МИНИСТЕРСТВО ОБРАЗОВАНИЯ РЕСПУБЛИКИ БЕЛАРУСЬ

БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

МЕХАНИКО-МАТЕМАТИЧЕСКИЙ ФАКУЛЬТЕТ

Кафедра дифференциальных уравнений и системного анализа

Аннотация к дипломной работе

АНАЛИЗ СИСТЕМЫ ЭЛЕКТРОННОГО ГОЛОСОВАНИЯ ELECTIONGUARD

Борсукова София Борисовна

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

2020

Дипломная работа содержит 56 страниц, 4 рисунка, 8 источников и одно приложение.

Ключевые слова: ELECTIONGUARD, ЭЛЕКТРОННОЕ ГОЛОСОВАНИЕ, ДОКАЗАТЕЛЬСТВО С НУЛЕВЫМ РАЗГЛАШЕНИЕМ, СКВОЗНАЯ ПРОВЕРЯЕМОСТЬ, E2E СИСТЕМЫ, ГОМОМОРФНЫЕ СВОЙСТВА, КРИПТОСИСТЕМА ЭЛЬ-ГАМАЛЯ, ХЕШ-ФУНКЦИЯ, WOLFRAM MATHEMATICA.

В ходе выполнения дипломной работы изучалась криптографическая основа системы электронного голосования ElectionGuard и ее структура.

Целью дипломной работы является исследование свойств системы электронного голосования ElectionGuard.

В дипломной работе получены следующие результаты:

- Рассмотрены существующие модели систем сквозного проверяемого (E2E) голосования;
- Исследована система электронного голосования ElectionGuard и показана ее принадлежность к системам E2E;
- Проведен сравнительный анализ ElectionGuard с другими системами;
- Реализованы некоторые алгоритмы системы голосования ElectionGuard.

В дипломной работе представлена реализация следующих алгоритмов: генерация ключей, шифрование, дешифрование, а также проверка гомоморфных свойств. Практическая часть работы реализована в пакете Wolfram Mathematica.

Дипломная работа носит исследовательский характер. Ее результаты могут быть использованы как для дальнейшего исследования в области электронного голосования, так и для практической реализации системы сквозного проверяемого голосования.

Дипломная работа выполнена автором самостоятельно.

The research has 56 pages, 4 figures, 8 sources and one Appendix.

Keywords: ELECTIONGUARD, ELECTRONIC VOTING, ZERO-KNOWLEDGE PROOF, END-TO-END VERIFIABILITY, E2E SYSTEMS, HOMOMORPHIC PROPERTIES, EL GAMAL CRYPTOSYSTEM, HASH FUNCTION, WOLFRAM MATHEMATICA.

The cryptographic basis of the ElectionGuard electronic voting system and its structure were studied.

The purpose of this research is to study the properties of the ElectionGuard electronic voting system.

The following results were obtained:

- The existing models of end-to-end verifiable (E2E) voting systems are considered;
- The electronic voting system ElectionGuard is investigated and its belonging to E2E systems is shown;
- A comparative analysis of ElectionGuard with other systems was performed;
- Some algorithms of the ElectionGuard voting system are implemented.

The research presents the implementation of the following algorithms: key generation, encryption, decryption, and verification of homomorphic properties. The practical basis of research consists in realization algorithms in the Wolfram Mathematica package.

The thesis is of a research nature. Its results can be used for further research in the field of electronic voting, as well as for the practical implementation of a system of end-to-end verified voting.

The research was done solely by the author.