ИСПОЛЬЗОВАНИЕ КРИПТОГРАФИИ ПРИ ОБЛАЧНЫХ ВЫЧИСЛЕНИЯХ

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Агаев И.А.

Ганжа Виктор Александрович (доцент, кандидат физико-математических наук)

В последнее время облачные технологии и облачные вычисления приобретают все большую популярность. К ним проявляют интерес как крупные компании, которые хотят сократить затраты на оптимизацию инфраструктуры, так и небольшие фирмы, у которых нет возможности сразу развернуть собственную структуру для обработки данных. Несмотря на явные преимущества использования облачных вычислений, они требуют решения ряда вопросов, основными из которых являются обеспечение целостности, конфиденциальности, защита от несанкционированного доступа и сохранность личных данных пользователей, передаваемых и обрабатываемых в облаке.

Для обработки данных в публичных «облаках» работать необходимо с открытыми данными. В случае работы с конфиденциальной информацией необходимо предусмотреть использование организационных мер по хранению ключей либо специализированной аппаратуры. Существуют определенные риски, так как нельзя повлиять на то, как это происходит на стороне провайдера. Эту проблему можно решить путем передачи данных на облако в зашифрованном виде. При этом операции, которые производятся над этими данными в облаке, не смогут распространять информацию об этих данных.

Общая схема такого механизма представляет собой следующее:

- пользователь отправляет данные на облако в зашифрованном виде;
- пользователь отправляет запрос на выполнение некоторых операций над этими данными;
- программа, находящаяся в облаке, выполняет вычисления над этими данными;
- обработанные данные возвращаются пользователю;
- пользователь расшифровывает полученный результат.

Чтобы создать защищенное облачное хранилище необходимо использовать гомоморфные схемы шифрования. Данный тип шифрования позволяет делать любые вычисления с зашифрованными данными без их расшифровки. То есть, облако, которое производит вычисления, делает операции с зашифрованными данными, выполняя свой алгоритм (анализ на спам, поиск в базе данных, и т.д.), но при этом не имеет никакого понятия о зашифрованной внутри информации. Только пользователь, зашифровавший свои данные, может расшифровать результат вычисления.

Стандартная система шифрования состоит из трех алгоритмов:

- генерация ключей;
- шифрование;
- расшифровка.

Кромевышеперечисленных алгоритмов гомоморфная криптосистема включает в себя алгоритм вычислений. Алгоритм вычисления представлен следующим образом:

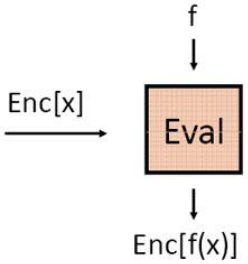

Рис.1 – Схема алгоритма гомоморфного вычисления

В качестве входных данных алгоритма используются зашифрованное сообщение Enc(M) и некая математическая функция f(). В ходе вычисления алгоритма на выходе появляется другое зашифрованное сообщение Enc(M2), причем M2=f(M).

Отрасль гомоморфного шифрования богата как глубокими теоретическими результатами, так и востребованными практикой приложениями. Инструменты гомоморфной криптографии оказывают свое влияние на рынок облачных услуг, что и в той или иной степени сказывается на облике современных информационных технологий.

Список использованных источников:

1. Гомоморфное шифрование [Электронный ресурс]. – Режим доступа: http://www.ispras.ru/proceedings/docs/2007/12/isp_12_2007_27.pdf.
2. Защищенные вычисления и гомоморфное шифрование [Электронный ресурс]. – Режим доступа: http://2014.nscf.ru/TesisAll/4_Systemnoe_i_promezhytochnoe_PO/01_141_ByrtikaFB.pdf.