НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ»

Факультет прикладної математики

Кафедра програмного забезпечення комп'ютерних систем

«До захисту допущено»
Науковий керівник кафедри
_____ І. А. Дичка
(підпис)
"___" _____ 2016 р.

Дипломна робота

на здобуття ступеня бакалавра

з напряму підготовки 6.050103 "Програмна інженерія"

на тему МЕТОД ПРОГРАМНО-АПАРАТНОЇ РЕАЛІЗАЦІЇ ОПЕРАЦІЇ ПОШУКУ МУЛЬТИПЛІКАТИВНО-ОБЕРНЕНОГО ЕЛЕМЕНТА У КІЛЬЦІ ЛИШКІВ ЗА ДОВІЛЬНИМ МОДУЛЕМ

Виконав: студент 4 курсу, групи КП-21
Приходько Ернест Вікторович _____
(підпис)

Керівник старший викладач Онай М.В. _____
(підпис)

Рецензент. доц, каф. СПіСКС, доц., к.т.н. Романкевич В. О. _____
(підпис)

Засвідчую, що у цій дипломній роботі
немає запозичень з праць інших авторів
без відповідних посилань.
Студент _____
(підпис)

Київ – 2016

АНОТАЦІЯ

Дана дипломна робота присвячена дослідженню методів програмно-апаратної реалізації операції пошуку мультиплікативно-оберненого елемента у кільці лишків за довільним модулем.

ЇЇ метою є створення прототипів апаратних схем, які дозволяють виконувати операцію пошуку мультиплікативно-оберненого елемента у кільці лишків за довільним модулем, заснованих на різних відомих алгоритмах. Визначення їх складності і ефективності побудованих прототипів апаратних схем. Проведення порівняльного аналізу апаратних і програмних реалізацій.

Результатом виконання даної роботи є запропонована модифікація одного з варіантів розширеного RS-бінарного алгоритму Евкліда, його аналіз, та висновки щодо ефективності і доцільності апаратної реалізації певних груп алгоритмів пошуку мультиплікативно-оберненого елемента у кільці лишків за довільним модулем.

ABSTRACT

This thesis researches the methods for software-hardware implementation of the operation of search for modular multiplicative inverse in multiplicative group of integers modulo *n*.

Its purpose is to create hardware circuit prototypes capable of search for modular multiplicative inverse in multiplicative group of integers modulo *n*, based on various known algorithms, to evaluate their complexity and efficiency, to conduct a comparative analysis of hardware and software implementations.

The findings of this thesis are a proposed modification to one version of extended RS-binary Euclidean algorithm, its analysis and conclusions about effectiveness and expediency of hardware implementation for various groups of algorithms for modular multiplicative inverse search in multiplicative group of integers modulo *n*.