УДК 004.056.55

ОБОБЩЕННЫЕ ОПЕРАЦИИ НАД ШИФРТЕКСТОМ

Кадыков В.Ю. (федеральное государственное автономное образовательное учреждение высшего образования «Национальный исследовательский университет ИТМО»)
Научный руководитель – к.ф.-м.н., доцент Левина А.Б.
(федеральное государственное автономное образовательное учреждение высшего образования «Национальный исследовательский университет ИТМО»)

Анализ систем полностью гомоморфного шифрования на данный момент является актуальным направлением для многих исследований. В данной работе приводится новый метод анализа таких систем, а также рассматривается существующий метод получения полностью гомоморфных систем на основе гомоморфного шифрования с ограничением, в котором основным способом является введение гомоморфной операции перешифровки.

Введение. В последние годы за рубежом активно исследуется отдельное направление в гомоморфном шифровании, а именно возможность реализации систем полностью гомоморфного шифрования. Характер работ имеет в своей основе результаты, опубликованные в 2009 году, согласно которым, обязательное условия для получения полностью гомоморфной системы - наличие механизма гомоморфной перешифровки шифртекста. При этом основной гомоморфной операцией является операция NAND над двумя шифртекстами, с помощью которой реализуются алгебраические операции. Все это порождает тенденцию к работам с выраженным техническим уклоном, в ходе которых используются логические элементы и булевы функции, отсутствию чисто математических изысканий. Это относится лишь к работам над полностью гомоморфными системами шифрования. Описанные выше тенденции выражаются, во-первых, в том, что операции перестают быть дистрибутивными в вычислительном плане, во-вторых, при формировании шифртекста в целях реализации возможности перешифровки происходит добавление некоторой части ключевой информации. Этот процесс способен снизить стойкость для определенных видов атак при порожденном взаимодействии нескольких вычислительных задач. При этом возникает вопрос о систематизации и анализе таких систем, например, за счет поиска примитива, пригодного для анализа целой системы, поиска закономерностей в принципах работы гомоморфных систем на решетках идеалов для исследования возможности их применения к другим математическим примитивам, способы синтеза гомоморфных систем. В работе рассматривается несколько гомоморфных систем шифрования, с обобщением которых исследуется возможность синтеза систем полностью гомоморфного шифрования относительно некоторого параметра безопасности. С помощью этого обобщения показывается, как схемы работы негомоморфных систем могут быть дополнены гомоморфными операциями. Исследуются пути построения полностью гомоморфных систем с использованием методов, основанных на основе теории множеств.

Основная часть. В качестве возможного решения предлагается использование конгруэнтной системы шифрования, которая с помощью определенных способов может быть приведена к наиболее исследованным гомоморфным системам шифрования на данный момент, таким как NTRU, система Джентри, система на целых числах. Выводятся основные соотношения для анализа конгруэнтной системы шифрования, на основе которых предлагается метод дополнения гомоморфными операциями для негомоморфных систем. В качестве элементарной конструкции для анализа гомоморфных систем шифрования используется основанный на теории множеств примитив, включающий значащую часть и шумовую составляющую. Показывается, какое влияние оказывает операция перешифровки в контексте исследуемой системы со стороны представленных теоретических положений, основное проявление которого – наличие редуцированного множества шифртекста.

Предлагаются пути разрешения этого побочного явления, вместе с которым и некоторые новые концепции для построения полностью гомоморфных систем шифровании.

Выводы. В качестве практических результатов исследования предлагаются: способ дополнения гомоморфными операциями для получения гомоморфной системы шифрования с ограничением в NTRU, метод выбора параметров в системе полностью гомоморфного шифрования на целых числах, а также оценка стойкости конгруэнтной системы шифрования.

Кадыков В.Ю. (автор) Подпись

Левина А.Б. (научный руководитель) Подпись