

МИНИСТЕРСТВО ОБРАЗОВАНИЯ РЕСПУБЛИКИ БЕЛАРУСЬ
БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
ФАКУЛЬТЕТ РАДИОФИЗИКИ И КОМПЬЮТЕРНЫХ ТЕХНОЛОГИЙ
Кафедра информатики и компьютерных систем

Аннотация к дипломной работе
«Параллельное решение задач криптоанализа хэш-функции»

Борбут Евгений Сергеевич

Научный руководитель — ст. преподаватель Серикова Н. В.

Минск, 2017

РЕФЕРАТ

Работа содержит 10 источников, 15 иллюстраций, 2 схемы, 5 таблиц, 1 приложение. Объем работы составляет 72 страницы.

Перечень ключевых слов: КРИПТОАНАЛИЗ, ХЭШ-ФУНКЦИЯ, MD5, ПАРАЛЛЕЛЬНОЕ ПРОГРАММИРОВАНИЕ, MPI.

Целью дипломной работы является анализ эффективности решения задач криptoанализа хэш-функции с помощью параллельных вычислений.

Объектом данной дипломной работы являются алгоритмы, методы и средства параллельного решения задачи криptoанализа хэш-функции.

Автор работы подтверждает, что работа выполнена самостоятельно, а также, что приведенный в ней аналитический 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

Пры напісанні работы выкарыстоўваліся 10 крыніц. У працы прымяняюцца 15 ілюстрацый, 2 схемы, 5 табліц, 1 прыкладанне. Агульны аб'ём працы складае 72 старонак.

Пералік ключавых слоў: КРЫПТААНАЛІЗ, ХЭШ-ФУНКЦЫЯ, MD5, ПАРАЛЕЛЬНАЕ ПРАГРАМАВАННЕ, MPI.

Мэтай дыпломнай працы з'яўляецца аналіз эфектыўнасці рашэння задач крывааналіза хэш-функцыі з дапамогай паралельных вылічэнняў.

Аб'ектам дадзенай дыпломнай працы з'яўляюцца алгарытмы, методы і сродкі паралельнага рашэння задачи крывааналіза хэш-функцыі.

Аўтар працы пацвярджае, што праца выканана самастойна, а таксама, што прыведзены ў ёй аналітычны матэрыял правільна і аб'ектыўна адлюстроўвае стан доследнага працэсу, а ўсе запазычаныя з літаратурных і іншых крыніц тэарэтычныя, метадалагічныя і методычныя палажэнні і канцепцыі суправаджаюцца спасылкамі на іх аўтараў.

ABSTRACT

10 sources are used in the work. Work includes 15 illustrations, 2 schemes, 5 tables, 1 attachment. The total amount of the work is 73 pages.

The list of key words: CRYPTANALYSIS, HASH FUNCTION, MD5, PARALLEL PROGRAMMING, MPI.

The aim of the study is analysis of the effectiveness of solving cryptanalysis problems of hash functions using parallel programming.

The object of this study are algorithms and methods of parallel solution of the cryptanalysis of the hash function.

The author of the study confirms that the work is done independently, and analytical material used reflects the state of the process under investigation correctly and objectively, and all theoretical and methodological terms and concepts borrowed from the literature and other sources accompanied by references to their authors.