Секция «Дискретная математика и математическая кибернетика»

Коды в групповой алгебре диэдральной группы

Научный руководитель – Деундяк Владимир Михайлович

Веденев Кирилл Владимирович
Студент (бакалавр)
Южный федеральный университет, Институт математики, механики и компьютерных наук им. И.И. Воровича, Ростов-на-Дону, Россия
E-mail: vedenevk@gmail.com

В 1978 году Р. Мак–Элисом построена первая асимметричная кодовая криптосистема, основанная на применении помехоустойчивых кодов Гоппы, при этом эффективные атаки на секретный ключ этой криптосистемы до сих пор не найдены. К настоящему врмени известно достаточно много кодовых криптосистем, но их криптографическая стойкость уступает стойкости классической криптосистемы Мак–Элиса. В связи с развитием квантовых вычислений кодовые криптосистемы рассматриваются как альтернатива теоретико–числовым [4], поэтому актуальной представляется задача поиска перспективных классов кодов для построения новых стойких кодовых криптосистем. Для этого можно использовать некоммутативные коды, т.е. идеалы в групповых алгебрах $\mathbb{F}_q G$ над конечными некоммутативными группами G. Ранее изучалась стойкость криптосистем на кодах, индуцированных кодами на подгруппах [1] – [3].

Диэдральной группой D_{2n}, где $n \geq 2$, называется группа симметрий правильного плоского n-угольника с центром в точке O, состоящая из поворотов вокруг точки O на углы, кратные $\frac{2\pi}{n}$, и отражений относительно прямых, проходящих через O и одну из вершин или середину одной из сторон. В настоящей работе доказана теорема о структуре кодов в групповой алгебре $\mathbb{F}_q D_{2n}$, для этого были использованы результаты Ф. Е. Б. Мартинеса о разложении Ваддербёрна алгебры $\mathbb{F}_q D_{2n}$ [5]. Также рассмотрена структура кодов, которые индуцированны кодами над циклическими подгруппами группы D_{2n}.

Источники и литература

1) Деундяк В. М., Косолапов Ю. В. Криптосистема на индуцированных групповых кодах // Модел. и анализ информ. систем, 23:2 (2016), С. 137–152
2) Деундяк В. М., Косолапов Ю. В. Алгоритмы для мажоритарного декодирования групповых кодов // Модел. и анализ информ. систем, 22:4 (2015), С. 464–482
3) Деундяк В. М., Косолапов Ю. В., Лелюк Е.А. Декодирование тензорного произведения MLD-кодов и приложения к кодовым криптосистемам // Модел. и анализ информ. систем, 24:2 (2017), С. 239–252
4) D. J. Bernstein, J. Buchmann, E. Dahmen. Post-Quantum Cryptography. Springer-Verlag Berlin Heidelberg, 2009
5) F. E. Brochero Martinez. Structure of finite dihedral group algebra // Finite Fields and Their Applications, 35 (2015), P. 204–214.