БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

МЕХАНИКО-МАТЕМАТИЧЕСКИЙ ФАКУЛЬТЕТ

Кафедра дифференциальных уравнений и системного анализа

Аннотация к дипломной работе

КРИПТОСИСТЕМА NTRU

Виланский Арсений Юрьевич

Научный руководитель:
кандидат физ.-мат. наук,
доцент Д. Н. Чергинец

2015

В дипломной работе 49 страниц, 7 рисунков, 2 таблицы, 19 источников, два приложения.

NTRU-КРИПТОСИСТЕМА, ЧИСЛОВЫЕ РЕШЕТКИ, АТАКА НА ОСНОВЕ РЕШЕТКИ, СЛОЖНОСТЬ АЛГОРИТМОВ.

Работа состоит из 3 глав, введения и заключения. Во введении обоснована актуальность работы и описаны задачи данного исследования.

В первой главе выполнен обзор литературы по вопросам, связанным с алгоритмической сложностью, квантовыми вычислениями, методологии построения криптографических систем с открытым ключом и обзором типичных атак на такие системы.

Вторая глава посвящена описанию криптосистемы NTRUEncrypt и связанным с ней математических основам теории решеток. В этой главе рассмотрены основные атаки на криптосистему NTRUEncrypt и обсуждается сложность этих атак.

Третья глава посвящена реализации атак на основе решетки и подобранного шифртекста. Приводятся примеры атак. Рассматриваются результаты выполненных атак при разных параметрах алгоритма NTRU. Также в этой главе приводятся результаты сравнения NTRUEncrypt с другими криптосистемами с открытым ключом, в частности, с рюкзачной криптосистемой Меркля-Хеллмана.

Дипломная работа носит практический характер и может быть использована в дальнейших исследования данной криптосистемы.

Все результаты дипломной работы строго доказаны в соответствии с принятыми в математике правилами. Обоснованность и достоверность полученных результатов обусловлена строгими математическими доказательствами сформулированных в работе лемм и теорем и согласованностью с результатами, известными ранее для конкретных частных случаев. Дипломная работа выполнена автором совместно с руководителем.

There are 49 pages, 7 images, 2 tables, 19 sources and 2 applications in the thesis work.

NTRU-CRYPTOSYSTEM, LATTICES, LATTICE-BASED ATTACK, ALGORITHM COMPLEXITY.

The work consists of three chapters, introduction and conclusion. In the introduction, the relevance of the work is defined and described the problem of the study.

The first chapter gives an overview of the literature on issues related to algorithmic complexity, quantum computing, methodology cryptographic public key, and an overview of common attacks on such systems.

The second chapter is devoted to describing the cryptosystem NTRUEncrypt and related mathematical foundations of the theory of lattices. This chapter describes the main attack on the cryptosystem NTRUEncrypt and discusses the complexity of these attacks.

The third chapter is devoted to the realization of attacks based on lattice matched ciphertext. Examples of attacks. The results of the attacks made at different parameters of the algorithm NTRU. This chapter also presents the results of the comparison NTRUEncrypt with other public-key cryptosystems, particularly with backpack Merkle-Hellman cryptosystem.

Diploma work is practical. Its results can be used in further studies of this cryptosystem.

All results of the thesis rigorously proved in accordance with the rules of mathematics. Validity and reliability of the results is due to the strict mathematical proofs formulated in the lemmas and theorems and consistency with the results previously known for certain special cases. Diploma work performed by the author together with the supervisor.