МИНИСТЕРСТВО ОБРАЗОВАНИЯ РЕСПУБЛИКИ БЕЛАРУСЬ

БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

МЕХАНИКО-МАТЕМАТИЧЕСКИЙ ФАКУЛЬТЕТ

Кафедра высшей алгебры и защиты информации

МИХЕЙЧИК
Андрей Дмитриевич

ЭЛЛИПТИЧЕСКИЕ КРИВЫЕ И ИХ ПРИМЕНЕНИЕ В КРИПТОСИСТЕМАХ С ОТКРЫТЫМ КЛЮЧОМ

Дипломная работа

Научный руководитель:
доцент, кандидат физ.-мат. наук
Васильев Денис Владимирович

Допущена к защите
«___» _____ 2022 г.
Зав. кафедрой высшей алгебры и защиты информации
доктор физико-математических наук, профессор В.В. Беняш-Кривец

Минск, 2022

РЕФЕРАТ

Дипломная работа: 38 с., 18 рис., 11 источников.

Ключевые слова: ЭЛЛИПТИЧЕСКИЕ КРИВЫЕ, ЭЛЛИПТИЧЕСКАЯ КРИПТОГРАФИЯ, КРИПТОГРАФИЯ ОТКРЫТЫХ КЛЮЧЕЙ, АТАКИ ПО СТОРОННИМ КАНАЛАМ.

Объект исследования: Эллиптические кривые

Цель исследования: Анализ использования эллиптических кривых в криптографии.

Методы исследования: Изучение литературы и проведение вычислительного эксперимента.

Полученные результаты и их новизна: Проведён эксперимент показывающий возможные уязвимости и их решения при использовании эллиптических кривых в криптографии.

Область возможного практического применения: криптография, защита информации.

Автор работы подтверждает, что приведенный в ней расчетноаналитический материал правильно и объективно отражает состояние исследуемого процесса, а все заимствованные из литературных и других источников теоретические, методологические и методические положения и концепции сопровождаются ссылками на их авторов.

РЭФЕРАТ

Дыпломная праца: 38 с., 18 мал. , 11 крыніц.

Ключавыя словы: ЭЛІПТЫЧНЫЯ КРЫВЫЯ, ЭЛІПТЫЧНАЯ КРЫПТАГРАФІЯ, КРЫПТАГРАФІЯ АДКРЫТЫХ КЛЮЧОЎ, АТАКІ ПА ПАБОЧНЫМ КАНАЛАХ.

Аб'ект даследавання: Эліптычныя крывыя.

Цэль даследавання: Аналіз выкарыстання эліптычных крывых у крыптаграфіі.

Метады даследавання: Вывучэнне літаратуры і правядзенне вылічальнага эксперыменту.

Атрыманыя вынікі і іх навізна: Праведзены эксперымент які паказвае магчымыя ўразлівасці і іх рашэнні пры выкарыстанні эліптычных крывых у крыптаграфіі.

Вобласць магчымага практычнага прымянення: крыптаграфія, абарона інфармацыі.

Аўтар працы пацвярджае, што прыведзены ў èй разлікова-аналітычны матэрыял правільна і аб'ектыўна адлюстроўвае стан доследнага працэсу, а ўсе запазычаныя з літаратурных і іншыхкрыніц тэарэтычныя, метадалагічныя і метадычныя становішча і канцэпцыі суправаджаюцца спасылкамі на іх аўтараў.

ANNOTATION

Degree paper: 38 p., 18 ill., 11 sources.

Key words: ELLIPTIC CURVES, ELLIPTIC CRYPTOGRAPHY, PUBLIC KEY CRYPTOGRAPHY, SIDE CHANNEL ATTACKS.

Object of research: Elliptic Curves.

Purpose of research: Analysis of the use of elliptic curves in cryptography.

Research methods: Studying the literature and conducting a computational experiment.

Obtained results and their novelty: An experiment was conducted showing possible vulnerabilities and their solutions when using elliptic curves in cryptography.

Area of possible practical application: cryptography, information security.

The author of the work confirms that computational and analytical material presented in it correctly and objectively reproduces the picture of investigated process, and all the theoretical, methodological and methodical positions and concepts borrowed from literary and other sources are given references to their authors.