп’ютерна система. На основі огляду існуючих моделей та стратегій розгортання хмарних сервісів, зроблено висновок, що особлива увага повинна бути приділена публічним хмарним сервісам. Проведено аналіз сучасних методів захисту інформації, при її передачі, зберіганні та обробці у публічному хмарному сервісі, при його використанні у складі комп’ютерної системи.
2. Розроблено систему деперсоналізації користувачів, при використанні публічного хмарного сервісу комп’ютерних обчислень на основі частково гомоморфного алгоритму шифрування, що дозволила виконувати обчислення у публічному хмарному сервісі без розкриття приватної інформації користувачів.
3. Визначено критерій ефективності алгоритму частково гомоморфного шифрування, що орієнтована на використання у складі системи деперсоналізації користувачів, кількість часу витраченого на одну операцію гомоморфного додавання. Даний критерій може бути використаний для порівняння ефективності алгоритмів частково гомоморфного шифрування при використанні публічного хмарного сервісу.
4. Розроблено теоретично обґрунтовану модифікацію схеми шифрування на основі еліптичних кривих з метою надання їй гомоморфних властивос-

тей відносно операції додавання. Проаналізовано криптостійкість частково гомоморфного алгоритму на основі еліптичних кривих. Виконано порівняння створеного алгоритму з аналогом – алгоритмом Пейє (створений алгоритм швидший на 38%).

5. Розроблено математичні моделі системи деперсоналізації користувачів хмарного сервісу з використанням частково гомоморфного алгоритму шифрування на основі еліптичних кривих, що дозволяють захистити приватну інформацію користувачів комп'ютерної системи, що використовує хмарний сервіс як один із складових компонентів.

6. Розроблено методику декодування чисел, закодованих точками еліптичної кривої. Процес декодування складається з двох етапів – попереднього (генерація достатньої кількості точок еліптичної кривої, способом, що базується на методі з фіксованою точкою), та декодування (знаходження закодованого числа по координатам закодованої точки). У ході роботи було визначено кількість пам'яті необхідного для збереження 2^{32} точок еліптичної кривої – 256 Gb, та час необхідний для генерації даного числа точок у одно поточному режимі – 13 год 9 хв. Даний метод дозволив використовувати алгоритми шифрування на основі еліптичних кривих відносно цілих чисел.

7. Розроблено методику створення систем, що орієнтовані на захист приватної інформації користувачів, шляхом перетворення моделі обчислень з метою використання алгоритмів часткового або повністю гомоморфного шифрування. Основною ціллю створеної методики є виокремлення обчислювальних процедур, які будуть виконуватися на стороні публічного хмарного сервісу, та перенесення їх на арифметичну базу обраного методу шифрування.

8. Реалізовано програмне забезпечення, що використовує обчислювальні процедури частково гомоморфного шифрування на основі еліптичних кривих з використанням обчислювальних потужностей технічних засобів.

9. Розроблено алгоритмічне забезпечення та програмний моделюючий комплекс з використанням мов програмування високого рівня.

10. Результати проведених досліджень впроваджено в ТОВ „Скайсофттек", при проектуванні засобів та пристроїв, що обробляють інформацію у публічному хмарному сервісі.

СПИСОК ОПУБЛІКОВАНИХ ПРАЦЬ ЗА ТЕМОЮ ДИСЕРТАЦІЇ

[1] Є. О. Титарчук, «Захист даних в хмарних технологіях комп'ютерних обчислень», *Придніпровський науковий вісник*, № 5, no 152, с. 77–82, 2014.

[2] Р. Н. Квєтний і Є. О. Титарчук, «Використання гібридної криптографії в хмарних технологіях комп'ютерних обчислень», *Сборник научных трудов Sworld*, № 3, с. 63–67, 2014.

[3] Р. Н. Квєтний, Є. О. Титарчук, і А. А. Гуржій, «Метод та алгоритм обміну ключами серед груп користувачів на основі асиметричних шифрів ECC та RSA», *Інформаційні технології та комп'ютерна інженерія*, № 3 (37), с. 38-44, 2016.

[4] Р. Н. Квєтний і Є. О. Титарчук, «Використання частково гомоморфного

алгоритму шифрування на еліптичних кривих у хмарній системі електронного голосування», *Оптико-електронні інформаційно-енергетичні технології*, № 3 (32), с. 14–22, 2016.

[5] R. N. Kvyetnyy, E. A. Titarchuk, O. N. Romanyuk, K. Gromaszek, і N. Mussabekov, «Usage of the hybrid encryption in a cloud instant messages exchange system», *Photonics Appl. Astron. Commun. Ind. High-Energy Phys. Exp.*, no 10031, pp 117-126, 2016.

[6] Р. Н. Квєтний і Є. О. Титарчук, «Аналіз криптостійкості частково гомоморфного алгоритму шифрування на основі еліптичних кривих», *Інформаційні технології та комп'ютерна інженерія*, № 1 (38), с. 83–87, 2017.

[7] Р. Н. Квєтний і Є. О. Титарчук, «Хмарна система обміну електронними грошима на основі алгоритму частково гомоморфного шифрування», *Інформаційні технології та комп'ютерна інженерія*, № 2, с. 37-41, 2017.

[8] Є. О. Титарчук, «Захист даних в хмарних технологіях комп'ютерних обчислень», в *XLII регіональна науково-технічна конференція професорсько-викладацького складу, співробітників та студентів університету з участю працівників науково-дослідних організацій та інженерно-технічних працівників підприємств м. Вінниці та області*, 2013, с. 3, [Електронний ресурс]. Доступно: http://inmad.vntu.edu.ua/portal/static/3EDC7485-CE4C-47B6-8BC7-560FBB074395.pdf. Дата доступу: 14/5/2018

[9] Р. Н. Квєтний і Є. О. Титарчук, «Використання гібридної криптографії в хмарних технологіях комп'ютерних обчислень», в *Міжнародна науково-практична Інтернет-конференція. Наукові дослідження і їх практичне застосування. Сучасний стан та шляхи розвитку '2014*, 2014, с. 181-182.

[10] Р. Н. Квєтний і Є. О. Титарчук, «Використання гібридного шифрування в хмарних технологіях комп'ютерних обчислень», в *IX Міжнародна науково-практична конференція ІОН2014*, 2014, с. 170-172.

[11] Р. Н. Квєтний і Є. О. Титарчук, «Захист даних в хмарних технологіях комп'ютерних обчислень», в *XII Міжнародна конференція. Контроль і управління в складних системах. КУСС 2014*, 2014, с. 90-91.

[12] Р. Н. Квєтний і Є. О. Титарчук, «Використання гібридного шифрування в хмарній системі обміну миттєвими повідомленнями», в *InfoCom 2015: Матеріали 1-ї Міжнародної конференції присвяченої 70-річчю кафедри автоматики та управління в технічних системах*, 2015, с. 104-106.

[13] Р. Н. Квєтний і Є. О. Титарчук, «Алгоритм частково гомоморфного шифрування на основі еліптичних кривих», в *XIII міжнародна конференція «Контроль і управління в складних системах (КУСС-2016)»*, 2016, с. 18-20.

[14] Р. Н. Квєтний і Є. О. Титарчук, «Хмарна система обміну електронними грошима на основі алгоритму частково гомоморфного шифрування», в *Вимірювання, контроль та діагностика в технічних системах (ВКДТС-2017)*, 2017, с. 202-204

АНОТАЦІЯ

Титарчук Є. О. **Захист персональної інформації користувачів комп'ютерних систем при використанні публічних хмарних сервісів. – Кваліфікаційна наукова праця на правах рукопису.**

Дисертація на здобуття наукового ступеня кандидата технічних наук за спеціальністю 05.13.05 «Комп'ютерні системи та компоненти». – Вінницький національний технічний університет. – Вінниця, 2018.

У дисертаційній роботі поставлена та вирішена актуальна задача захисту персональної інформації користувачів комп'ютерної системи, одним із компонентів якої є публічний хмарний сервіс, шляхом удосконалення моделі взаємодії компонентів комп'ютерної системи.

Запропоновано та розроблено нову математичну модель сервісу деперсоналізації користувачів, яка на відміну від існуючих, використовує метод частково гомоморфного шифрування на основі еліптичних кривих, що дозволяє захистити інформацію користувача від несанкціонованого доступу до неї зі сторони провайдера хмарного сервісу, враховуючи необхідність її обробки.

Запропоновано новий метод частково гомоморфного шифрування відносно операції додавання, що на відміну від існуючих аналогів використовує математичний апарат еліптичних кривих, який, при однаковій криптографічній стійкості запропонованого алгоритму, робить його швидшим, ніж аналогічні алгоритми відносно часу виконання однакової кількості операцій гомоморфного додавання за секунду (141.4 оп/с проти 119 оп/с алгоритму Пейє), а його довжину ключа – меншою (256 біт проти 2048 біт алгоритму Пейє).

Запропоновано метод кодування чисел точками еліптичної кривої з попередньою побудовою таблиці відповідності, що на відміну від існуючих аналогів включає етап попередньої генерації n-точок еліптичної кривої (де n – максимальне число, яке необхідно декодувати), що дозволяє виконувати операцію декодування числа, при відомому його максимальному розмірі.

Представлено метод генерації спільного ключа симетричного алгоритму шифрування на основі еліптичних кривих, що може бути використаний у комп'ютерній системі, що складається з декількох компонентів, кожен з яких має доступ до єдиного хмарного сховища даних. Особливістю методу є можливість формування симетричного ключа шифрування для групи компонентів комп'ютерної системи.

Реалізовано програмне забезпечення, що реалізує ядро системи деперсоналізації користувачів при використанні інформаційної системи, що виконує обчислення на стороні хмарного сервісу публічного типу.

Ключові слова: публічний хмарний сервіс, частково гомоморфне шифрування, еліптична крива, гібридне шифрування, кодування чисел точками еліптичної кривої.

ABSTRACT

Titarchuk E. A. **Protection of personal information of users of computer systems which use public cloud services. – Qualification scientific paper as manuscript.**

Thesis for PhD degree in technical sciences on the speciality 05.13.05 «Computer systems and components» (123 – Computer engineering). – Vinnytsia National Technical University. – Vinnytsia, 2018.

Thesis solves the actual task of protection of personal information of users of the computer system, one component of which is a public cloud service, by improving the model of components interaction in the computer system.

A new mathematical model of user depersonalization service is proposed and developed, which, unlike existing ones, uses partially homomorphic encryption method based on elliptic curves, which allows to protect user information from unauthorized access to it from the side of the provider of a cloud service, taking into account the processing necessity of this data.

Modern computer systems increasingly contain in their composition several components presented by public or private cloud services. Usage of the components provided by third-party cloud services can greatly simplify the development of a computer system and improve its characteristics due to the flexible scaling of computing resources, the collection of usage statistics, the choice of physical location of the server, etc.

However, this manifests itself in the main disadvantage of cloud services - the private user information actually becomes available to third parties - the provider, in addition, data can become vulnerable when they are transmitted by communication channels, processing and storage.

The paper analyzed the problems associated with the use of public cloud computing technologies. It is shown that a significant threat to modern computer systems is the unlawful actions committed by owners of third-party computing resources that are used by the computer system. Based on an overview of the existing models and cloud deployment strategies, it is concluded that special attention should be paid to public cloud services. Also, was carried out an analysis of modern methods of information security, data transmission, storage and processing in the public cloud service, while it is used as a part of a computer system.

A new method of additive homomorphic encryption scheme is proposed, which, in contrast to existing analogues, uses the mathematical apparatus of elliptic curves, which, with the same cryptographic strength of the proposed algorithm, makes it faster than similar algorithms with respect to the execution time of the same number of homomorphic addition operations per second (141.4 op/s versus 119 op/s Paillier's algorithm), and its key length is smaller (256 bits versus 2048 bits of the Paillier's algorithm).The designed algorithm allows to add two encrypted numbers homomorphically without decrypting them, and get correct result after decrypting. The peculiarity of the algorithm is the use of session encryption keys, due to which was achieved the difference between encrypted texts even of identical numbers.

This encryption scheme operates with point of an elliptic curve, so to map field of integer numbers to field of the elliptic curve we offer a new method of numbers encoding to the elliptic curve's points with the preliminary construction of the table of correspondence, which, in contrast to the existing analogues, includes the stage of the previous generation of n-points of the elliptic curve (where n is the maximum number that needs to be decoded), and allows to decode the number, known to its maximum size.

During the storage the information in a public cloud for performance purposes, it is expedient to use symmetric encryption algorithms. In work was presented the method of generating a common key for a symmetric encryption algorithm based on elliptic curves is presented, which can be used in a computer system consisting of several components, each of which has access to a single cloud data warehouse. A feature of the method is the possibility of forming a symmetric encryption key for a group of components of the computer system

Are developed the software tools that enable to determine the speed of execution of operations of homomorphic addition and the required number of takts of the computer processor for software implementation of the proposed method and the similar algorithm is Paillier's additive partially homomorphic scheme

Also was developed the method of creating systems aimed at protecting private information of users, by transforming the computing model to use algorithms of partial or completely homomorphic encryption. The main purpose of the established methodology is to isolate the computational procedures that will be performed on the side of the public cloud service, and transfer them to the arithmetic base of the selected encryption method.

Was made a software that implements the core of the user's depersonalization system with the use of an information system that performs computing on the side of a cloud-based public-service service.

Was developed the protected cloud system that aimed to collect responses of a mobile application. The advantage of this system over existing counterparts is the inability to access the private information of users and the general statistical information of the application. During the work an experimental study was performed, the results of which showed the advantage of the speed of the proposed encryption algorithm over existing analogues.

Key words: public cloud service, partially homomorphic encryption, elliptic curve, hybrid encryption, encoding of numbers by points of an elliptic curve.

АННОТАЦИЯ

Титарчук Е. А. **Защита персональной информации пользователей компьютерных систем при использовании публичных облачных сервисов. – Квалификационная научная работа на правах рукописи.**

Диссертация на соискание ученой степени кандидата технических наук по специальности 05.13.05 «Компьютерные системы и компоненты». - Винницкий национальный технический университет. - Винница, 2018.

В диссертационной работе поставлена и решена актуальная задача защиты персональной информации пользователей компьютерной системы, одним из компонентов которой является публичный облачный сервис, путем усовершенствования модели взаимодействия компонентов компьютерной системы.

Предложена и разработана новая математическая модель сервиса деперсонализации пользователей, которая в отличие от существующих, использует метод частично гомоморфного шифрования на основе эллиптических кривых, позволяет защитить информацию пользователя от несанкционированного доступа к ней со стороны провайдера облачного сервиса, учитывая необходимость ее обработки.

Предложен новый метод частично гомоморфного шифрования относительно операции сложения, что в отличие от существующих аналогов использует математический аппарат эллиптических кривых, который, при одинаковой криптографической стойкости предложенного алгоритма, делает его быстрее, чем аналогичные алгоритмы относительно времени выполнения одинакового количества операций гомоморфного сложения в секунду (141.4 оп/с против 119 оп/с алгоритма Пейе), а его длину ключа - меньше (256 бит против 2048 бит алгоритма Пейе).

Предложен метод кодирования чисел точками эллиптической кривой с предварительным построением таблицы соответствия, в отличие от существующих аналогов включает этап предварительной генерации n-точек эллиптической кривой (где n - максимальное число, которое необходимо декодировать), что позволяет выполнять операцию декодирования числа, при известном его максимальном размере.

Представлен метод генерации общего ключа симметричного алгоритма шифрования на основе эллиптических кривых, который может быть использован в компьютерной системе, состоящей из нескольких компонентов, каждый из которых имеет доступ к единому облачного хранилища данных. Особенностью метода является возможность формирования симметричного ключа шифрования для группы компонентов компьютерной системы.

Имплементировано программное обеспечение, реализующее ядро системы деперсонализации пользователей при использовании информационной системы, выполняет вычисления на стороне облачного сервиса публичного типа.

Ключевые слова: публичный облачный сервис, частично гомоморфное шифрования, эллиптическая кривая, гибридное шифрования, кодирование чисел точками эллиптической кривой.