УДК 621.396:004.056.5

# ГОМОМОРФНЕ ШИФРУВАННЯ

Марчук І.Ю.
Науковий керівник – В’юхін Даніїл Олександрович
Харківський національний університет радіоелектроніки, каф.БІТ,
Харків, Україна
тел.+38(067)-526-12-40, e-mail ivan.marchuk@nure.ua

This work contains information about the benefits and operation of Homomorphic Encryption. This type of encryption has prospects and ways of integration into life. The use of this encryption can ensure the confidentiality of information, which is very important nowadays due to the large number of threats on the network. The use of this type of encryption can be used in voting, petitions, elections and other areas where user privacy is important. The implementation of this type of encryption began in the last century, but specialists from IBM were able to achieve success and high-quality integration. This type of encryption can be modernized in different ways depending on the field of application.

Ця робота містить інформацію про переваги та роботу гомоморфного шифрування. Цей вид шифрування має перспективи і різні шляхи інтеграції в життя. Використання цього шифрування може забезпечити конфіденційність інформації, що дуже важливо в наш час через велику кількість загроз в мережі. Використання цього типу шифрування може використовуватися під час голосування, петицій, виборів та інших сфер, де конфіденційність користувачів важлива. Впровадження такого типу шифрування почалося ще в минулому столітті, але досягли фахівці з IBM перші змогли досягти успіху і якісної інтеграції цього шифрування. Цей тип шифрування можна модернізувати різними способами залежно від сфери застосування.

Гоморфне шифрування має велике значення та область застосування, основна мета доповіді створення шифрування що забезпечить захист приватних даних та хмарних ресурсів, контроль конфіденційності даних при їх передачі або зберіганні, аутентифікації джерела даних. Розроблений продукт має ціль виконувати ряд функції, що задовільнили б потреби користувача а саме організація процедури введення даних для шифрування, контроль вхідної інформації, генерування криптографічного ключа з заднами параметрами, організація процедури шифрування та виведення зашифрованих даних. Варто також врахувати основні вимоги що були поставлені до шифру розробником, а саме безпека, забезпечення конфеденційності, швидкості виконання простота реалізації на недорогому обладнанні.

Криптографічний захист може бути здійснений програмний апаратний,програмним або ж комбінованиим способом. Програмна реалізація криптографічного захисту менш затратна та легша в реалізації, проте

криптоаналітик може перехопити криптографічні ключі під час роботи програмного забезпечення, а іноді і після завершення, тому, потрібно вжити заходів для забезпечення повного очищення пам'яті від криптографічних ключів, які були використані в процесі роботи. Апаратна реалізація більш затратна через свою технологію експлуатації. Інформація для апаратних засобів передається в електронній формі через порт обчислювальної машини в середину апаратури де відбувається шифрування даних. Перехоплення або підробка інформації під час передавання для апаратури можливо лише при спеціально створених вірусах. Тому потрібно пам'ятати, що вибираючи апаратні засоби для зберігання криптографічних ключів, треба забезпечити захист від перехоплення ключів під час їх зчитування з носія та використання в програмному сегменті.Цей вид захисту має значно більшу швидкість оскільки в надійному програмному алгоритмі виконується значне число складних математичних операцій що сповільнює процес обрахування, до того ж апаратний захист надійніший від зовнішнього проникнення та універсальний оскільки апаратура більш проста в установці та важче піддається розумінню звичайним користувачем без глибоких знань, що потрібно при роботі з програмним захистом, його оновленням та модифікуванням. Щоб отримати цього результату за допомогою програмних засобів, шифрування повинне бути сховане в ядро операційної системи.

Проаналізувавши різного роду статті на тему програмного на апаратного шифрування даних можна прийти до висновку ,що наразі відомо вже багато різних способів шифрування , проте технології розвиваються тому та система, яка буда надійною декілька років тому, можливо вже завтра стане ненадійною, хтось може підібрати ключ до її взлому або ж створить програмне забезпечення який швидко підбере пароль.

При створенні алгоритму варто врахувати вимоги до продукти та потреби користувачів, а значить алгоритм має забезпечити безпеку, збереження конфіденційності, швидку швидкість виконання та простота виконання на недорогому обладнанні. Перша вдала спроба створення повністю гоморфного шифрування належить Крейгу Джентрі який запропонував використовувати даний тип шифрування з використанням операцій додавання та множення. Стоврення данного шифруання було взяте за основу та враховуючи уязвимості данного шифрування дозволило б зробити його модиікації та виправити недоліки.

Отже, врахоовуючи всі роботи по даній темі варто забезпечити шифрування яке б використовувало повний набір математичних функцій, точність і швидкість мають бути однаковими на всіх етапах обчислення, а кортеж ключів має бути настільки великимм щоб унеможливити атаку повним перебором, при цьому розмір зашифрованих даних та довжина ключа не має значно впливати на продуктивність системи.

Список використаних джерел:

1. Т.Г. Білова, В.О. Ярута, В.В. Побіженко Харківська державна академія культури, Харків, УДК 004.738.5 Кібернетика та системний аналіз (2015р.) https://openarchive.nure.ua/server/api/core/bitstreams/9fc60515-57ba-40a8-a281-d8cd27e1b3b1/content

2. Іванов Р.Є., д.т.н., проф. Писаренко Л.Д. КПІ ім. Ігоря Сікорського, УДК 003.26 Використання криптографічних методів для захисту даниху ПК(2018р.) https://ed.kpi.ua/wp-content/uploads/conferences/2018/2018-065-069.pdf