БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

Факультет радиофизики и компьютерных технологий

Кафедра системного анализа и компьютерного моделирования

Аннотация к дипломной работе

«Разработка и реализация асимметричной системы криптографии по схеме Нидеррайтера для процессоров с ядром Cortex M3»

Горбанов Павел Иванович

Научный руководитель – ст. преподаватель Коржуков П.П.

2014

РЕФЕРАТ

Дипломная работа содержит 91страницу (включая титульный лист, оглавление, списки сокращений и используемой литературы, рефераты, приложение), 7 рисунков, 16 таблиц и 40 наименований источников. Одно приложение.

ЛИНЕЙНЫЙ КОД, ГРУППОВОЙ КОД, ЦИКЛИЧЕСКИЙ КОД, КВАЗИ-ЦИКЛИЧЕСКИЙ КОД, ВЕС ХЭММИНГА, КОЛЬЦО, ГРУППА, ПОЛЕ, ПОЛЕ ГАЛУА, ПОРОЖДАЮЩАЯ МАТРИЦА, ПРОВЕРОЧНАЯ МАТРИЦА, ЦИРКУЛЯНТ, СИНДРОМ, КОДЕР, ДЕКОДЕР, КОД С МАЛОЙ ПЛОТНОСТЬЮ ПРОВЕРОК НА ЧЁТНОСТЬ, КОД С УМЕРЕННОЙ ПЛОТНОСТЬЮ ПРОВЕРОК НА ЧЁТНОСТЬ, ГРАФ ТАННЕРА, КРИПТОГРАФИЯ, КРИПТОСИСТЕМА, СХЕМА МАКЭЛИСА, СХЕМА НИДЕРРАЙТЕРА, ШИФРАЦИЯ, ДЕШИФРАЦИЯ, ГЕНЕРАЦИЯ КЛЮЧЕЙ, УРОВЕНЬ БЕЗОПАСНОСТИ, АТАКА НА КРИПТОСИСТЕМУ, ОПТИМИЗАЦИЯ АЛГОРИТМОВ, МИКРОПРО-ЦЕССОР, АРИФМЕТИКО-ЛОГИЧЕСКОЕ УСТРОЙСТВО, ТАКТОВАЯ ЧАСТОТА, ОПЕРАТИВНАЯ ПАМЯТЬ.

Работа посвящена разработке и построению асимметричной криптосистемы на 32-разрядном процессоре с RISC архитектурой на основе одного из классов кодов, контролирующих ошибки. Для этого в работе исследуются две самостоятельные подсистемы: подсистема кодирования-декодирования выбранных в работе кодов, а именно, квазициклических кодов с умеренной плотностью проверок на чётность, и подсистема шифрации-дешифрации сообщений. Целью работы является разработка, поиск эффективных решений и реализация алгоритмов исследуемой асимметричной криптосистемы по схеме Нидеррайтера с длиной ключа 9216 бит на ARM-процессоре с ядром Cortex M3. Для поиска эффективных решений исследуются основные операции, выполняемые в двух независимых подсистемах, и даются предложения по использованию эффективных алгоритмов для их выполнения, подходящих структур данных; производится выбор пороговых значений в схеме декодера на основе имеющихся некоторых экспериментальных данных.

Результатом работы является разработанный и реализованный на ARM-процессоре макетный образец самостоятельной асимметричной криптосистемы с системным программным обеспечением, пригодной для дальнейших ее усовершенствований и модификаций.

Выполненные разработки будут использоваться для факультативных заданий отлично успевающим студентам в лабораторном практикуме по курсу «Программирование микропроцессорных систем».

ABSTRACT

Thesis consists of 91pages (including the cover page, table of contents, lists of abbreviations and used literature, essays and application), 7 drawings, 16 tables, single application. 40 sources were used.

LINEAR CODE, GROUP CODE, CYCLIC CODE, QUASI-CYCLIC CODE, HAMMING WEIGHT, RING, GROUP, FIELD, GALOIS FIELD, GENERATOR MATRIX, PARITY-CHECK MATRIX, CIRCULANT, SYN-DROME, ENCODER, DECODER, LOW-DENSITY PARITY-CHECK CODE, MODERATE-DENSITY PARITY-CHECK CODE, TANNER GRAPH, CRYPTOGRAPHY, CRYPTOSYSTEM, MCELIECE SCHEME, NIEDERREITER SCHEME, ENCRYPTION, DECRYPTION, KEY GENERATION, SECURITY LEVEL, THE ATTACK ON THE CRYPTOSYSTEM, OPTIMIZATION ALGORITHMS, A MICROPROCESSOR, AN ARITHMETIC LOGIC UNIT, CLOCK RATE, RAM.

Investigation is devoted to the development and creating asymmetric cryptosystem on a 32-bit RISC processor with architecture based on one of Error correction codes. For this paper, we study two separate subsystems: the subsystem of coding-decoding codes selected for work, namely, the quasi-cyclic codes with moderatedensity paritcheck code and the subsystem of encryption-decryption messages. Aim is to develop, finding effective solutions and implementation of algorithms studied asymmetric cryptosystem on scheme Niederreiter with a key length of 9216 bits per processor with ARM-core Cortex M3. To find effective solutions were studied the basic operation of two independent subsystems, and were provided suggestions for using efficient algorithms for their implementation, suitable data structures; selects of threshold scheme on the basis of the decoder of some experimental data was made.Result is developed and implemented on ARM-processor scale-model of independent asymmetric crypto system with software suitable for its further improvements and modifications.Completed developments will be used for optional tasks for perfectly performing students in the laboratory practical course "Programming of microprocessor systems."