ТЕОРЕТИКО-КОДОВАЯ СИСТЕМА ЗАЩИТЫ МАКЭЛИС С ПЕРЕСТРАИВАЕМЫМ КОДОМ ГОППЫ

В.В. Панькова, С.Б. Саломатин

Теоретико-кодовая система защиты использует высокую сложность решения задачи декодирования случайного кода над конечным полем. Система защиты задается совокупностью множеств: открытых текстов, криптограмм, прямых отображений, обратных отображений, ключей, параметризирующих прямые отображения, ключей, параметризирующих обратные отображения, таких, что сложность обратного отображения без знания ключа сопряжена с решением теоретико-сложностной задачи декодирования случайного кода [1, с. 47–62]. К недостаткам кодовых криптосистем можно отнести детерминизм генераторной матрицы, что делает их уязвимыми для атак с использованием алгоритмов распознавания кодовых структур.

В настоящей работе рассматривается теоретико-кодовая система, использующая рандомизированные коды Гоппа. В основе построения коды лежат полином Гоппы $g(x)$ над расширенным конечным полем, конечное подмножество L расширенного поля, а также функцию R, удовлетворяющая конгруэнтности нулю по модулю $g(x)$. Элементы L не являются корнями полинома $g(x)$. Декодирование кода Гоппы может быть выполнено различными методами [2].

Рассматриваются схемы кодирования и декодирования кода Гоппы с возможностью перестройки структуры путем автоматной рандомизации функции L, выбора требуемой формы функции распределения веса и алгоритма декодирования Патерсона. Анализ статистических свойств криптосистемы МакЭлис с рандомизированными кодами Гоппы показывает близость спектрально-корреляционных характеристик системы к характеристикам случайного процесса при заданной корректирующей способности кода. Применение рандомизированного кодов Гоппа в криптосистеме МакЭлис (Нидерайтер) расширяет область неопределенности задачи криптоаналитика распознавания кодовых конструкций, что в свою очередь повышает уровень защиты криптосистемы.

Литература

1. Biswas B., Sendrier N. McEliece Cryptosystem Implementation: Theory and practice / in “Post-Quantum Cryptography. Lecture Notes in Computer Science”. Berlin, Springer. 2009. 5299 p.

2. Влэдуц С.Г., Ногин Д.Ю., Цфасман М.А. Алгеброгеометрические коды. Основные понятия. М.: МЦНМО. 2003. 504 с.