УДК 51-74

ОПТИМИЗАЦИЯ АЛГОРИТМА НАХОЖДЕНИЯ КОРНЯ ДЛЯ ДВОИЧНЫХ СЕПАРАБЕЛЬНЫХ КОДОВ ГОППЫ

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 нахождения многочлена такого, квадрат которого в конечном поле будет равен x по модулю сепарабельного многочлена. Данное решение позволяет оптимизировать алгоритм декодирования для двоичных сепарабельных кодов Гоппа.

Введение. В настоящее время разработка квантовых компьютеров идет полным ходом. В связи с этим существующие криптосистемы становятся взламываемыми. Таким образом, необходимо разрабатывать новые, более стойкие алгоритмы, которые позволят сохранять информацию защищенной. В настоящее время большинство криптосистем, построенных на кодах Гоппы, используют такие алгоритмы декодирования, как расширенный алгоритм Эвклида и алгоритм Берлекэмпа-Месси несмотря на то, что существует алгоритм Паттерсона, который позволяет использовать в 2 раза меньше синдромных компонент. Это связано с тем, что алгоритм Паттерсона не оптимизирован для сепарабельных многочленов. Например, для использования алгоритма Паттерсона необходимо найти такой многочлен, что его квадрат в конечном поле будет равен x по модулю сепарабельного многочлена. В данной работе приводится данный алгоритм.

Основная часть. Суть предлагаемого решения заключается в том, чтобы разбить сепарабельный многочлен на множители, каждый из которых будет содержать все множители одной степени. Это можно сделать с помощью нахождения наибольшего общего делителя между многочленом и многочленом, который содержит все множители нужной степени. После разбиения многочлена на множители для каждого полученного многочлена необходимо найти многочлен, квадрат которого в конечном поле будет равен x по модулю данного множителя. Получив все такие многочлены, можно воспользоваться китайской теоремой об остатках для нахождения многочлена, который нам необходим.

Выводы. Данный метод может быть использован для оптимизации декодирования двоичных сепарабельных кодов Гоппы с помощью алгоритма Паттерсона. При использовании данного метода сокращается размер ключей в криптосистемах, построенных на помехоустойчивых кодах.

Носков И.К. (автор) Подпись

Беззатеев С.В. (научный руководитель) Подпись