**УДК 51-74**

# ОПТИМИЗАЦИЯ АЛГОРИТМА ДЕКОДИРОВАНИЯ ДВОИЧНЫХ КОДОВ ГОППЫ ПРИ ТРЕХ ОШИБКАХ

**Носков И.К.** (федеральное государственное автономное образовательное учреждение высшего образования «Национальный исследовательский университет ИТМО»)
**Научный руководитель – д. т. н., доцент Беззатеев С. В.**
(федеральное государственное автономное образовательное учреждение высшего образования «Национальный исследовательский университет ИТМО»)

В данном докладе предлагается решение проблемы декодирования двоичных кодов Гоппы, которые способны исправлять три ошибки. Данное решение позволяет оптимизировать алгоритм декодирования для двоичных кодов Гоппы.

**Введение.** В настоящее время коды Гоппы используются для построения криптосистем для постквантовой криптографии благодаря способности исправлению ошибок при высокой скорости кодирования. Например, одним из претендентов на новый криптографический стандарт для постквантовой криптографии является “современная криптосистема МакЭлиса”, построенная на двоичных кодах Гоппы. К сожалению, алгоритм Паттерсона для декодирования кодов Гоппы является сложной процедурой: для его использования необходимо найти обратный многочлен и извлечь квадратный корень из многочлена. Таким образом, возникает вопрос: можно ли реализовать алгоритм декодирования без решения таких сложных задач. В данной работе приводится вариант модификации алгоритма Паттерсона, который позволяет эффективно декодировать двоичные коды Гоппы, исправляющие три ошибки.

**Основная часть.** Суть предлагаемого решения заключается в том, чтобы использовать многочлен Гоппы вида $G(z)=z^3+z+a$, где $tr(a)=1$. Так как степень многочлена локаторов ошибок не может быть больше трех, а степень полученного при декодировании синдрома не может быть больше двух, то коэффициенты локатора ошибок можно найти, используя алгоритм описанный ниже. Коэффициенты многочлена $T(z)$ обратного многочлену синдрома $S(z)$ по модулю многочлена Гоппы можно найти с помощью уравнения $S(z)T(z)=1 \bmod G(z)$. Так как многочлены равны только в том случае, если коэффициенты при равных степенях равны, то получается система уравнений, которая содержит уравнения, которые получаются приравниванием коэффициентов одинаковой степени правой и левой части. Производя подобную процедуру для уравнения $f'(z)T(z)=f(z) \bmod G(z)$, где $f(z)$ – многочлен локаторов ошибок, а $f'(z)$ – его производная, однозначно находятся коэффициенты для многочлена локаторов ошибок. Таким образом, находится и сам многочлен локаторов ошибок.

**Выводы.** Данный метод может быть использован для оптимизации алгоритма декодирования двоичных кодов Гоппы, которые способны исправлять три ошибки. При использовании данного метода уменьшается время работы алгоритма декодирования, а также необходимость реализации алгоритма Евклида.

Носков И.К. (автор) Подпись

Беззатеев С.В. (научный руководитель) Подпись