Abstract

Asymmetric systems based on coding theory are one of the oldest and most secure cryptosystems. However, these systems use very large keys, so they were not considered an alternative to commonly used systems based on problems in number theory. The situation changed when it turned out that these systems are resistant to cryptanalysis using a quantum computer. The intensification of research on this branch of cryptography resulted in the emergence of new algorithms and the systematization of issues related to the security of these systems.

The dissertation presents the possibilities of choosing Goppa and MDPC codes for the asymmetrical system. The method of choosing Goppa code parameters for the McEliece system was presented. This method ensures the shortest public key length for established security. The dissertation also includes analyzes new McEliece systems based on QC-MDPC codes and presents an improved method of selecting algorithm parameters for decoding these codes. Also, the analysis of the suitability of cryptographic systems based on coding theory was carried out in systems with limited hardware resources, as well as in modern communication techniques, such as the 5G. Post-quantum algorithms based on coding theory are very well suited for use in a modern telecommunications environment that enables the transfer of large amounts of data in a short time. This property eliminates the major disadvantage of coding theory systems, which is the large size of the public key.

Keywords: *McEliece, asymetric cryptosystems, Goppa code, bit-flipping algorithms, QC-MDPC code, postquantum cryptography, ISD algorithms.*